Federal Office
for Information Security

Common Criteria Protection Profile
Cryptographic Service Provider
BSI-CC-PP-0104-2019

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn

Internet: https://www.bsi.bund.de

Table of Contents

Figures

Tables

1 PP introduction

1.1 PP reference

Title:	Common Criteria Protection Profile Cryptographic Service Provider
Sponsor:	BSI
CC Version:	3.1 Revision 5
Assurance Level:	EAL4 augmented with ALC_DVS.2 and AVA_VAN.5
General Status:	Final
Version Number:	0.9.8
Registration:	BSI-CC-PP-0104
Keywords:	Cryptographic Module, Cryptography

1.2 TOE overview

TOE type

The Target of Evaluation (TOE) is a cryptographic service provider (CSP) component. The TOE is dedicated to provide cryptographic services for the protection of the confidentiality and the integrity of user data, and for entity authentication.

TOE definition

The TOE is physically defined as a device consisting of hardware, firmware and software. The TOE may be implemented as security integrated circuit platform for application, dedicated system on chip core or security integrated circuit.

The TOE security functionality (TSF) is logically defined by a common set of security services for users and security mechanisms for internal use. The cryptographic services for users comprise

- authentication of users,
- authentication and attestation of the TOE to entities,
- data authentication and non-repudiation including time stamps,
- encryption and decryption of user data,
- trusted channel including mutual authentication of the communicating entities, encryption and message authentication proof for the sent data, decryption and message authentication verification for received data,
- management of cryptographic keys with security attributes including key generation, key derivation and key agreement, internal storage of keys, import and export of keys with protection of their confidentiality and integrity,
- generation of random bits which may be used for security services outside the TOE.

The TOE uses memory encryption for protection of internally stored data.

The TOE is dedicated for composed IT products comprising the TOE and one or more application components. The TOE provides the security services for these application components. The PP considers two different architecture of the composed IT product:

- Platform architecture: The TOE is a platform consisting of hardware and an operating system providing a secure execution environment and security services for the application component running on top.

- Client-server architecture: The TOE and the application component are physically separated components interacting through a trusted channel. The application component (in client role) uses the security services of the TOE (in server role).

The communication between the TOE and the application is protected by means of secure channel. A secure channel is a trusted channel (cf. for definition CC part 1 [CC1], paragraph 97) which is physically protected and logical separated communication channel between the TOE and the user, or is protected by means of cryptographic mechanisms. The TOE supports cryptographically protected trusted channel between the TOE and the external entities. In case of platform architecture the TOE protects the communication with the application physically and by logical separated communication channel. In case of client-server architecture the protection of the communication depends on the capabilities of the application. If the application supports cryptographically protected trusted channel the TOE and the application should enforce cryptographically protected communication. If the application does not support cryptographically protected trusted channel the operational environment of the TOE shall protect the communication between the TOE and the application.

The internal cryptographic TSF is used for

- TSF data import including certificates and cryptographic keys,
- confidentiality protection of stored user data and TSF data.

The non-cryptographic TSF provides human user authentication, access control on cryptographic TSF and cryptographic keys and TSF protection.

The TOE supports download, authenticity verification and decryption of Update Code Packages for the CSP.

The TOE may provide functionality to establish a cluster of TOE samples for scalability of performance and availability of security services. In this case the security target shall claim conformance to the PP configuration consisting of the PP in hand as Base-PP and the PP-Module Cryptographic Service Provider Clustering (certification ongoing).

The TOE may provide a time service, time stamp service and security audit. In this case the security target shall claim conformance to the PP configuration consisting of the PP in hand as Base-PP and the PP-Module Cryptographic Service Provider Time Stamp and Audit (certification ongoing).

Method of use

The TOE is intended to be used with different applications. The TOE security services are logically separated and provided through well-defined external interfaces. The TSF is self-contained, i. e. it is provided by the TOE itself. The operational environment can not affect the security and correctness of the TSF, but it supports the availability of the TSF.

Life cycle

The protection profile in hand allows for a wide range of life cycle models for the development and maintenance of a TOE. The TOE implementation may belong to the technical domain “Smartcards and Similar Devices” or “Hardware Devices with Security Boxes” (cf. [SOGIS IT-TDs]). The security target shall provide a more detailed description of the life cycle description as necessary for the understanding of the stages of existence of the TOE in time. If the TOE belongs to the technical domain “Smartcards and Similar Devices” the life cycle definition should meet [JILGuidance].

The TOE shall store authentication keys used for prove of its own identity. The TOE sample shall be delivered with attestation keys for attestation as genuine sample of the certified product, cf. chapter 6.1.5. The identity authentication keys and the attestation keys shall be managed by the TOE manufacturer, a TOE vendor, or a trust center depending on the security policy for the TOE delivery or usage.

The life cycle of the TOE ends with implementation of any update code package changing the TOE to a new IT product, cf. chapter 6.1.10.

Non-TOE hardware/software/firmware available to the TOE

The TOE does not need non-TOE hardware, firmware or software to run.

2 Conformance claims

2.1 CC conformance claims

The PP claims conformance to CC version 3.1 revision 5.

Conformance of this PP with respect to CC Part 2 [CC2] (security functional components) is CC Part 2 extended.

Conformance of this PP with respect to CC Part 3 [CC3] (security assurance components) is CC Part 3 conformant.

2.2 Package claim

This PP claims package-augmented conformance to EAL4. The minimum assurance level for this protection profile is EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.

2.3 PP claim

This PP does not claim conformance to any PP.

2.4 Conformance rationale

This chapter is not applicable because the PP does not claim conformance to any PP.

2.5 Conformance statement

Security targets and protection profiles claiming conformance to this PP at hand must conform with **strict** conformance to this PP.

3 Security problem definitions

3.1 Introduction

Assets

The assets of the TOE are

- user data which integrity and confidentiality shall be protected,
- cryptographic services and keys which shall be protected against unauthorized use or misuse,
- Update Code Packages (UCP).

The cryptographic keys are TSF data because they are used for cryptographic operations protecting user data and the enforcement of the SFR relies on these data for the operation of the TOE.

Users and subjects

The TOE knows external entities (users) as

- *human user* communicating with the TOE for security management of the TOE,
- *application component* using the cryptographic and other security services of the TOE and supporting the communication with remote entities (e. g. by providing certificates),
- *remote entity* exchanging user data and TSF data with the TOE over insecure media.

The TOE communicates with

- human user through a secure channel,
- application component through a secure channel,
- remote entities over a trusted channel using cryptographic mechanisms including mutual authentication.

The subjects as active entities in the TOE perform operations on objects. They obtain their associated security attributes from the authenticated users on behalf they are acting, or by default.

Objects

The TSF operates user data objects and TSF data objects (i. e. passive entities, that contain or receive information, and upon which subjects perform operations). User data objects are imported, used in cryptographic operation, temporarily stored, exported and destroyed after use. The Update Code Packages are user data objects imported and stored in the TOE until use for creation of an updated CSP. TSF data objects are created, temporarily or permanently stored, imported, exported and destroyed as objects of the security management. They may contain e. g. cryptographic keys with their security attributes, certificates, Authentication Data Records with authentication reference data of a user. Cryptographic keys are objects of the key management.

Security attributes

The security attributes of user known to the TOE are stored in *Authentication Data Records* containing

- *User Identity* (User-ID),
- *Authentication reference data*,

- *Role* with detailed access rights.

Passwords as Authentication Reference Data have the security attributes

- *status*: values *initial password*, *operational password*,
- *number of unsuccessful authentication attempts.*

Certificates contain security attributes of users including User identity, a public key and security attributes of the key. If certificates are used as authentication reference data for cryptographic entity authentication mechanisms they may contain the *Role* of the entity.

The user uses authentication verification data to prove its identity to the TOE. The TSF uses Authentication reference data to verify the claimed identity of a user. The TSF supports

- human user authentication by knowledge where the authentication verification data is a password and the authentication reference data is a password or an image of the password e. g. a salted hash value or a derived cryptographic key,
- human user authentication by possession of a token or as user of a terminal implementing user authentication by cryptographic entity authentication mechanism,
- cryptographic entity authentication mechanisms where the authentication verification data is a secret or private key and the authentication reference data is a secret or public key.

A human user may authenticate themselves to the TOE and the TOE authenticates to an external entity in charge of the authenticated authorized user.

The TOE knows at least the following roles taken by a user or a subject acting on behalf of a user:

- *Unidentified User*: this role is associated with any user not (successfully) identified by the TOE. This role is assumed after start-up of the TOE. The TSF associated actions allowed for the Unidentified User are defined in SFR FIA_UID.1.
- *Unauthenticated User*: this role is associated with an identified user but not (successfully) authenticated user. The TSF associated actions allowed for the Unauthenticated User are defined in SFR FIA_UAU.1.
- *Administrator*: successful authenticated user allowed to access the TOE in order to perform management functions. It is taken by a human user or a subject acting on behalf of a human user after successful authentication as Administrator.

  The Administrator role may be split in more detailed roles:

  - *Crypto-Officer*: role that is allowed to access the TOE in order to perform management of a cryptographic TSF.
  - *User Administrator*: role that is allowed to access the TOE in order to perform user management.
  - *Update Agent*: authorized user for import and verification of Update Code Package.

  The SFR uses the general term Administrator or a selection between Administrator role and these detailed roles in case they are supported by the TOE and separation of duties is appropriate.
- *Key Owner*: successful authenticated user allowed to perform cryptographic operation with their own keys. This role may be claimed by human user or an entity.
- *Application Component*: subjects in this role are allowed to use assigned security services of the TOE without authenticated human user session (e. g. export and import of wrapped keys). This role may be assigned to an entity communicating through a physically separated secure channel or through a trusted channel (which requires assured identification of its end points).

The TOE is delivered with initial Authentication Data Records for Unidentified User, Unauthenticated User and administrator role(s). The Authentication Data Records for Unidentified User and Unauthenticated User have no Authentication Reference Data. The roles are not exclusive, i. e. a user or subject may be in more then one role, e. g. a human user may claim the Crypto-Officer and Key Owner role at the same time. The SFR may define limitation on roles one user may associated with.

Cryptographic keys have at least the security attributes

- *Key identity* that uniquely identifies the key,
- *Key entity*, i. e. the identity of the entity this key is assigned to,
- *Key type*, i. e. as secret key, private key, public key,
- *Key usage type*, identifying the cryptographic mechanism or service the key can be used for, e. g. a private signature key may be used by a digital signature-creation mechanism (cf. FCS_COP.1/CDS-ECDSA or FCS_COP.1/CDS-RSA), and depending on the certificate for data authentication with identity of guarantor (cf. FDP_DAU.2/Sig) by key usage type "*DigSign*" or attestation (cf. FDP_DAU.2/Att) by key usage type "*Attestation*".
- *Key access control attributes*, i. e. list of combinations of the identity of the user, the role for which the user is authenticated and the allowed key management function or cryptographic operation, including
  - *Import* of the key is allowed or forbidden,
  - *Export* of the key is allowed or forbidden,

and may have the security attribute

- *Key validity time period*, i. e. the time period for operational use of the key; the key must not be used before or after this time slot,
- *Key usage counter*, i. e. the number of operations performed with this key e. g. number of signature created with a private signature key.

The UCP have at least the security attributes

- *Issuer* of the UCP,
- *Version Number* of the UCP.

3.2 Threats

T.DataCompr Compromise of communication data
An unauthorized entity gets knowledge of the information contained in data stored on TSF controlled media or transferred between the TOE and authenticated external entities.

T.DataMani Unauthorized generation or manipulation of communication data
An unauthorized entity generates or manipulates user data stored on TSF controlled media or transferred between the TOE and authenticated external entities and accepted as valid data by the recipient.

T.Masqu Masquerade authorized user
A threat agent might masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources.

T.ServAcc Unauthorized access to TOE security services
A attacker gets as TOE user unauthorized access to security services of the TOE.

T.PhysAttack Physical attacks
An attacker gets physical access to the TOE and may (1) disclose or manipulate user data under TSF control and TSF data, and (2) affect TSF by (a) physical probing and manipulation, (b) applying environmental stress or (c) exploiting information leakage from the TOE.

T.FaUpD Faulty Update Code Package
An unauthorized entity provides an unauthorized faulty Update Code Package enabling attacks against

integrity of TSF implementation, confidentiality and integrity of user data and TSF data after installation of the faulty Update Code Package.

3.3 Organisational security policies

OSP.SecCryM Secure cryptographic mechanisms
The TOE uses only secure cryptographic mechanisms as confirmed by the certification body for the specified TSF, the assurance security requirements and the operational environment.

OSP.SecService Security services of the TOE
The TOE provides security services to the authorized users for encryption and decryption of user data, authentication prove and verification of user data, entity authentication to external entities including attestation, trusted channel and random bit generation.

OSP.KeyMan Key Management
The key management ensures the integrity of all cryptographic keys and the confidentiality of all secret or private keys over the whole life cycle which comprises their generation, storage, distribution, application, archiving and deletion. The cryptographic keys and cryptographic key components shall be generated, operated and managed by secure cryptographic mechanisms and assigned to the secure cryptographic mechanisms they are intended to be used with and to the entities authorized for their use.

OSP.TC Trust center
The trust centers provide secure certificates for trustworthy certificate holder with correct security attributes. The TOE uses certificates for identification and authentication of users, access control and secure use of security services of the TOE including key management and attestation.

OSP.Update Authorized Update Code Packages
The Update Code Packages are delivered in encrypted form and signed by the authorized issuer. The TOE verifies the authenticity of the received Update Code Package using the CSP before storing in the TOE. The TOE restricts the storage of authentic Update Code Package to an authorized user.

3.4 Assumptions

A.SecComm Secure communication
Remote entities support trusted channel using cryptographic mechanisms. The operational environment shall protect the local communication channels by trusted channels using cryptographic mechanisms or by secure channel using non-cryptographic security measures..

4 Security objectives

4.1 Security objectives for the TOE

O.AuthentTOE Authentication of the TOE to external entities
The TOE authenticates themselves in charge of authorized users to external entities by means of secure cryptographic entity authentication and attestation.

O.Enc Confidentiality of user data by means of encryption and decryption
The TOE provides secure encryption and decryption as security service for the users to protect the confidentiality of user data imported, exported or stored on media in the scope of TSF control.

O.DataAuth Data authentication by cryptographic mechanisms
The TOE provides secure symmetric and asymmetric data authentication mechanisms as security services for the users to protect the integrity and authenticity of user data.

O.RBGS Random bit generation service
The TOE provide cryptographically secure random bit generation service for the users.

O.TChann Trusted channel
The TSF provides trusted channel using secure cryptographic mechanisms for the communication between the TSF and external entities. The TOE provides authentication of all communication end points, ensures the confidentiality and integrity of the communication data exchanged through the trusted channel.

Note the TSF can establish the trusted channel by means of secure cryptographic mechanisms only if the other endpoint supports these secure cryptographic mechanisms as well. If trusted channel cannot be established by means of secure cryptographic mechanisms due to missing security functionality of the user then the operational environment shall provide a secure channel protecting the communication by non-cryptographic security measures, cf. A.SecComm and OE.SecComm.

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 self-test, identification of the TOE and authentication of the TOE. The TOE shall authenticate IT entities using secure cryptographic mechanisms.

O.AccCtrl Access control
The TOE provides access control on security services, operations on user data, management of TSF and TSF data.

O.SecMan Security management
The TOE provides security management of users, TSF, TSF data and cryptographic keys by means of secure cryptographic mechanisms and using certificates. The TSF generates, derives, agrees, import and export cryptographic keys as security service for users and for internal use. The TSF shall destruct unprotected secret or private keys in such a way that any previous information content of the resource is made unavailable.

O.TST Self-test
The TSF performs self-tests during initial start-up, at the request of the authorised user and after power-on. The TSF enters secure state if self-test fails or attacks are detected.

O.PhysProt Physical protection
The TSF protects the confidentiality and integrity of user data, TSF data and its correct operation against physical attacks and environmental stress. In case of platform architecture the TSF protects the secure execution environment for and the communication with the application component running on the TOE.

O.SecUpCP Secure import of Update Code Package
The TSF verifies the authenticity of received encrypted Update Code Package, decrypts authentic Update Code Package and allows authorized users to store decrypted Update Code Package.

4.2 Security objectives for the operational environment

OE.CommInf Communication infrastructure
The operational environment shall provide public key infrastructure for entities in the communication networks. The trust centers generate secure certificates for trustworthy certificate holder with correct security attributes. They distribute securely their certificate signing public key for verification of digital signature of the certificates and run a directory service for dissemination of certificates and provision of revocation status information of certificates.

OE.AppComp Support of the Application component
The Application component supports the TOE for communication with users and trust centers.

OE.SecManag Security management
The operational environment shall implement appropriate security management for secure use of the TOE including user management, key management. It ensures secure key management outside the TOE and uses the trust center services to determine the validity of certificates. The cryptographic keys and cryptographic key components shall be assigned to the secure cryptographic mechanisms they are intended to be used with and to the entities authorized for their use.

OE.SecComm Protection of communication channel
Remote entities shall support trusted channels with the TOE using cryptographic mechanisms. The operational environment shall protect the local communication channels by trusted channels using cryptographic mechanisms or by secure channel using non-cryptographic security measures.

OE.SUCP Signed Update Code Packages
The secure Update Code Package is delivered in encrypted form and signed by the authorized issuer together with its security attributes.

4.3 Security objective rationale

The following table traces the security objectives for the TOE back to threats countered by that security objective and OSPs enforced by that security objective, and the 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.

	T.DataCompr	T.DataMani	T.Masqu	T.ServAcc	T.PhysAttack	T.FaUpD	OSP.SecCryM	OSP.SecService	OSP.KeyMan	OSP.TC	OSP.Update	A.SecComm
O.AccCtrl				x								
O.AuthentTOE							x	x				
O.DataAuth		x					x	x				
O.Enc	x						x	x				
O.I&A			x	x			x	x				
O.PhysProt					x							

	T.DataCompr	T.DataMani	T.Masqu	T.ServAcc	T.PhysAttack	T.FaUpD	OSP.SecCryM	OSP.SecService	OSP.KeyMan	OSP.TC	OSP.Update	A.SecComm
O.RBGS							x	x				
O.SecMan			x				x		x	x		
O.SecUpCP						x					x	
O.Tchann	x	x	x	x			x	x				
O.TST					x							
OE.AppComp	x	x		x						x		
OE.CommInf	x	x		x				x	x	x		
OE.SecComm	x	x		x								x
OE.SecManag			x					x	x			
OE.SUCP						x					x	

Table 1: Security objective rationale

The following part of the chapter demonstrate that the security objectives counter all threats and enforce all OSPs, and the security objectives for the operational environment uphold all assumptions.

The threat T.DataCompr "Compromise of communication data": is countered by the security objectives for the TOE and the operational environment

- O.Enc requires the TOE to provide encryption and decryption as security service for the users to protect the confidentiality of user data,
- O.TChann requires the TOE to support trusted channel between TSF and the application component, and between TSF and other users, and the application component and other users with authentication of all communication end points, protected communication ensuring the confidentiality and integrity of the communication and to prevent misuse of the session of authorized users.
- OE.AppComp requires the application component to support the TOE for communication with users and trust center.
- OE.CommInf requires the operational environment to provide the communication infrastructure especially trust center services.
- OE.SecComm requires the operational environment to protect the confidentiality and integrity of communication over local communication channel by physical security measures and remote entities to support trusted channels by means of cryptographic mechanisms. If a trusted channel cannot be established due to missing security functionality of the application component or human user communication channel the operational environment shall protect the communication, cf. A.SecComm and OE.SecComm.

The threat T.DataMani "Unauthorized generation or manipulation of communication data" is countered by the security objectives for the TOE and the operational environment:

- O.DataAuth requires the TOE to provide symmetric and asymmetric data authentication mechanisms as security service for the users to protect the integrity and authenticity of user data.
- O.TChann requires the TOE to support trusted channel for authentication of all communication end points, protected communication with the application component and other users to ensure the

confidentiality and integrity of the communication and to prevent misuse of the session of authorized users.

- OE.AppComp requires the application component to support the TOE for communication with users and trust center.
- OE.CommInf requires the operational environment to provide trust center services and securely distribute root public keys.
- OE.SecComm requires the operational environment to protect the confidentiality and integrity of communication with the TOE. Remote entities shall support trusted channels with the TOE using cryptographic mechanisms. The operational environment shall protect the local communication channels by trusted channels using cryptographic mechanisms or by secure channel using non-cryptographic security measures.

The threat T.Masqu “Masquerade authorized user” is countered by the security objectives for the TOE and the operational environment:

- O.I&A requires the TSF to identify uniquely users and verify the claimed identity of the user before providing access to any controlled resources with the exception of self-test, identification of the TOE and authentication of the TOE.
- O.TChann requires the TSF to provide authentication of all communication end points of the trusted channel.
- O.SecMan requiring the TSF to provides security management of users, TSF, TSF data and cryptographic keys by means of secure cryptographic mechanisms and using certificates.
- OE.SecMan requiring the operational environment to implement appropriate security management for secure use of the TOE including user management.

The threat T.ServAcc “Unauthorized access to TOE security services” is countered by the security objectives for the TOE and the operational environment:

- O.I&A requires the TSF to uniquely identify users and to authenticate users before providing access to any controlled resources with the exception of self-test, identification of the TOE and authentication of the TOE. Note an unauthenticated user is allowed to request authentication of the TOE.
- O.AccCtrl requires the TSF to control access on security services, operations on user data, management of TSF and TSF data.
- O.Tchann requires mutual authentication of the external entity and the TOE and the authentication of communicated data to prevent misuse of the communication with external entities. The operational environment is required by OE.SecComm to ensure secure channels if trusted channel cannot be established.
- The operational environment OE.CommInf requires provision of a public key infrastructure for entity authentication and OE.AppComp requires the application to support communication with trust centers.

The threat T.PhysAttack “Physical attacks” is directly countered by the security objectives

- O.PhysProt requires the TSF to protects the confidentiality and integrity of user data, TSF data and its correct operation against physical attacks and environmental stress.
- O.TST requires the TSF to perform self-tests and to enter secure state if self-test fails or attacks are detected as means to ensure robustness against perturbation.

The threat T.FaUpD ”Faulty Update Code Package” is directly countered by the security objective O.SecUpCP verifying the authenticity of UCP under the condition that trustworthy UCP are signed as required by OE.SUCP

- O.SecUpCP “Secure import of Update Code Package” requires the TOE to verify the authenticity of received encrypted Update Code Package before decrypting and storing authentic an Update Code Package.
- OE.SUCP “Signed Update Code Packages” requires the *Issuer* to sign secure Update Code packages together with its security attributes.

The organizational security policy OSP.SecCryM “Secure cryptographic mechanisms” is implemented by means of secure cryptographic mechanisms required in

- O.I&A “Identification and authentication of users” and O.AuthentTOE “Authentication of the TOE to external entities” requiring secure entity authentication mechanisms of users and TOE,
- O.Enc “Confidentiality of user data by means of encryption and decryption” and O.DataAuth ”Data authentication by cryptographic mechanisms” requiring secure cryptographic mechanisms for protection of confidentiality and integrity of user data,
- O.TChann “Trusted channel” requiring secure cryptographic mechanisms for entity authentication mechanisms of users and TOE, protection of confidentiality and integrity of communication data.
- O.RBGS “Random bit generation service” requires the TOE to provide cryptographically secure random bit generation service for the users.
- O.SecMan “Security management” requiring security management of TSF data and cryptographic keys by means of secure cryptographic mechanisms and using certificates.

The organizational security policy OSP.SecService “Security services of the TOE” is directly implemented by security objectives for the TOE O.Enc “Confidentiality of user data by means of encryption and decryption”, O.DataAuth ”Data authentication by cryptographic mechanisms”, O.I&A “Identification and authentication of users”, O.AuthentTOE “Authentication of the TOE to external entities”, O.TChann “Trusted channel” and O.RBGS “Random bit generation service” requiring TSF to provide cryptographic security services for the user. The OSP.SecService is supported by OE.CommInf “Communication infrastructure” and OE.SecManag “Security management” providing the necessary measure for the secure use of these services.

The organizational security policy OSP.KeyMan “Key Management” is directly implemented by O.SecMan “Security management” and supported by trust center services according to OE.CommInf “Communication infrastructure” and OE.SecManag “Security management”.

The organizational security policy OSP.TC “Trust center” is implemented by security objectives for the TOE and the operational environment:

- O.SecMan “Security management” uses certificates for security management of users, TSF, TSF data and cryptographic keys.
- OE.CommInf “Communication infrastructure” requires trust centers to generate secure certificates for trustworthy certificate holder with correct security attributes and to distribute certificates and revocation status information.
- OE.AppComp “Support of the Application component” requires the Application component to support the TOE for communication with trust centers.

The organizational security policy OSP.Update “Authorized Update Code Packages” is implemented directly by the security objectives for the TOE O.SecUpCP and the operational environment OE.SUCP.

The assumption A.SecComm “Secure communication” assumes that the operational environment protects the confidentiality and integrity of communication data and ensures reliable identification of its end points. The security objective for the operational environment OE.SecComm requires the operational environment to protect local communication physically and the remote entities to support trusted channels using cryptographic mechanisms.

5 Extended component definition

5.1 Generation of random numbers (FCS_RNG)

Family Behaviour

This family defines quality requirements for the generation of random numbers that are intended to be used for cryptographic purposes.

Component levelling:

FCS_RNG.1 Generation of random numbers, requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no auditable events foreseen.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].

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

5.2 Cryptographic key derivation (FCS_CKM.5)

This chapter describes a component of the family Cryptographic key management (FCS_CKM) for key derivation as process by which one or more keys are calculated from either a pre-shared key or a shared secret and other information. Key derivation is the deterministic repeatable process by which one or more keys are calculated from both a pre-shared key or shared secret, and other information, while key generation required by FCS_CKM.1 uses internal random numbers.

The component FCS_CKM.5 is on the same level as the other components of the family FCS_CKM.

Management: FCS_CKM.5

There are no management activities foreseen

Audit: FCS_CKM.5

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

a) Minimal: Success and failure of the activity.

b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).

FCS_CKM.5 Requires the TOE to provide key derivation.

FCS_CKM.5 Cryptographic key derivation

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.5.1 The TSF shall derive cryptographic keys [assignment: *key type*] from [assignment: *input parameters*] in accordance with a specified cryptographic key derivation algorithm [assignment: *cryptographic key derivation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

5.3 Authentication Proof of Identity (FIA_API)

To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

Family Behaviour

This family defines functions provided by the TOE to prove its identity and to be verified by an external entity in the TOE IT environment.

Component levelling:

FIA_API Authentication Proof of Identity
1

FIA_API.1 Authentication Proof of Identity, provides prove of the identity of the TOE to an external entity.

Management: FIA_API.1

The following actions could be considered for the management functions in FMT:

a) Management of authentication information used to prove the claimed identity.

Audit: FIA_API.1

There are no auditable events foreseen.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *object, authorized user or role*] to an external entity.

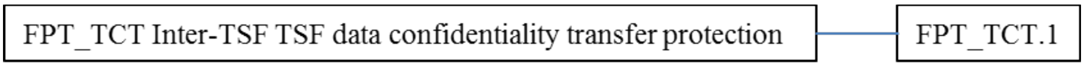
5.4 Inter-TSF TSF data confidentiality transfer protection (FPT_TCT)

This section describes the functional requirements for confidentiality protection of inter-TSF transfer of TSF data. The family is similar to the family Basic data exchange confidentiality (FDP_UCT) which defines functional requirements for confidentiality protection of exchanged user data.

Family Behaviour

This family requires confidentiality protection of exchanged TSF data.

Component levelling:


FPT_TCT Inter-TSF TSF data confidentiality transfer protection
FPT_TCT.1

FPT_TCT.1 Requires the TOE to protect the confidentiality of information in exchanged the TSF data.

Management: FPT_TCT.1

There are no management activities foreseen.

Audit: FPT_TCT.1

There are no auditable events foreseen.

FPT_TCT.1 TSF data confidentiality transfer protection

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FMT_MTD.1 Management of TSF data or
FMT_MTD.3 Secure TSF data]

FPT_TCT.1.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] by providing the ability to [selection: *transmit, receive, transmit and receive*] TSF data in a manner protected from unauthorised disclosure.

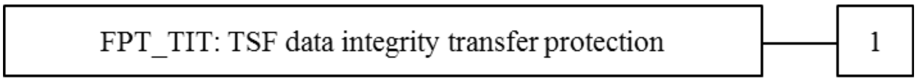
5.5 Inter-TSF TSF data integrity transfer protection (FPT_TIT)

This section describes the functional requirements for integrity protection of TSF data exchanged with another trusted IT product. The family is similar to the family Inter-TSF user data integrity transfer protection (FDP_UIT) which defines functional requirements for integrity protection of exchanged user data.

Family Behaviour

This family requires integrity protection of exchanged TSF data.

Component levelling:



FPT_TIT.1 Requires the TOE to protect the integrity of information in exchanged the TSF data.

Management: FPT_TIT.1

There are no management activities foreseen.

Audit: FPT_TIT.1

There are no auditable events foreseen.

FPT_TIT.1 TSF data integrity transfer protection

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FMT_MTD.1 Management of TSF data or
FMT_MTD.3 Secure TSF data]

FPT_TIT.1.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to [selection: *transmit, receive, transmit and receive*] TSF data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors.

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

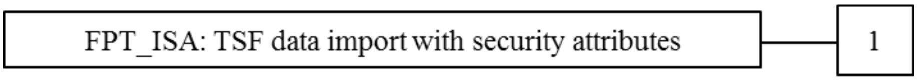
5.6 TSF data import with security attributes (FPT_ISA)

This section describes the functional requirements for TSF data import with security attributes from another trusted IT product. The family is similar to the family Import from outside of the TOE (FDP_ITC) which defines functional requirements for user data import with security attributes.

Family Behaviour

This family requires TSF data import with security attributes.

Component levelling:



FPT_ISA.1 Requires the TOE to import TSF data with security attributes.

Management: FPT_ISA.1

There are no management activities foreseen.

Audit: FPT_ISA.1

There are no auditable events foreseen.

FPT_ISA.1 Import of TSF data with security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FMT_MTD.1 Management of TSF data or
FMT_MTD.3 Secure TSF data]
[FMT_MSA.1 Management of security attributes, or
FMT_MSA.4 Security attribute value inheritance]
FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_ISA.1.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] when importing TSF data, controlled under the SFP, from outside of the TOE.

FPT_ISA.1.2 The TSF shall use the security attributes associated with the imported TSF data.

FPT_ISA.1.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the TSF data received.

FPT_ISA.1.4 The TSF shall ensure that interpretation of the security attributes of the imported TSF data is as intended by the source of the TSF data.

FPT_ISA.1.5 The TSF shall enforce the following rules when importing TSF data controlled under the SFP from outside the TOE: [assignment: *additional importation control rules*].

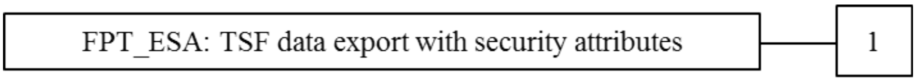
5.7 TSF data export with security attributes (FPT_ESA)

This section describes the functional requirements for TSF data export with security attributes to another trusted IT product. The family is similar to the family Export to outside of the TOE (FDP_ETC) which defines functional requirements for user data export with security attributes.

Family Behaviour

This family requires TSF data export with security attributes.

Component levelling:



FPT_ESA.1 Requires the TOE to export TSF data with security attributes.

Management: FPT_ESA.1

There are no management activities foreseen.

Audit: FPT_ESA.1

There are no auditable events foreseen.

FPT_ESA.1 Export of TSF data with security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FMT_MTD.1 Management of TSF data or
FMT_MTD.3 Secure TSF data]
[FMT_MSA.1 Management of security attributes, or
FMT_MSA.4 Security attribute value inheritance]
FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_ESA.1.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] when exporting TSF data, controlled under the SFP(s), outside of the TOE.

FPT_ESA.1.2 The TSF shall export the TSF data with the TSF data's associated security attributes.

FPT_ESA.1.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported TSF data.

FPT_ESA.1.4 The TSF shall enforce the following rules when TSF data is exported from the TOE: [assignment: *additional exportation control rules*].

5.8 Stored data confidentiality (FDP_SDC)

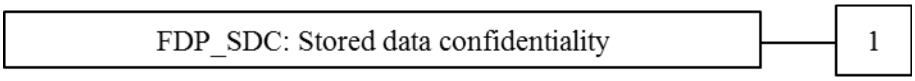
To define the security functional requirements of the TOE an additional family (FDP_SDC.1) of the Class FDP (User data protection) is defined here.

The family "Stored data confidentiality (FDP_SDC)" is specified as follows.

Family behaviour

This family provides requirements that address protection of user data confidentiality while these data are stored within memory areas protected by the TSF. The TSF provides access to the data in the memory through the specified interfaces only and prevents compromise of their information bypassing these interfaces. It complements the family Stored data integrity (FDP_SDI) which protects the user data from integrity errors while being stored in the memory.

Component levelling



FDP_SDC.1 Requires the TOE to protect the confidentiality of information of the user data in specified memory areas.

Management: FDP_SDC.1

There are no management activities foreseen.

Audit: FDP_SDC.1

There are no auditable events foreseen.

FDP_SDC.1	Stored data confidentiality
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_SDC.1.1	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the [assignment: *memory area*].

6 Security requirements

The CC allows several operations to be performed on functional requirements: *refinement*, *selection*, *assignment*, and *iteration*. 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) directly included in the requirement text as **bold** text. In cases where words from a CC requirement component were deleted, these words are ~~crossed out~~.
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

The TOE provides cryptographic security services for encryption and decryption of user data, entity authentication of external entities and to external entities, authentication prove and verification of user data, trusted channel and random number generation.

The TOE enforces the *Cryptographic Operation SFP* for protection of theses cryptographic services which subjects, objects, and operations are defined in the SFRs FDP_ACC.1/Oper and FDP_ACF/Oper.

The TOE provides hybrid encryption and decryption combined with data integrity mechanisms for the cipher text as cryptographic security service of the TOE. The encryption FCS_COP.1/HEM combines the generation of a data encryption key and message authentication code (MAC) key, the asymmetric encryption of the data encryption key with an asymmetric key encryption key, cf. FCS_CKM.1/ECKA-EG, FCS_CKM.1/RSA, and the symmetric encryption of the data with the data encryption key and data integrity mechanism with MAC calculation for the cipher text. The receiver reconstructs the data encryption key and the MAC key, cf. FCS_CKM.5/ECKA-EG, calculates the MAC for the cipher text and compares it with the received MAC. If the integrity of the cipher text is determined than the receiver decrypts the cipher text with the data decryption key, cf. FCS_COP.1/HDM.

In general, authentication is the provision of assurance of the claimed identity of an entity. The TOE authenticates human users by password, cf. FIA_UAU.5.1 clause 1. But a human user may authenticate themselves to a token and the token authenticates to the TOE. Cryptographic authentication mechanisms allow an entity to prove its identity or the origin of its data to a verifying entity by demonstrating its knowledge of a secret. The entity authentication is required by FIA_UAU.5.1 clauses (2) to (6). The chapter 5.3 describes SFR for the authentication of the TOE to external entities required by the SFR FIA_API.1. This authentication may include attestation of the TOE as genuine TOE sample, cf. 6.1.4. The authentication may be mutual as required for trusted channels in chapter 6.1.5.

Protocols may use symmetric cryptographic algorithms, where the proving and the verifying entity using the same secret key, may demonstrate that the proving entity belongs to a group of entities sharing this key, e.g. sender and receiver (cf. FTP_ITC.1, FCS_COP.1/TCM). In case of asymmetric entity authentication mechanisms the proving entity uses a private key and the verifying entity uses the corresponding public key closely linked to the claimed identity often by means of a certificate. The same cryptographic mechanisms for digital signature generation algorithm (FCS_COP.1/CDS-*) and signature verification algorithm (cf. FCS_COP.1/VDS-*) may be used for entity authentication, data authentication and non-repudiation depending on the security attributes of the cryptographic keys e.g. encoded in the certificate (cf. FPT_ISA.1/Cert).

Trusted channel requires mutual authentication of endpoints with key exchange of key agreement, protection of confidentiality by means of encryption and cryptographic data integrity protection.

The TSF provides security management for user and TSF data including cryptographic keys. The key management comprises administration and use of generation, derivation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation and destruction of keying material in accordance with a security policy. The key management of the TOE supports the generation, derivation, export, import, storage and destruction of cryptographic keys. The cryptographic keys are managed together with their security attributes.

The TOE enforces the *Key Management SFP* to protect the cryptographic keys (as data objects fo TSF data) and the key management services (as operation, cf. to SFR of the FMT class) provided for Administrators, Crypto-Officers, Key Owners and (as subjects). Note the cryptographic keys will be used for cryptographic operations under Cryptographic Operation SFP as well.

The subjects, objects and operations of the *Update SFP* are defined in the SFR FDP_ACC.1/UCP and FDP_ACF.1/UCP.

The SFR for cryptographic mechanisms based on elliptic curves refer to the following table for selection of curves, key sizes and standards.

Elliptic curve	Key size	Standard
brainpoolP256r1	*256 bits*	*RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111]*
brainpoolP384r1,	*384 bits*	*RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111]*
brainpoolP512r1	*512 bits*	*RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111]]*
Curve P-256	*256 bits*	*FIPS PUB 186-4 B.4 and D.1.2.3 [FIPS PUB 186-4]*
Curve P-384	*384 bits*	*FIPS PUB 186-4 B.4 and D.1.2.4 [FIPS PUB 186-4]*
Curve P-521	*521 bits*	*FIPS PUB 186-4 B.4 and D.1.2.5 [FIPS PUB 186-4]*

Table 2: Elliptic curves, key sizes and standards

For Diffie-Hellman key exchange refer to the following groups

Name	IANA no.	Specified in
256-bit random ECP group	19	[RFC5903]
384-bit random ECP group	20	[RFC5903]
521-bit random ECP group	21	[RFC5903]
brainpoolP256r1	28	[RFC6954]
brainpoolP384r1	29	[RFC6954]
brainpoolP512r1	30	[RFC6954]

Table 3: Recommended groups for the Diffie-Hellman key exchange

6.1.1 Key management

6.1.1.1 Management of security attributes

FDP_ACC.1/KM Subset access control – Cryptographic operation

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/KM The TSF shall enforce the *Key Management SFP*[1] on

(1) *subjects: [selection: Administrator, Crypto-Officer], Key Owner;*

(2) *objects: operational cryptographic keys*;

(3) *operations: key generation, key derivation, key import, key export, key destruction*[2].

FMT_MSA.1/KM Management of security attributes – Key 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/KM The TSF shall enforce the *Key Management SFP and Cryptographic Operation SFP*[3] to restrict the ability to

(1) *change_default*[4] the security attributes *Identity of the key, Key entity of the key, Key type, Key usage type, Key access control attributes, Key validity time period*[5] to *[selection: Administrator, Crypto-Officer]*[6],

(2) ***modify or delete***[7] **the security attributes *Identity of the key, Key entity, Key type, Key usage type, Key validity time period of an existing key***[8] **to *none***[9],

(3) ***modify independent on key usage***[10] ***the security attributes Key usage counter of an existing key***[11] **to *none***[12].

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

[2] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

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

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

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

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

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

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

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

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

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

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

(4) ***modify***[13] **the security attribute~~s~~** ***Key access control attribute of an existing key***[14] **to** ***[selection: Administrator, Crypto-Officer]***[15]*,*

(5) ***query***[16] **the security attributes** ***Key type, Key usage type, Key access control attributes, Key validity time period and Key usage counter of an identified key***[17] **to** ***[selection: Administrator, Crypto-Officer, Key Owner]***[18]*.*

Application note 1: The refinements repeats parts of the SFR component in order to avoid iteration of the component.

FMT_MSA.3/KM Static attribute initialisation – Key management

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1/KM The TSF shall enforce the *Key Management SFP, Cryptographic Operation SFP and Update SFP*[19] to provide *restrictive*[20] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/KM The TSF shall allow the [selection: *Administrator, Crypto-Officer*][21] to specify alternative initial values to override the default values when a **cryptographic key** ~~object or information~~ is created.

FMT_MTD.1/KM Management of TSF data – Key management

Hierarchical to: No other components.

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

FMT_MTD.1.1/KM The TSF shall restrict the ability to

(1) *create according to FCS_CKM.1*[22] the *cryptographic keys*[23] to [selection: *Administrator, Crypto-Officer, Key Owner*][24],

(2) ***import according to FPT_TCT.1/CK, FPT_TIT.1/CK and FPT_ISA.1/CK***[25] **the** ***cryptographic keys***[26] **to** ***[selection: Administrator, Crypto-Officer***]**[27],**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3) ***export according to FPT_TCT.1/CK, FPT_TIT.1/CK and FPT_ESA.1/CK***[28] **the *cryptographic keys***[29] **to *[selection: Administrator, Crypto-Officer, Key Owner*]**[30] ***if security attribute of the key allows export,***

(4) ***delete according to FCS_CKM.4***[31] **the *cryptographic keys***[32] **to *[selection: Administrator, Crypto-Officer, Key Owner]***[33].

Application note 2: The bullets (2) to (4) are refinements to avoid an iteration of component and therefore printed in bold.

6.1.1.2 Hash based functions

FCS_COP.1/Hash Cryptographic operation – Hash

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/Hash The TSF shall perform *hash generation*[34] in accordance with a specified cryptographic algorithm *SHA-256, SHA-384, SHA-512*[35] and cryptographic key sizes *none*[36] that meet the following: *FIPS 180-4 [FIPS PUB 180-4]*[37].

Application note 3: The hash function is a cryptographic primitive used for HMAC, cf. FCS_COP.1/HMAC, digital signature creation, cf. FCS_COP.1/CDS-*, digital signature verification, cf. FCS_COP.1/VDS-*, and key derivation, cf. FCS_CKM.5.

6.1.1.3 Management of Certificates

FMT_MTD.1/RK Management of TSF data – Root key

Hierarchical to: No other components.

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

FMT_MTD.1.1/RK The TSF shall restrict the ability to

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

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

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

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

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

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

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

[35] [assignment: *cryptographic algorithm*]

[36] [assignment: *cryptographic key sizes*]

[37] [assignment: *list of standards*]

(1) *create*[38]*, modify, clear and delete*[39] the *root key pair*[40] to [selection: *Administrator, Crypto-Officer*][41].

(2) *import and delete*[42] a *known as authentic public key of a certification authority in a PKI*[43] to *[selection: Administrator, Crypto-Officer]*[44].

Application note 4: The root key is defined here with respect to the key hierarchy known to the TOE. In case of clause (1), i. e. may be a key pair of an TOE internal key hierarchy. In clause (2) it may be a root public key of a PKI or a public key of another certification authority in a PKI known as authentic certificate signing key. The PKI may be used for user authentication, key management and signature-verification. The second bullet is a refinement to avoid an iteration of component and therefore printed in bold.

FPT_TIT.1/Cert TSF data integrity transfer protection – Certificates

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FMT_MTD.1 Management of TSF data or
FMT_MTD.3 Secure TSF data]

FPT_TIT.1.1/Cert The TSF shall enforce the *Key Management SFP*[45] to *receive*[46] **certificate** ~~TSF data~~ in a manner protected from *modification and insertion*[47] errors.

FPT_TIT.1.2/Cert The TSF shall be able to determine on receipt of **certificate** ~~TSF data~~ , whether *modification and insertion*[48] has occurred.

FPT_ISA.1/Cert Import of TSF data with security attributes - Certificates

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FMT_MTD.1 Management of TSF data or
FMT_MTD.3 Secure TSF data]
[FMT_MSA.1 Management of security attributes, or
FMT_MSA.4 Security attribute value inheritance]
FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_ISA.1.1/Cert The TSF shall enforce the *Key management SFP*[49] when importing **certificates** ~~TSF data~~, controlled under the SFP, from outside of the TOE.

FPT_ISA.1.2/Cert The TSF shall use the security attributes associated with the imported **certificate** ~~TSF data~~.

[38] "create" denotes initial setting a root key

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

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

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

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

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

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

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

[46] [selection: *transmit, receive, transmit and receive*]

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

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

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

FPT_ISA.1.3/Cert The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the **certificates** ~~TSF data~~ received.

FPT_ISA.1.4/Cert The TSF shall ensure that interpretation of the security attributes of the imported **certificates** ~~TSF data~~ is as intended by the source of the **certificates** ~~TSF data~~.

FPT_ISA.1.5/Cert The TSF shall enforce the following rules when importing **certificates** ~~TSF data~~ controlled under the SFP from outside the TOE:

(1) *The TSF imports the TSF data in certificates only after successful verification of the validity of the certificate in the certificate chain until known as authentic certificate according to FMT_MTD.1/RK.*

(2) *The validity verification of the certificate shall include*

(a) the verification of the digital signature of the certificate issuer except for root certificates,

(b) the security attributes in the certificate pass the interpretation according to FPT_TDC.1[50].

FPT_TDC.1/Cert Inter-TSF basic TSF data consistency - Certificate

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TDC.1.1/Cert The TSF shall provide the capability to consistently interpret *security attributes of cryptographic keys in the certificate and identity of the certificate issuer*[51] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Cert The TSF shall use **the following rules**:

(1) *the TOE reports about conflicts between the Key identity of stored cryptographic keys and cryptographic keys to be imported,*

(2) *the TOE does not change the security attributes Key identity, Key entity, Key type, Key usage type and Key validity time period of public key being imported from the certificate,*

(3) *the identity of the certificate issuer shall meet the identity of the signer of the certificate*[52]

when interpreting **the certificate from a trust center** ~~TSF data from another trusted IT product~~.

Application note 5: The security attributes assigned to certificate holder and cryptographic key in the certificate are used as TSF data of the TOE. The certificate is imported from trust center directory service or any other source but verified by the TSF (i.e. if verified successfully the source is the trusted IT product trust center directory server).

6.1.1.4 Key generation, agreement and destruction

Key generation (cf. FCS_CKM.1/ECC, FCS_CKM.1/RSA) is a randomized process which uses random secrets (cf. FCS_RNG.1), applies key generation algorithms and defines security attributes depending on the intended use of the keys and which has the property that it is computationally infeasible to deduce the output without prior knowledge of the secret input. *Key derivation* (cf. FCS_CKM.5/ECC) is a deterministic process by which one or more keys are calculated from a pre-shared key or shared secret or other information. It allows repeating the key generation if the same input is provided. *Key agreement* (cf.

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

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

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

FCS_CKM.5/ECDHE) is a key-establishment procedure process for establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key independently of the other party's contribution. Key agreement allows each participant to enforce the cryptographic quality of the agreed key. The component FCS_CKM.1 was refined for key agreement because it normally uses random bits as input. Hybrid cryptosystems (FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA) are a combination of a public key cryptosystem with an efficient symmetric key cryptosystem.

The user may need to specify the type of key, the cryptographic key generation algorithm, the security attributes and other necessary parameters.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].

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

Application note 6: The random bit generation shall be used for key generation and key agreement according to all instantiations of FCS_CKM.1, challenges in cryptographic protocols and cryptographic operations using random values according to FCS_COP.1/HEM and FCS_COP.1/TCE. The TOE provides the random number generation as security service for the user.

FCS_CKM.1/AES Cryptographic key generation – AES key

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/AES The TSF shall generate cryptographic **AES** keys in accordance with a specified cryptographic key generation algorithm *AES*[53] and specified cryptographic key sizes *128 bits, [*selection: *256 bits, no other key size]*[54] that meet the following: *ISO 18033-3 [ISO/IEC 18033-3]*[55].

Application note 7: The cryptographic key may be used with FCS_COP.1/ED, e. g. for internal purposes.

FCS_CKM.5/AES Cryptographic key derivation – AES key derivation

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.5.1/AES The TSF shall derive cryptographic *AES* key[56] from [assignment: *input parameters*] in accordance with a specified cryptographic key derivation algorithms *AES key generation using bit string derived from input parameters with KDF*[57] and specified cryptographic key

[53] [assignment: c*ryptographic key generation algorithm*]

[54] [assignment: *cryptographic key sizes*]

[55] [assignment: *list of standards*]

[56] [assignment: *key type*]

[57] [assignment: c*ryptographic key derivation algorithm*]

sizes *128 bits,* [selection: *256 bits, no other key size]*[58] that meet the following: *NIST SP800-56C [NIST-SP800-56C]*[59].

FCS_CKM.1/ECC Cryptographic key generation – Elliptic curve key pair ECC

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/ECC The TSF shall generate cryptographic **elliptic curve** key~~s~~ ***pair*** in accordance with a specified cryptographic key generation algorithm *ECC key pair generation with [selection: elliptic curves in the table 2]*[60] and specified cryptographic key sizes *[selection: key size in the table 2]*[61] that meet the following: *[selection: standards in the table 2]*[62].

Application note 8: The elliptic key pair generation uses a random bit string as input for the ECC key generation algorithm. The keys generation according to FCS_CKM.1/ECC and key derivation according to FCS_CKM.5/ECC are intended for different key management use cases but the keys itself may be used for same cryptographic operations.

FCS_CKM.5/ECC Cryptographic key derivation – ECC key pair derivation

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.5.1/ECC The TSF shall derive cryptographic *elliptic curve* key~~s~~ *pair*[63] from [assignment: *input parameters*] in accordance with a specified cryptographic key derivation algorithm *ECC key pair generation with [selection: elliptic curves in table 2] using bit string derived from input parameters with [assignment: KDF]* [64] and specified cryptographic key sizes *[selection: key size in the table 2]*[65] that meet the following: *[selection: standards in the table 2], [TR-03111]*[66].

Application note 9: The elliptic key pair derivation applies a key derivation function (KDF), e.g. from *[TR-03111] (Section 4.3.3.)* to the input parameter. It uses the output string of KDF instead of the random bit string as input for the ECC key generation algorithm (*[TR-03111]„ Section 4.1.1, Algorithms 1 or 2).* The input parameters shall include a secret of the length at least of the key size to ensure the confidentiality of the private key. The input parameters may include public known values or even values provided by external entities.

[58] [assignment: *cryptographic key sizes*]

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

[60] [assignment: c*ryptographic key generation algorithm*]

[61] [assignment: *cryptographic key sizes*]

[62] [assignment: *list of standards*]

[63] [assignment: *key type*]

[64] [assignment: c*ryptographic key derivation algorithm*]

[65] [assignment: *cryptographic key sizes*]

[66] [assignment: *list of standards*]

FCS_CKM.1/RSA Cryptographic key generation – RSA key pair

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/RSA The TSF shall generate cryptographic **RSA** key **pair** in accordance with a specified cryptographic key generation algorithm *RSA*[67] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: *PKCS #1 v2.2 [PKCS#1]*[68].

Application note 10: The cryptographic key sizes assigned in FCS_CKM.1/RSA must be at least 2000 bits. Cryptographic key sizes of at least 3000 bits are recommended. The FCS_CKM.1/RSA assigns given security attributes *Key identity* and *Key entity*. The security attribute *Key usage type* is DS-RSA for the private signature-creation key and public signature-verification key, RSA_ENC for public RSA encryption key and private RSA decryption key.

FCS_CKM.5/ECDHE Cryptographic key derivation – Elliptic Curve Diffie-Hellman ephemeral key agreement

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.5.1/ECDHE The TSF shall derive cryptographic *ephemeral* keys[69] **for data encryption and MAC with AES-128, [selection: *AES-256, none other*]** from *an agreed shared secret*[70] in accordance with a specified cryptographic key derivation algorithm *Elliptic Curve Diffie-Hellman ephemeral key agreement [selection: elliptic curves in table 2] and [selection: DH group in table 3] with a key derivation from the shared secret [assignment: key derivation function]*[71] and specified cryptographic key sizes *128 bits [selection:256 bits, none other]*[72] that meet the following: *TR-03111 [TR-03111]*[73].

Application note 11: The input parameters for key derivation is an agreed shared secret established by means of Elliptic Curve Diffie-Hellman. The table 2 lists elliptic curves and table 3 lists the Diffie-Hellman Groups for agreement of the shared secret. The SHA-1 shall be supported for generation of 128 bits AES keys. The SHA-256 shall be selected and used to generate 256 bits AES keys.

FCS_CKM.1/ECKA-EG Cryptographic key generation – ECKA-EG key generation with ECC encryption

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/ECKA-EG

The TSF shall generate **an ephemeral** cryptographic **elliptic curve** key **pair for ECKGA-EG***[TR-03111], sender role*) in accordance with a specified cryptographic key generation algorithm *ECC key pair generation with [selection: elliptic curves in the table 2]*[74] and

[67] [assignment: c*ryptographic key generation algorithm*]

[68] [assignment: *list of standards*]

[69] [assignment: *key type*]

[70] [assignment: *input parameters*]

[71] [assignment: *cryptographic key derivation algorithm*]

[72] [assignment: *cryptographic key sizes*]

[73] [assignment: *list of standards*]

[74] [assignment: c*ryptographic key generation algorithm*]

specified cryptographic key sizes *[selection: key size in the table 2]*[75] that meet the following: *[selection: standards in the table 2]*[76].

FCS_CKM.5/ECKA-EG Cryptographic key derivation – ECKA-EG key derivation

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.5.1/ECKA-EG The TSF shall derive cryptographic *data encryption and MAC* keys *for AES-128, [selection: AES-256, none other]*[77] from *a private and a public ECC key*[78] in accordance with a specified cryptographic key derivation algorithms *ECKGA-EG[TR-03111] [selection: elliptic curves in table 2] and X9.63 Key Derivation Function*[79] and specified cryptographic **symmetric** key sizes *128 bits [selection:256 bits, none other]*[80] that meet the following: *TR-03111[TR-03111], chapter 4.3.2.2*[81].

Application note 12: FCS_CKM.5/ECKA-EG is used by both the sender (encryption) and the recipient (decryption) to compute a secret point S_{AB} on an elliptic curve and the derived shared secret Z_{AB}. The shared secret is then used as input to the key derivation function to derive two symmetric keys, the encryption key and the MAC key which are used to encrypt or decrypt the message according to FCS_COP.1/HEM or FCS_COP.1/HDM, respectively. Sender and recipient use however different inputs to FCS_CKM.5/ECKA-EG. The sender first generates an ephemeral ECC key pair according to FCS_CKM.1/ECKA-EG and uses the generated ephemeral private key and the static public key of the recipient as input. The recipient first extracts the ephemeral public key from the encrypted message and uses the ephemeral public key and the static private key (cf. FCS_CKM.1/ECC for key generation) as input. The selection of elliptic curve, the ECC key size and length of the shared secret shall correspond to the selection of the AES key size, e. g. brainpoolP256r1 and 256 bits seed, ECC key and AES keys. FCS_CKM.1/ECKA-EG and FCS_CKM.5/ECKA-EG do not provide self-contained security services for the user but are necessary steps for FCS_COP.1/HEM and FCS_COP.1/HDM (refer to the next section 6.1.3).

FCS_CKM.1/AES_RSA Cryptographic key generation – Key generation and RSA encryption

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/AES_RSA The TSF shall generate **and encrypt seed, derive** cryptographic keys **from seed for data encryption and MAC with AES-128,** [**selection:** ***AES-256, none other***] in accordance with a specified cryptographic key generation algorithm *X9.63 Key Derivation Function[ANSI-X9.63] and RSA EME-OAEP[PKCS#1]*[82] and specified cryptographic **symmetric** key sizes *128 bits [selection:256 bits, none other]*[83] that meet the following: *ISO/IEC18033-3 [ISO/IEC 18033-3], PKCS #1 v2.2 [PKCS#1]*[84].

[75] [assignment: *cryptographic key sizes*]

[76] [assignment: *list of standards*]

[77] [assignment: *key type*]

[78] [assignment: *input parameters*]

[79] [assignment: c*ryptographic key derivation algorithm*]

[80] [assignment: *cryptographic key sizes*]

[81] [assignment: *list of standards*]

[82] [assignment: c*ryptographic key generation algorithm*]

[83] [assignment: *cryptographic key sizes*]

[84] [assignment: *list of standards*]

Application note 13: The asymmetric cryptographic key sizes used in FCS_CKM.1/AES_RSA must be at least 2000 bits. Cryptographic key sizes of at least 3000 bits are recommended. FCS_CKM.1/AES_RSA and FCS_CKM.5/AES_RSA do not provide self-contained security services for the user but they are only necessary steps for FCS_COP.1/HEM respective FCS_COP.1/HDM (refer to the next section 6.1.3).

FCS_CKM.5/AES_RSA Cryptographic key derivation – RSA key derivation and decryption

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.5.1/AES_RSA The TSF shall derive cryptographic *data encryption* key *and MAC* key *for AES-128, [selection: AES-256, none other]*[85] from **decrypted** *RSA encrypted seed*[86] in accordance with a specified cryptographic key derivation algorithm *RSA EME-OAEP[PKCS#1] and X9.63[ANSI-X9.63] Key Derivation Function*[87] and specified cryptographic **symmetric** key sizes *128 bits [selection:256 bits, none other]*[88] that meet the following: *ISO/IEC 14888-2 [ISO/IEC 14888-2]*[89].

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 standards*].

Refinement: The destruction of cryptographic keys shall ensure that any previous information content of the resource about the key is made unavailable upon the deallocation of the resource.

6.1.1.5 Key import and export

FCS_COP.1/KW Cryptographic operation – Key wrap

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,
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/KW The TSF shall perform *key wrap*[90] in accordance with a specified cryptographic algorithm *AES-Keywrap [selection: KW, KWP]*[91] and cryptographic key sizes **of the *key encryption***

[85] [assignment: *key type*]

[86] [assignment: *input parameters*]

[87] [assignment: c*ryptographic key derivation algorithm*]

[88] [assignment: *cryptographic key sizes*]

[89] [assignment: *list of standards*]

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

[91] [assignment: *cryptographic algorithm*]

***key** 128 bits [selection:256 bits, none other]*[92] that meet the following: *NIST SP800-38F [NIST-SP800-38F]*[93].

Application note 14: The selection of the length of the key encryption key shall be equal or greater than the security bits of the wrapped key for its cryptographic algorithm.

FCS_COP.1/KU Cryptographic operation – Key unwrap

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/KU The TSF shall perform *key unwrap*[94] in accordance with a specified cryptographic algorithm *AES-Keywrap [selection: KW, KWP]*[95] and cryptographic key sizes **of the *key encryption key*** *128 bits [selection:256 bits, none other]*[96] that meet the following: *NIST SP800-38F [NIST-SP800-38F]*[97].

FPT_TCT.1/CK TSF data confidentiality transfer protection – Cryptographic keys

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FMT_MTD.1 Management of TSF data or
FMT_MTD.3 Secure TSF data]

FPT_TCT.1.1/CK The TSF shall enforce the *Key Management SFP*[98] by providing the ability to *transmit and receive*[99] **cryptographic key** ~~TSF data~~ in a manner protected from unauthorised disclosure **according to FCS_COP.1/KW and FCS_COP.1/KU**.

FPT_TIT.1/CK TSF data integrity transfer protection – Cryptographic keys

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FMT_MTD.1 Management of TSF data or
FMT_MTD.3 Secure TSF data]

FPT_TIT.1.1/CK The TSF shall enforce the *Key Management SFP*[100] to *transmit and receive*[101] **cryptographic keys** ~~TSF data~~ in a manner protected from *modification and insertion*[102] errors **according to FCS_COP.1/KW**.

[92] [assignment: *cryptographic key sizes*]

[93] [assignment: *list of standards*]

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

[95] [assignment: *cryptographic algorithm*]

[96] [assignment: *cryptographic key sizes*]

[97] [assignment: *list of standards*]

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

[99] [selection: *transmit, receive, transmit and receive*]

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

[101] [selection: *transmit, receive, transmit and receive*]

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

FPT_TIT.1.2/CK The TSF shall be able to determine on receipt of **cryptographic keys** ~~TSF data~~, whether *modification and insertion*[103] has occurred **according to FCS_COP.1/KU**.

FPT_ISA.1/CK Import of TSF data with security attributes – Cryptographic keys

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FMT_MTD.1 Management of TSF data or
FMT_MTD.3 Secure TSF data]
[FMT_MSA.1 Management of security attributes, or
FMT_MSA.4 Security attribute value inheritance]
FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_ISA.1.1/CK The TSF shall enforce the *Key Management SFP*[104] when importing **cryptographic key** ~~TSF data~~, controlled under the SFP, from outside of the TOE.

FPT_ISA.1.2/CK The TSF shall use the security attributes associated with the imported **cryptographic key** ~~TSF data~~.

FPT_ISA.1.3/CK The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the **cryptographic key** ~~TSF data~~ received.

FPT_ISA.1.4/CK The TSF shall ensure that interpretation of the security attributes of the imported **cryptographic key** ~~TSF data~~ is as intended by the source of the **cryptographic key** ~~TSF data~~.

FPT_ISA.1.5/CK The TSF shall enforce the following rules when importing **cryptographic key** ~~TSF data~~ controlled under the SFP from outside the TOE:

(1) *The TSF imports the TSF data in certificates only after successful verification of the validity of the certificate including verification of digital signature of the issuer and validity time period.*

(2) *[assignment: additional importation control rules]*[105].

Application note 15: The operational environment is obligated to use trust center services for secure key management, cf. OE.SecManag.

FPT_TDC.1/CK Inter-TSF basic TSF data consistency – Key import

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TDC.1.1/CK The TSF shall provide the capability to consistently interpret *security attributes of* the *imported cryptographic keys* [106] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/CK The TSF shall use **the following rules**:

(1) *the TOE reports about conflicts between the Key identity of stored cryptographic keys and cryptographic keys to be imported,*

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

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

[105] [assignment: *importation control rules*]

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

(2) *the TOE does not change the security attributes Key identity, Key type, Key usage type and Key validity time period of the key being imported*[107]

when interpreting **the imported key data object** ~~TSF data from another trusted IT product~~.

FPT_ESA.1/CK Export of TSF data with security attributes – Cryptographic keys

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FMT_MTD.1 Management of TSF data or
FMT_MTD.3 Secure TSF data]
[FMT_MSA.1 Management of security attributes, or
FMT_MSA.4 Security attribute value inheritance]
FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_ESA.1.1/CK The TSF shall enforce the *Key Management SFP*[108] when exporting **cryptographic key** ~~TSF data~~, controlled under the SFP(s), outside of the TOE.

FPT_ESA.1.2/CK The TSF shall export the **cryptographic key** ~~TSF data~~ with the **cryptographic key's** ~~TSF data~~ associated security attributes.

FPT_ESA.1.3/CK The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported **cryptographic key** ~~TSF data~~.

FPT_ESA.1.4/CK The TSF shall enforce the following rules when **cryptographic key** ~~TSF data~~ is exported from the TOE: [assignment: *additional exportation control rules*].

Application note 16: There are no fixed rules for presentation of security attributes defined. The element FPT_ESA.1.4/CK must define rules expected in FPT_TDC.1 Inter-TSF basic TSF data consistency if inter-TSF key exchange is intended.

6.1.2 Data encryption

FCS_COP.1/ED Cryptographic operation – Data encryption and decryption

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/ED The TSF shall perform *data encryption and decryption*[109] in accordance with a specified cryptographic algorithm *symmetric data encryption according to AES-128 and [selection: AES-256, no other algorithm] in CBC and [selection: CRT, OFB, CFB, no other] mode* [110] and cryptographic key size *128 bits,* [selection: *256 bits, no other key size]*[111] that meet the following: *NIST-SP800-38A[NIST-SP800-38A], ISO 18033-3 [ISO/IEC 18033-3], ISO 10116 [ISO/IEC 10116]*[112].

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

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

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

[110] [assignment: *cryptographic algorithm*]

[111] [assignment: *cryptographic key sizes*]

[112] [assignment: *list of standards*]

Application note 17: Data encryption and decryption should be combined with data integrity mechanisms in Encrypt-then-MAC order, i. e. the MAC is calculated for the ciphertext and verified before decryption. The modes of operation should combine encryption with data integrity mechanisms to authenticated encryption, e. g. the Cipher Block Chaining Mode (CBC, cf. NIST SP800-38A) should be combined with CMAC (cf. FCS_COP.1/MAC) or HMAC (cf. FCS_COP.1/HMAC). For combination of symmetric encryption, decryption and data integrity mechanisms by means of CCM or GCM refer to the next section 6.1.3.

6.1.3 Hybrid encryption with MAC for user data

FCS_COP.1/HEM Cryptographic operation – Hybrid data encryption and MAC calculation

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/HEM The TSF shall perform *hybrid data encryption and MAC calculation*[113] in accordance with a specified cryptographic algorithm *asymmetric key encryption according to [selection: FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA, FCS_CKM.5/ECDHE], symmetric data encryption according to AES-128, [selection: AES-256, none other][FIPS197] in [selection: CBC[NIST-SP800-38A], CCM[NIST-SP800-38C], GCM[NIST-SP800-38D]] mode with [selection: CMAC[NIST-SP800-38B], GMAC[NIST-SP800-38D], HMAC[RFC2104]] calculation*[114] and cryptographic **symmetric** key sizes *128 bits,* [selection: *256 bits, no other key size]*[115] that meet the following: *the referenced standards above according to the chosen selection*[116].

Application note 18: Hybrid data encryption and MAC calculation is a self-contained security services of the TOE. The generation and encryption of the seed, derivation of encryption and MAC keys as well as the AES encryption and MAC calculation are only a steps of this service. The hybrid encryption is combined with MAC as data integrity mechanisms for the cipher text, i. e. encrypt-then-MAC creation for CMAC.

FCS_COP.1/HDM Cryptographic operation – Hybrid data decryption and MAC verification

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/HDM The TSF shall perform *hybrid MAC verification and data decryption*[117] in accordance with a specified cryptographic algorithm *asymmetric key decryption according to [selection: FCS_CKM.5/ECDHE, FCS_CKM.5/ECKA-EG, FCS_CKM.5/AES_RSA], verification of [selection: CMAC[NIST-SP800-38B], GCM[NIST-SP800-38D], HMAC[RFC2104]] and symmetric data decryption according to AES with [selection: AES-128, AES-256][FIPS197] in mode [selection: CBC[NIST-SP800-38A], CCM[NIST-SP800-38C], GMAC[NIST-SP800-38D]]*

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

[114] [assignment: *cryptographic algorithm*]

[115] [assignment: *cryptographic key sizes*]

[116] [assignment: *list of standards*]

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

[118] and cryptographic **symmetric** key sizes *128 bits, [selection: 256 bits, no other key size]*[119] that meet the following: *the referenced standards above according to the chosen selection*[120].

Application note 19: Hybrid data decryption and MAC verification is a self-contained security services of the TOE. The decryption of the seed and derivation of the encryption key and MAC keys as well as the AES decryption and MAC verification are only a steps of this service. The used symmetric key shall meet the AES CMAC or GMAC and the AES algorithm for decryption of the cipher text for MAC, e. g. verification-then-decrypt for CMAC.

6.1.4 Data integrity mechanisms

Cryptographic data integrity mechanisms comprise 2 types of mechanisms – symmetric message authentication code mechanisms and asymmetric digital signature mechanisms. A message authentication code mechanism comprises the generation of a MAC for original message, the verification of a given pair of message and MAC and symmetric key management. The MAC may be applied to plaintext without encryption but if combined with encryption it should be applied to ciphertexts in Encrypt-then-MAC order.

FCS_COP.1/MAC Cryptographic operation – MAC using AES

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/MAC The TSF shall perform *MAC generation and verification*[121] in accordance with a specified cryptographic algorithm *AES-128 and [selection: AES-256, none other][FIPS197] CMAC[NIST-SP800-38B] and [selection: GMAC[NIST-SP800-38D], no other]*[122] and cryptographic key sizes *128 bits [selection: 256 bits, no other key size]*[123] that meet the following: *the referenced standards above according to the chosen selection* [124].

Application note 20: The MAC may be applied to plaintext and cipher text. The AES-128 CMAC is mandatory. The selection of AES-256 and the key sizes shall correspond to each other.

FCS_COP.1/HMAC Cryptographic operation – HMAC

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/HMAC The TSF shall perform *HMAC generation and verification*[125] in accordance with a specified cryptographic algorithm *HMAC-SHA256 and [selection: HMAC-SHA-1, HMAC-*

[118] [assignment: *cryptographic algorithm*]

[119] [assignment: *cryptographic key sizes*]

[120] [assignment: *list of standards*]

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

[122] [assignment: *cryptographic algorithm*]

[123] [assignment: *cryptographic key sizes*]

[124] [assignment: *list of standards*]

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

SHA384, no other][126] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: *RFC2104 [RFC2104] , ISO 9797-2 [ISO/IEC 9797-2]*[127].

Application note 21: The cryptographic key is a random bit string generated by. FCS_RNG.1 or a referenced internal secret. The cryptographic key sizes assigned in FCS_COP.1/HMAC must be at least 128 bits.

FCS_COP.1/CDS-ECDSA Cryptographic operation – Creation of digital signatures ECDSA

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/CDS-ECDSA The TSF shall perform *signature-creation*[128] in accordance with a specified cryptographic algorithm *ECDSA with [selection: elliptic curves in the table 2]*[129] and cryptographic key sizes *[selection: key size in the table 2]*[130] that meet the following: *[selection: standards in the table 2]*[131].

Application note 22: The selection of elliptic curve and cryptographic key sizes shall correspond to each other, e. g. elliptic curve *brainpoolP256r1* and key size *256 bits*.

FCS_COP.1/VDS-ECDSA Cryptographic operation – Verification of digital signatures ECDSA

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/VDS-ECDSA The TSF shall perform *signature-verification*[132] in accordance with a specified cryptographic algorithm *ECDSA with [selection: elliptic curves in the table 2]*[133] and cryptographic key sizes *[selection: key size in the table 2]*[134] that meet the following: *[selection: standards in the table 2]*[135].

[126] [assignment: *cryptographic algorithm*]

[127] [assignment: *list of standards*]

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

[129] [assignment: c*ryptographic key generation algorithm*]

[130] [assignment: *cryptographic key sizes*]

[131] [assignment: *list of standards*]

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

[133] [assignment: c*ryptographic key generation algorithm*]

[134] [assignment: *cryptographic key sizes*]

[135] [assignment: *list of standards*]

FCS_COP.1/CDS-RSA Cryptographic operation – Creation of digital signatures RSA

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/CDS-RSA The TSF shall perform *signature-creation*[136] in accordance with a specified cryptographic algorithm *RSA and EMSA-PSS*[137] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: *ISO/IEC 14888-2 [ISO/IEC 14888-2], PKCS #1, v2.2 [PKCS#1]*[138].

Application note 23: The cryptographic key sizes assigned in FCS_CKM.1/RSA must be at least 2000 bits. Cryptographic key sizes of at least 3000 bits are recommended.

FCS_COP.1/VDS-RSA Cryptographic operation – Verification of digital signatures RSA

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/VDS-RSA The TSF shall perform *signature-verification*[139] in accordance with a specified cryptographic algorithm *RSA and EMSA-PSS*[140] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: *ISO/IEC 14888-2 [ISO/IEC 14888-2] , PKCS #1, v2.2 [PKCS#1]*[141].

Application note 24: The cryptographic key sizes assigned in FCS_CKM.1/RSA must be at least 2000 bits. Cryptographic key sizes of at least 3000 bits are recommended.

FDP_DAU.2/Sig Data Authentication with Identity of Guarantor - Signature

Hierarchical to: FDP_DAU.1 Basic Data Authentication

Dependencies: FIA_UID.1 Timing of identification

FDP_DAU.2.1/Sig The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of *user data*[142] **imported according to FDP_ITC.2/UD by means of [selection: *FCS_COP.1/CDS-RSA, FCS_COP.1/CDS-ECDSA*] and keys holding the security attributes Key identity assigned to the guarantor and Key usage type "Signature service"**.

FDP_DAU.2.2/Sig The TSF shall provide *external entities*[143] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

Application note 25: The TSF according to FDP_DAU.2/Sig is intended for a signature service for user data. The user data source shall select the security attributes *Key entity* of the guarantor and *Key usage type* "*Signature service*" of the cryptographic key for the signature service in the security attributes provided with the user data. The user data source subject shall meet the *Key access control attributes* for the signature-

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

[137] [assignment: *cryptographic algorithm*]

[138] [assignment: *list of standards*]

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

[140] [assignment: *cryptographic algorithm*]

[141] [assignment: *list of standards*]

[142] [assignment: *list of objects or information types*]

[143] [assignment: l*ist of subjects*]

creation operation. The verification of the evidence requires a certificate showing the identity of the key entity as user generated the evidence and the key usage type as digital signature.

6.1.5 Authentication and attestation of the TOE, trusted channel

FIA_API.1/PACE Authentication Proof of Identity – PACE authentication to Application component

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/PACE The TSF shall provide a *PACE in ICC role*[144] to prove the identity of the *TOE*[145] to an external entity **and establishing a trusted channel according to FTP_ITC.1 case 1 or 2**.

FIA_API.1/CA Authentication Proof of Identity – Chip authentication to user

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/CA The TSF shall provide a *Chip Authentication Version 2 according to [TR-03110] section 3.4*[146] to prove the identity of the *TOE*[147] to an external entity **and establishing a trusted channel according to FTP_ITC.1 case 3**.

FDP_DAU.2/Att Data Authentication with Identity of Guarantor - Attestation

Hierarchical to: FDP_DAU.1 Basic Data Authentication

Dependencies: FIA_UID.1 Timing of identification

FDP_DAU.2.1/Att The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of *attestation data*[148] **by means of** [**selection:** ***FCS_COP.1/CDS-RSA, FCS_COP.1/CDS-ECDSA, ECDAA according to [selection: [TPMLib,Part 1][FIDO-ECDAA]], [assignment: other cryptographic authentication mechanism]***] **and keys holding the security attributes Key identity assigned to the TOE sample and Key usage type "Attestation".**

FDP_DAU.2.2/Att The TSF shall provide *external entities*[149] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

Application note 26: The attestation data shall represent the TOE sample as genuine sample of the certified product. The attestation data may include the identifier of the certified product, the serial number of the device or a group of product samples as certified product, the hash value of the TSF implementation and some TSF data as result of self-test, or other data. It may be generated internally or may include internally generated and externally provided data. The assigned cryptographic mechanisms shall be appropriate for attestation meeting OSP.SecCryM, e. g. digital signature, a group signature or a direct anonymous attestation mechanism as used for Trusted Platform Modules ***[TPMLib,Part 1]*** or FIDO U2F Authenticators ***[FIDO-ECDAA]***.

[144] [assignment: *authentication mechanism*]

[145] [assignment: *object, authorized user or role*]

[146] [assignment: *authentication mechanism*]

[147] [assignment: *object, authorized user or role*]

[148] [assignment: *list of objects or information types*]

[149] [assignment: l*ist of subjects*]

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 TSF and another trusted IT product that is l~~ogically distinct from other communication channels~~ [**selection:** ***logically separated from other communication channels, using physical separated ports***] and provides assured identification of its end points [**selection:** ***Authentication of TOE and remote entity according to the case in table 4***] and protection of the channel data from modification or disclosure [**assignment:** ***according to the case in table 4***] **as required by** [**selection: c*ryptographic operation according to the case in table 4***].

FTP_ITC.1.2 The TSF shall permit *the remote trusted IT product*[150] **determined according to FMT_MOF.1.1 clause (3)** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *communication with entities defined according to FMT_MOF.1 clause (4)*[151].

Case	Authentication of TOE and remote entity	Key agreement	Protection of communication data	Cryptographic operation
1	FIA_API.1/PACE, FIA_UAU.5.1 (2)	FCS_CKM.1/PACE	modification	FCS_COP.1/TCM
2	FIA_API.1/PACE, FIA_UAU.5.1 (2)	FCS_CKM.1/PACE	modification	FCS_COP.1/TCM
			disclosure	FCS_COP.1/TCE
3	FIA_API.1/CA, FIA_UAU.5.1 (4) or (5), and (6)	FCS_CKM.1/TCAP	modification	FCS_COP.1/TCM
			disclosure	FCS_COP.1/TCE

Table 4: Operation in SFR for trusted channel

FCS_CKM.1/PACE Cryptographic key generation – Key agreement for trusted channel PACE

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/PACE The TSF shall generate cryptographic keys ***for MAC with for FCS_COP.1/TCM and if selected encryption keys for FCS_COP.1/TCE*** in accordance with a specified cryptographic key ~~generation~~ **agreement** algorithm *PACE with [selection: elliptic curves in table 2] and Generic Mapping in ICC role*[152] and specified cryptographic key sizes *[selection: 128 bits, 192 bits, 256 bits]*[153] that meet the following: *ICAO Doc9303*, *Part 11, section 4.4 [ICAO Doc9303]*[154].

Application note 27: PACE is used to authenticate the TOE and the application component, or TOE and human user using a terminal. It establishes a trusted channel with MAC integrity protection and if selected encryption.

[150] [selection: *the TSF, the remote trusted IT product*]

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

[152] [assignment: *cryptographic algorithm*]

[153] [assignment: *cryptographic key sizes*]

[154] [assignment: *list of standards*]

FCS_CKM.1/TCAP Cryptographic key generation – Key agreement by Terminal and Chip authentication protocols

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/TCAP The TSF shall generate cryptographic keys **for *encryption according to FCS_COP.1/TCE and MAC according to FCS_COP.1/TCM*** in accordance with a specified cryptographic key ~~generation~~ **agreement** algorithms *Terminal Authentication version 2 and Chip Authentication Version 2* [155] and specified cryptographic key sizes *[selection: 128 bits, 192 bits, 256 bits]*[156] that meet the following: *BSI TR-03110 [TR-03110], section 3.3 and 3.4*[157].

Application note 28: The terminal authentication protocol version 2 is used for authentication of the Application component according to FIA_UAU.5 and is a prerequisite for Chip Authentication Version 2.

FCS_COP.1/TCE Cryptographic operation - Encryption for trusted channel

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/TCE The TSF shall perform *encryption and decryption*[158] in accordance with a specified cryptographic algorithm *AES in [selection: CBC[NIST-SP800-38A], CCM[NIST-SP800-38C], GCM[NIST-SP800-38D]] mode*[159] and cryptographic key sizes [*selection: 128 bits, 192 bits, 256 bits]* [160] that meet the following: *[FIPS197]*[161].

FCS_COP.1/TCM Cryptographic operation - MAC for trusted channel

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/TCM The TSF shall perform *MAC calculation and MAC verification*[162] in accordance with a specified cryptographic algorithm *AES [selection: CMAC[NIST-SP800-38B], GMAC[NIST-SP800-38D]]*[163] and cryptographic key sizes *[selection: 128 bits, 192 bits, 256 bits]*[164] that meet the following: *[FIPS197]*[165].

[155] [assignment: *cryptographic algorithm*]

[156] [assignment: *cryptographic key sizes*]

[157] [assignment: *list of standards*]

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

[159] [assignment: *cryptographic algorithm*]

[160] [assignment: *cryptographic key sizes*]

[161] [assignment: *list of standards*]

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

[163] [assignment: *cryptographic algorithm*]

[164] [assignment: *cryptographic key sizes*]

[165] [assignment: *list of standards*]

6.1.6 User identification and authentication

FIA_ATD.1 User attribute definition – Identity based authentication

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) *Authentication reference data,*

(3) *Role*.

FMT_MTD.1/RAD Management of TSF data – Authentication reference data

Hierarchical to: No other components.

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

FMT_MTD.1.1/RAD The TSF shall restrict the ability to

(1) create[166] the *initial Authentication reference data of all authorized users*[167] to *[selection: Administrator, User Administrator]*[168]*,*

(2) *delete*[169] the *Authentication reference data of an authorized user*[170] to *[selection: Administrator, User Administrator]*[171],

(3) *modify*[172] the *Authentication reference data*[173] to *the corresponding authorized user*[174].

(4) *create*[175] the *permanently stored session key of trusted channel as Authentication reference data*[176] to *[selection: Administrator, User Administrator]*[177]

(5) *define*[178] the *time in range [assignment: time frame] after which the user security attribute Role is reset according to FMT_SAE.1*[179] *to [selection: Administrator, User Administrator]*[180]*,*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(6) ***define*[181] the *value [selection: Unidentified user, Unauthenticated user] to which the security attribute Role shall be reset according to FMT_SAE.1*[182] *to [selection: Administrator, User Administrator]*[183].**

Application note 29: The Administrator is responsible for user management. The Administrator install and revoke a user as known authorized user of the TSF as defined in clause (1). The Administrator may define additional authentication reference data as described in clause (3), i. e. the trusted channel combines initial authentication of communication endpoints (cf. FIA_UAU.5.1 clause (3) and (4)) with agreement of session keys used for authentication of exchanged messages (cf. FIA_UAU.5.1 clause (5)). The session keys may be permanently stored for the trusted communication with the known authorized entity. The user manages its own authentication reference data to prevent impersonation based of known authentication data (e.g. as addressed by FMT_MTD.3). The bullets (2) to (6) are refinements in order to avoid an iteration of component and therefore printed in bold.

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for *passwords*[184] **by enforcing change of initial passwords after first successful authentication of the user to different operational password**.

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~~ [**selection: Administrator, User Administrator**] configurable positive integer within [assignment: range of 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 [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].

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*[185].

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*[186].

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

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

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

[184] [assignment: list of TSF data]

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

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

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) *after successful identification of the user the attribute Role of the subject shall be changed from Unidentified user to Unauthenticated user;*

(2) *after successful authentication of the user for a selected role the attribute Role of the subject shall be changed from Unauthenticated User to that role;*

(3) *after successful re-authentication of the user for a selected role the attribute Role of the subject shall be changed to that role*[187].

FMT_SAE.1 Time-limited authorisation

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FPT_STM.1 Reliable time stamps

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for *Role*[188] to *[selection: Administrator, User Administrator]*[189].

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to *reset the Role to the value assigned according to FMT_MTD.1/RAD, clause (6)*[190] after the expiration time for the indicated security attribute has passed.

Application note 30: The TSF shall implement means to handle expiration time for the roles whithin a session (i.e. between power-up and power-down of the TOE) which may not necessarily meet the requirements for a reliable time stamp as required by FPT_STM.1. If the security target require FPT_STM.1 (e.g. if the PP-module “Time Stamp and Audit” claimed) this time stamp shall be used to meet FMT_SAE.1.

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.1*,

(2) *identification of the TOE to the user*,

(3) *[assignment: list of other TSF-mediated actions]*[191]

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~~ **the Unauthenticated User**.

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.1*,

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

[188] [assignment: *list of security attributes for which expiration is to be supported*]

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

[190] [assignment: *list of actions to be taken for each security attribute*]

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

(2) *authentication of the TOE to the user*,

(3) *identification of the user to the TOE and selection of [selection: a role, a set of role] for authentication,*

(4) *[assignment: list of other TSF mediated actions]*[192]

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 31: Clause (2) and (3) in FIA_UAU.1.1 allows mutual identification for mutual authentication, e. g. by exchange of certificates.

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

(1) *password authentication*,

(2) *PACE with Generic Mapping with TOE in ICC and user in PCD context with establishment of trusted channel according to FTP_ITC.1,*

(3) *certificate based Terminal Authentication Version 2 according to section 3.3 in [TR-03110] with the TOE in ICC and user in PCD context,*

(4) *Terminal Authentication Version 2 with the TOE in ICC context and user in PCD context modified by omitting the verification of the certificate chain,*

(5) *Chip Authentication Version 2 with establishment of trusted channel according to FTP_ITC.1,*

(6) *message authentication by MAC verification of received messages*[193]

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **rules**

(1) *password authentication shall be used for authentication of human users if enabled according to FMT_MOF.1.1, clause (1),*

(2) *PACE shall be used for authentication of human users using terminals with establishment of trusted channel according to FTP_ITC.1,*

(3) *PACE may be used for authentication of IT entities with establishment of trusted channel according to FTP_ITC.1,*

(4) *certificate based Terminal Authentication Version 2 may be used for authentication of users which certificate imported as TSF data,*

(5) *simplified version of Terminal Authentication Version 2 may be used for authentication of identified users associated with known user's public key,*

(6) *message authentication by MAC verification of received messages shall be used after initial authentication of remote entity according to clauses (2) or (3) for trusted channel according to FTP_ITC.1,*

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

[193] [assignment: *list of multiple authentication mechanisms*]

(7) *[assignment: additional rules]*[194].

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) *every message received from entities after establishing trusted channel according to FIA_UAU.5.1, clause (2), (3) or (6),*

(4) *[assignment: list of other conditions under which re-authentication is required]*[195].

6.1.7 Access control

FDP_ITC.2/UD Import of user data with security attributes – User data

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/UD The TSF shall enforce the *Cryptographic Operation SFP*[196] when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.2.3/UD 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/UD 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/UD The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

(1) *user data imported for encryption according to FCS_COP.1/ED shall be imported with Key identity of the key and the identification of the requested cryptographic operation,*

(2) *user data imported for encryption according to FCS_COP.1/HEM shall be imported with Key identity of the public key encryption key or key agreement method,*

(3) *user data imported for decryption according to FCS_COP.1/HDM shall be imported with Key identity of the asymmetric decryption key, encrypted seed and data integrity check sum,*

(4) *user data imported for digital signature creation shall be imported with the Key identity of the private signature key,*

(5) *user data imported for digital signature verification shall be imported with digital signature and Key identity of the public signature key*[197].

[194] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

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

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

Application note 32: Keys to be used for the cryptographic operation of the imported user data are identified by security attribute *Key identity*.

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]

FDP_ETC.2.1 The TSF shall enforce the *Cryptographic Operation SFP*[198] 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) *user data exported as ciphertext according to FCS_COP.1/HEM shall be exported with reference to key decryption key, encrypted data encryption key and data integrity check sum*,

(2) *user data exported as plaintext according to FCS_COP.1/HDM shall be exported only if the MAC verification confirmed the integrity of the ciphertext,*

(3) *user data exported as signed data according to FCS_COP.1/CDS-ECDSA or FCS_COP.1/CDS-RSA shall be exported with digital signature and Key identity of the used signature-creation key*[199].

Application note 33: The TOE imports data to be signed by CSP shall be imported with Key identity of the signature key and exports the signature. In case of internally generated data exported as signed data shall be exported with Key identity of the used key in order to enable identification of the corresponding signature-verification key. Note, the TOE may implement more than one signature-creation key for signing internally generated data.

FDP_ETC.1 Export of user data without security attributes

Hierarchical to: No other components.

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

FDP_ETC.1.1 The TSF shall enforce the *Cryptographic Operation SFP*[200] when exporting user data **as plaintext according to FCS_COP.1/HDM**, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the ~~user data~~ **successfully MAC verified and decrypted ciphertext as plaintext according to FCS_COP.1/HDM** without the user data's associated security attributes.

FDP_ACC.1/Oper Subset access control – Cryptographic operation

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/Oper The TSF shall enforce the *Cryptographic Operation SFP*[201] on

(1) *subjects: [selection: Administrator, Crypto-Officer], Key Owner, [assignment: other roles];*

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

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

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

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

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

(2) *objects: operational cryptographic keys*, *user data*;

(3) *operations:* c*ryptographic operation*[202]

FDP_ACF.1/Oper Security attribute based access control – Cryptographic operations

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*[203] to objects based on the following:

(1) *subjects: subjects with security attribute Role [selection: Administrator, Crypto-Officer], Key Owner, [assignment: other roles]*;

(2) *objects:*

(a) c*ryptographic keys with security attributes: Identity of the key, Key entity, Key type, Key usage type, Key access control attributes, Key validity time period*;

(b) *user data*[204].

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 [selection: Administrator, Crypto-Officer] role is allowed to perform cryptographic operation on cryptographic keys in accordance with their security attributes.*

(2) *Subject Key Owner is allowed to perform cryptographic operation on user data with cryptographic keys in accordance with the security attribute Key entity, Key type, Key usage type, Key access control attributes and Key validity time period*;

(3) *[assignment: other rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]*[205].

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

(1) *subjects with security attribute Role are allowed to perform cryptographic operation on user data and cryptographic keys with security attributes as shown in the rows of table 5.*

(2) [assignment: *additional 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 following additional rules:

(1) *No subject is allowed to use cryptographic keys by cryptographic operation other than those identified in the security attributes Key usage type and the Key access control attributes*;

(2) *No subject is allowed to decrypt ciphertext according to FCS_COP.1/HDM if MAC verification fails.*

[202] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

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

[204] [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*]

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

(3) *[assignment: additional rules, based on security attributes, that explicitly deny access of subjects to objects].*[206]

Access control rules for cryptographic operation:

Security attribute Role of the subject	Security attribute of the cryptographic key	Cryptographic operation referenced by SFR allowed for the subject on user data with the cryptographic key
[selection: Administrator, Crypto-Officer, Key Owner]	*Key type: symmetric* *Key usage type: Key wrap* *Key validity time period:*	*FCS_COP.1/KW*
[selection: Administrator, Crypto-Officer, Key Owner]	*Key type: symmetric* *Key usage type: Key unwrap* *Key validity time period:*	*FCS_COP.1/KU*
(any authenticated user)	*Key type: public* *Key usage type: ECKA-EG* *Key validity time period: as in certificate*	*FCS_COP.1/HEM,* *FCS_CKM.1/ECKA-EG*
Key Owner	*Key type: private* *Key usage type: ECKA-EG* *Key validity time period:*	*FCS_COP.1/HDM* *FCS_CKM.5/ECKA-EG*
(any authenticated user)	*Key type: public* *Key usage type: RSA_ENC* *Key validity time period: as in certificate*	*FCS_COP.1/HEM* *FCS_CKM.1/AES_RSA*
Key Owner	*Key type: private* *Key usage type: RSA_ENC* *Key validity time period: as in certificate*	*FCS_COP.1/HDM* *FCS_CKM.5/AES_RSA*
Key Owner	*Key type: private* *Key usage type: DS-ECDSA* *Key validity time period:*	*FCS_COP.1/CDS-ECDSA*
(any authenticated user)	*Key type: public* *Key usage type: DS-ECDSA* *Key validity time period:*	*FCS_COP.1/VDS-ECDSA*
Key Owner	*Key type: private* *Key usage type: DS-RSA* *Key validity time period:*	*FCS_COP.1/CDS-RSA*
(any authenticated user)	*Key type: public* *Key usage type: DS-RSA* *Key validity time period:*	*FCS_COP.1/VDS-RSA*

Table 5: Security attributes and access control

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

6.1.8 Security Management

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)*,

(2) *management of Authentication reference data (FMT_MTD.1/RAD),*

(3) *management of security attributes of cryptographic keys (FMT_MSA.1/KM, FMT_MSA.2, FMT_MSA.3/KM,*

(4) *[assignment: additional list of security management functions to be provided by the TSF]*[207].

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles: *Unidentified User, Unauthenticated User, Key Owner, Application component, [selection: Administrator, Crypto-Officer, User Administrator, Update Agent] [selection: [assignment: other roles], no other roles]*[208].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application note 34: The ST may select the general role *Administrator* or more detailed administrator roles as supported by the TOE.

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 *security attributes*

(1) *Key identity,*

(2) *Key type,*

(3) *Key usage type,*

(4) *[assignment: additional security attributes]*[209].

The cryptographic keys shall have

(1) Key identity uniquely identifying the key among all keys implemented in the TOE,

(2) exactly one Key type as secret key, private key, public key,

(3) exactly one Key usage type identifying exactly one cryptographic mechanism the key can be used for.

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

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

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

FMT_MOF.1 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 The TSF shall restrict the ability to

(1) *enable*[210] the function~~s~~ *password authentication according to FIA_UAU.5.1, clause (1)*[211] to *[selection: Administrator, User Administrator]*[212].

(2) *disable*[213] the function~~s~~ *password authentication according to FIA_UAU.5.1, clause (1)*[214] to *[selection: Administrator, User Administrator]*[215],

(3) *determine the behaviour of*[216] the functions *trusted channel according to FDP_ITC.1.2*[217] by defining the remote trusted IT products permitted to initiate communication via the trusted channel to *[selection: Administrator, User Administrator]*[218],

(4) *determine the behaviour of*[219] the functions *trusted channel according to FDP_ITC.1.3*[220] by defining the entities for which the TSF shall enforce communication via the trusted channel to *[selection: Administrator, User Administrator]*[221].

Application note 35: The refinements of FMT_MOF.1.1 in bullets (2) to (4) are made in order to avoid iteration of the component. In case of client-server architecture the applications using the TOE and supporting cryptographically protected trusted channel belong to the entities for which the TSF shall enforce trusted channel according to FDP_ITC.1, cf. FMT_MOF.1.1 in bullet (4).

6.1.9 Protection of the TSF

FDP_SDC.1 Stored data confidentiality

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SDC.1.1 The TSF shall ensure the confidentiality of the information of the ~~user~~ data while it is stored in the [assignment: *memory area*] **by encryption according to *FCS_COP.1/SDE***.

Application note 36: The memory encryption does not distinguish between user data and TSF data when encrypting memory areas. The refinement extends the SFR to any data in the assigned memory area, which may contain user data, TSF data, software and firmware as TSF implementation.

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

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

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

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

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

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

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

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

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

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

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

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

FCS_CKM.1/SDEK Cryptographic key generation – Stored data encryption 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/SDEK The TSF shall generate cryptographic **stored data encryption** key~~s~~ in accordance with a specified cryptographic key generation algorithm [assignment: c*ryptographic key generation algorithm*] **using random bit generation according to FCS_RNG.1** and specified cryptographic key sizes *[assignment: cryptographic key sizes]* that meet the following: *[assignment: list of standards]*.

FCS_COP.1/SDE Cryptographic operation – Stored data encryption

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/SDE The TSF shall perform *stored data encryption and decryption*[222] 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 standards*].

Application note 37: The generation of data encryption keys according to FCS_CKM.1/SDEK, the encryption and the decryption according to FCS_COP.1/SDE are only used for stored data in the memory areas assigned in FDP_SDC.1.1. They are not a security services of the TOE to the user. If cryptographic algorithm does not provide integrity protection for stored user data the stored data should contain redundancy for detection of data manipulation, e. g. in order to meet FPT_TST.1.2 and FPT_TST.1.3.

FRU_FLT.2 Limited fault tolerance

Hierarchical to: FRU_FLT.1 Degraded fault tolerance

Dependencies: FPT_FLS.1 Failure with preservation of secure state.

FRU_FLT.2.1 The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: *exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1)*[223].

Refinement: The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" defined above.

Application note 38: Environmental conditions include but are not limited to power supply, clock, and other external signals (e. g. reset signal) necessary for the TOE operation.

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:

(1) *self test fails*,

(2) *exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur*,

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

[223] [assignment: *list of types of failures*]

(3) *manipulation and physical probing is detected and secure state is reached as response (FPT_PHP.3).*

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

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 *during initial start-up, at the request of the authorised user and after power-on*[224] to demonstrate the correct operation of [assignment: *parts of TSF]*[225].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of *TSF data*[226].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of *TSF* ***implementation***[227].

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist

(1) *physical probing and manipulation and (2) perturbation and environmental stress*[228] to

the *(1) TSF implementation and (2) the TSF*[229]

by responding automatically such that the SFRs are always enforced.

Refinement: The TSF will implement appropriate mechanisms to continuously counter physical probing and manipulation. In case of platform architecture the resistance to physical attacks shall include the secure execution environment for and the communication with the application component running on the TOE.

Application note 39: “Automatic response” of protection against physical probing and manipulation means (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time. Perturbation and environmental stress to the TSF is relevant when the TOE is running. Note, exploration of information leakage from the TOE like side channels is addressed as bypassability of TSF by the security architecture (cf. ADV_ARC.1.1D and ADV_ARC.1.5C) and shall consider these physical attack scenarios.

6.1.10 Import and verification of Update Code Package

The TOE imports Update Code Package as user data objects with security attributes according to FDP_ITC.2/UCP, verifies the authenticity of the received Update Code Package according to FCS_COP.1/VDSUCP, decrypts authentic Update Code Package according to FCS_COP.1/DecUCP.

[224] [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]*]

[225] [selection: *[assignment: parts of TSF], the TSF]*

[226] [selection: *[assignment: parts of TSF data], TSF data*]

[227] [selection: *[assignment: parts of TSF], TSF*]

[228] [assignment: *physical tampering scenarios*]

[229] [assignment: *list of TSF devices/elements*]

FDP_ITC.2/UCP Import of user data with security attributes – Update Code Package

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/UCP The TSF shall enforce the *Update SFP*[230] when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.2.3/UCP 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/UCP 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/UCP The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

(1) *storing of encrypted Update Code Package only after successful verification of authenticity according to FCS_COP.1/VDSUCP,*

(2) *decrypts authentic Update Code Package according to FCS_COP.1/DecUCP*[231].

FPT_TDC.1/UCP Inter-TSF basic TSF data consistency

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TDC.1.1/UCP The TSF shall provide the capability to consistently interpret *security attributes Issuer and Version Number*[232] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/UCP The TSF shall use **the following rules**:

(1) t*he Issuer must be identified and known,*

(2) *the Version Number must be identified*

when interpreting the TSF data from another trusted IT product.

FCS_COP.1/VDSUCP Cryptographic operation – Verification of digital signature of the Issuer

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/VDSUCP The TSF shall perform *verification of the digital signature of the authorized Issuer*[233] 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 standards*].

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

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

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

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

Application note 40: The authorized *Issuer* is identified in the security attribute of the received Update Code Package and the public key of the authorized *Issuer* shall be known as TSF data before receiving the Update Code Package. Only public key of the authorized Issuer shall be used for verification of the digital signature of the Update Code Package.

FCS_COP.1/DecUCP Cryptographic operation – Decryption of authentic Update Code Package

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/DecUCP The TSF shall perform *decryption of authentic encrypted Update Code Package*[234] 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 standards*].

FDP_ACC.1/UCP Subset access control – Update code Package

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/UCP The TSF shall enforce the *Update SFP*[235] on

(1) *subjects: [selection: Administrator, Update Agent];*

(2) *objects: Update Code Package*;

(3) *operations: import, store*[236].

FDP_ACF.1/UCP Security attribute based access control – Import Update Code Package

Hierarchical to: No other components.

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

FDP_ACF.1.1/UCP The TSF shall enforce the *Update SFP*[237] to objects based on the following:

(1) *subjects: [selection: Administrator, Update Agent];*

(2) *objects: Update Code Package with security attributes Issuer and Version Number*[238].

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

(1) *[selection: Administrator, Update Agent] is allowed to import Update Code Package according to FDP_ITC.2/UCP.*

(2) *[selection: Administrator, Update Agent] is allowed to store Update Code Package if*

(a) authenticity is successful verified according to FCS_COP.1/VDSUCP and decrypted according to FCS_COP.1/DecUCP

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

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

[236] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

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

[238] [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*]

(b) the Version Number of the Update Code Package is equal or higher than the Version Number of the TSF.[239]

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

FDP_RIP.1/UCP Subset residual information protection

Hierarchical to: No other components

Dependencies: No dependencies.

FDP_RIP.1.1/UCP The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource* ***after unsuccessful verification of the digital signature of the Issuer according to FCS_COP.1/VDSUCP***[240] the following objects: *received Update Code Package* [241].

6.2 Security assurance requirements

The PP requires the TOE to be evaluated to EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.

6.3 Security requirements rationale

6.3.1 Dependency rationale

This chapter demonstrates that each dependency of the security requirements is either satisfied, or justifies the dependency not being satisfied.

Note, the column SFR components showing the concrete SFR satisfying the dependencies are typical use cases. It does not exclude that the SFR in the first column may solve dependencies of other SFR as well. E. g. the SFR FCS_CKM.1 defines requirements for ECC key generation and the ECC key pair may be directly used for ECDSA digital signatures according to FCS_COP.1/CDS-RSA and FCS_COP.1/VDS-RSA but also for encryption and decryption of the AES key in FCS_COP.1/HEM and FCS_COP.1/HDM.

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

[240] [selection: *allocation of the resource to, deallocation of the resource from*]

[241] [assignment: *list of objects*]

SFR	Dependencies of the SFR	SFR components
FCS_CKM.1/AES	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/ED FCS_CKM.4
FCS_CKM.1/AES_RSA	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/HEM with FCS_CKM.1/AES_RSA, FCS_CKM.4
FCS_CKM.1/ECC	FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/CDS-ECDS, FCS_COP.1/VDS-ECDS, FCS_CKM.4
FCS_CKM.1/ECKA-EG	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/HEM with FCS_CKM.1/ECKA-EG, FCS_CKM.4
FCS_CKM.1/PACE	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/TCE, FCS_COP.1/TCM, FCS_CKM.4
FCS_CKM.1/RSA	FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/CDS-RSA, FCS_COP.1/VDS-RSA FCS_CKM.4
FCS_CKM.1/SDEK	FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/SDE, FCS_CKM.4
FCS_CKM.1/TCAP	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/TCE, FCS_COP.1/TCM, FCS_CKM.4
FCS_CKM.4	[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.1/ECC, FCS_CKM.1/RSA, FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA, FCS_CKM.1/TCAP, FCS_CKM.1/PACE
FCS_CKM.5/AES	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/ED FCS_CKM.4
FCS_CKM.5/AES_RSA	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/HDM with FCS_CKM.5/AES_RSA, FCS_CKM.4
FCS_CKM.5/ECC	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/CDS-ECDS, FCS_COP.1/VDS-ECDS, FCS_CKM.4
FCS_CKM.5/ECDHE	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/HEM with FCS_CKM.5/ECDHE, FCS_CKM.4
FCS_CKM.5/ECKA-EG	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/HDM with FCS_CKM.5/ECKA-EG, FCS_CKM.4

SFR	Dependencies of the SFR	SFR components
FCS_COP.1/CDS-ECDSA	[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/ECC, FCS_CKM.4
FCS_COP.1/CDS-RSA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/RSA, FCS_CKM.4
FCS_COP.1/DecUCP	[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	Import of UCP decryption key as TSF data with confidentiality protection FPT_TCT.1/CK and FCS_COP.1/KU, FCS_CKM.4
FCS_COP.1/ED	[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/AES, FCS_CKM.4
FCS_COP.1/Hash	[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	Hash functions do not use keys
FCS_COP.1/HDM	[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.5/ECKA-EG, FCS_CKM.5/AES_RSA, FCS_CKM.5/ECDHE (note deterministic FCS_CKM.5 play the role of randomized FCS_CKM.1) FCS_CKM.4
FCS_COP.1/HEM	[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/ECKA-EG, FCS_CKM.1/AES_RSA, FCS_CKM.5/ECDHE, FCS_CKM.1/AES_RSA FCS_CKM.4
FCS_COP.1/HMAC	[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_RNG.1 generates random strings as HMAC keys FCS_CKM.4

SFR	Dependencies of the SFR	SFR components
FCS_COP.1/KU	[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/AES FCS_CKM.4
FCS_COP.1/KW	[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/AES FCS_CKM.4
FCS_COP.1/MAC	[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_CKM.1/AES, FCS_CKM.4
FCS_COP.1/SDE	[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/SDEK, FCS_CKM.4
FCS_COP.1/TCE	[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/TCAP, FCS_CKM.1/PACE, FCS_CKM.4
FCS_COP.1/TCM	[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/TCAP, FCS_CKM.1/PACE, FCS_CKM.4
FCS_COP.1/VDS-ECDSA	[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	FPT_ISA.1/Cert (note keys are TSF data), FCS_CKM.4
FCS_COP.1/VDS-RSA	[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	FPT_ISA.1/Cert (note keys are TSF data), FCS_CKM.4

SFR	Dependencies of the SFR	SFR components
FCS_COP.1/VDSUCP	[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	Import of signature verification key of UCP Issuer as TSF data FPT_ISA.1/Cert, FPT_TIT.1/Cert, FCS_CKM.4
FCS_RNG.1	No dependencies	
FDP_ACC.1/KM	FDP_ACF.1 Security attribute based access control	Dependency on FDP_ACF.1 is not fulfilled. Access control to key management functions are specified by FMT_MTD.1/KM because cryptographic keys are TSF data.
FDP_ACC.1/Oper	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/Oper
FDP_ACC.1/UCP	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/UCP
FDP_ACF.1/Oper	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/Oper, FMT_MSA.3/KM
FDP_ACF.1/UCP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/UCP, FMT_MSA.3 is not included, because the security attributes of UCP are imported according to FDP_ITC.2/UCP without default values.
FDP_DAU.2/Att	FIA_UID.1 Timing of identification	FIA_UID.1
FDP_DAU.2/Sig	FIA_UID.1 Timing of identification	FIA_UID.1
FDP_ETC.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/Oper
FDP_ETC.2	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/Oper
FDP_ITC.2/UCP	[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.1/UCP trusted communication is provided by FCS_COP.1/VDSUCP and FCS_COP.1/DecUCP, FPT_TDC.1/UCP
FDP_ITC.2/UD	[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.1/Oper trusted communication is provided by FCS_COP.1/HDM and FCS_COP.1/VDS-*, FPT_TDC.1/CK because import of user data is intended for cryptographic operation with key

SFR	Dependencies of the SFR	SFR components
FDP_RIP.1/UCP	No dependencies	
FDP_SDC.1	No dependencies	
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_API.1/CA	No dependencies	
FIA_API.1/PACE	No dependencies	
FIA_ATD.1	No dependencies	
FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.1
FIA_UAU.5	No dependencies	
FIA_UAU.6	No dependencies	
FIA_UID.1	No dependencies	
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MSA.1/KM	[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.1/KM, FDP_ACC.1/Oper, FMT_SMF.1, FMT_SMR.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.1/KM, FDP_ACC.1/Oper, FMT_MSA.1/KM, FMT_SMR.1
FMT_MSA.3/KM	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/KM, FMT_SMR.1
FMT_MTD.1/KM	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/RAD	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/RK	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MTD.3	FMT_MTD.1 Management of TSF data	FMT_MTD.1/RAD
FMT_SAE.1	FMT_SMR.1 Security roles, FPT_STM.1 Reliable time stamps	FMT_SMR.1, dependency on FPT_STM.1 is not fulfilled, cf. to the application note to FMT_STM.1
FMT_SMF.1	No dependencies	

SFR	Dependencies of the SFR	SFR components
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.1
FPT_ESA.1/CK	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/KM, FMT_MTD.1/KM FMT_MSA.1/KM FPT_TDC.1/CK
FPT_FLS.1	No dependencies	
FPT_ISA.1/Cert	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/KM, FMT_MTD.1/RK, FMT_MSA.1/KM FPT_TDC.1/Cert
FPT_ISA.1/CK	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/KM, FMT_MTD.1/RK, FMT_MTD.1/KM FMT_MSA.1/KM FPT_TDC.1/Cert
FPT_PHP.3	No dependencies	
FPT_TCT.1/CK	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]	FDP_ACC.1/KM, FMT_MTD.1/RK, FMT_MTD.1/KM
FPT_TDC.1/Cert	No dependencies	
FPT_TDC.1/CK	No dependencies	
FPT_TDC.1/UCP	No dependencies	
FPT_TIT.1/Cert	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]	FDP_ACC.1/KM, FMT_MTD.1/RK
FPT_TIT.1/CK	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]	FDP_ACC.1/KM, FMT_MTD.1/KM
FPT_TST.1	No dependencies	

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

Table 6: Dependency rationale

6.3.2 Security functional requirements rationale

The table 7 trace each SFR back to the security objectives for the TOE.

	O.I&A	O.AuthentTOE	O.Enc	O.DataAuth	O.RBGS	O.Tchann	O.AccCtrl	O.SecMan	O.PhysProt	O.TST	O.SecUpCP
FCS_CKM.1/AES			x	x				x			
FCS_CKM.1/AES_RSA			x	x				x			
FCS_CKM.1/ECC		x	x	x				x			
FCS_CKM.1/ECKA-EG			x	x				x			
FCS_CKM.1/PACE		x				x		x			
FCS_CKM.1/RSA		x	x	x				x			
FCS_CKM.1/SDEK									x		
FCS_CKM.1/TCAP		x				x		x			
FCS_CKM.4			x	x				x			
FCS_CKM.5/AES			x	x				x			
FCS_CKM.5/AES_RSA			x	x				x			
FCS_CKM.5/ECC			x	x				x			
FCS_CKM.5/ECDHE			x	x				x			
FCS_CKM.5/ECKA-EG			x	x				x			
FCS_COP.1/CDS-ECDSA		x		x							
FCS_COP.1/CDS-RSA		x		x							
FCS_COP.1/DecUCP											x
FCS_COP.1/ED			x					x			
FCS_COP.1/Hash				x				x			
FCS_COP.1/HDM			x	x							
FCS_COP.1/HEM			x	x							
FCS_COP.1/HMAC		x		x							
FCS_COP.1/KU								x			
FCS_COP.1/KW								x			
FCS_COP.1/MAC				x							

	O.I&A	O.AuthentTOE	O.Enc	O.DataAuth	O.RBGS	O.Tchann	O.AccCtrl	O.SecMan	O.PhysProt	O.TST	O.SecUpCP
FCS_COP.1/SDE									x		
FCS_COP.1/TCE						x					
FCS_COP.1/TCM						x					
FCS_COP.1/VDS-ECDSA				x							
FCS_COP.1/VDS-RSA				x							
FCS_COP.1/VDSUCP											x
FCS_RNG.1					x			x			
FDP_ACC.1/KM							x	x			
FDP_ACC.1/Oper							x				
FDP_ACC.1/UCP											x
FDP_ACF.1/Oper							x				
FDP_ACF.1/UCP											x
FDP_DAU.2/Att		x									
FDP_DAU.2/Sig				x							
FDP_ETC.1				x							
FDP_ETC.2			x	x							
FDP_ITC.2/UCP											x
FDP_ITC.2/UD			x	x							
FDP_RIP.1/UCP											x
FDP_SDC.1									x		
FIA_AFL.1	x										
FIA_API.1/CA	x	x				x					
FIA_API.1/PACE	x	x				x					
FIA_ATD.1	x						x	x			
FIA_UAU.1	x										
FIA_UAU.5	x					x					
FIA_UAU.6	x										
FIA_UID.1	x										
FIA_USB.1	x										
FMT_MOF.1	x					x					
FMT_MSA.1/KM			x	x		x	x	x			
FMT_MSA.2							x	x			
FMT_MSA.3/KM							x	x			x

	O.I&A	O.AuthentTOE	O.Enc	O.DataAuth	O.RBGS	O.Tchann	O.AccCtrl	O.SecMan	O.PhysProt	O.TST	O.SecUpCP
FMT_MTD.1/KM								x			
FMT_MTD.1/RAD	x										
FMT_MTD.1/RK	x		x	x				x			
FMT_MTD.3	x										
FMT_SAE.1	x										
FMT_SMF.1								x			
FMT_SMR.1	x							x			
FPT_ESA.1/CK								x			
FPT_FLS.1									x	x	
FPT_ISA.1/Cert	x			x				x			x
FPT_ISA.1/CK								x			
FPT_PHP.3									x		
FPT_TCT.1/CK								x			x
FPT_TDC.1/CK			x	x				x			
FPT_TDC.1/Cert	x		x	x				x			
FPT_TDC.1/UCP											x
FPT_TIT.1/Cert	x			x				x			x
FPT_TIT.1/CK								x			
FPT_TST.1										x	
FRU_FLT.2									x		
FTP_ITC.1						x					

Table 7: Security functional requirement rationale

The following part of the chapter demonstrate that the SFRs meet all security objectives for the TOE.
The security objective for the TOE O.I&A “Identification and authentication of users” is met by the following SFR:

- The SFR FIA_ATD.1 lists the security attributes *Identity*, *Authentication reference data* and *Role* belonging to individual users and the SFR FMT_SMR.1 defines the security roles maintained by TSF.
- The SFR FIA_USB.1 requires the TSF to associate the user security attributes *Identity* and *Role* with subjects acting on the behalf of that user.
- The SFR FIA_UID.1 defines the TSF-mediated actions allowed on behalf of Unidentified User.
- The SFR FIA_UAU.1 defines the TSF-mediated actions allowed on behalf of Unauthenticated User.
- The SFR FIA_UAU.5 requires the TSF lists the authentication mechanisms and the rules for their application.
- The SFR FIA_API.1/CA and FIA_API.1/PACE require the TSF to authenticate external entities using Chip Authentication and PACE to communication endpoints of trusted channels.

- The SFR FIA_UAU.6 requires the TSF to request re-authentication of users under the listed conditions.
- The SFR FMT_MOF.1 requires the TSF to enable and disable of human user authentication.
- The SFR FMT_MTD.1/RAD and The SFR FMT_MTD.1/RK defines the management function of and the access limitation to authentication mechanisms and their TSF data including the root public keys.
- The SFR FMT_MTD.3 enforce secure values for password mechanisms.
- The SFR FMT_SAE.1 requires the TSF to limit the validity of user authentication and reset the security attribute Role to a values defined by an administrator according to FMT_MTD.1/RAD.
- The SFR FIA_AFL.1 requires the TSF to detect and react on failed authentication attempts.
- The SFR FPT_ISA.1/Cert and FPT_TIT.1/Cert require the TSF to import certificates integrity protected and with their security attributes including those for entity authentication.
- The SFR FPT_TDC.1/Cert requires the TSF to interpret the certificates correctly.

The security objective for the TOE O.AuthentTOE “Authentication of the TOE to external entities” is met by the following SFR:

- The SFR FCS_CKM.1/ECC, FCS_CKM.1/RSA require the TSF to generate TOE authentication keys and SFR FCS_CKM.1/PACE and FCS_CKM.1/TCAP require the TSF to agree keys for authentication of the TOE to external entities.
- The SFR FCS_COP.1/CDS-ECDSA and FCS_COP.1/CDS-RSA require the TSF to generate digital signatures for authentication of the TOE to external entities.
- SFR FCS_COP.1/HMAC requires the TSF to generate HMAC for authentication of the TOE to external entities.
- The SFR FIA_API.1/CA, and FIA_API.1/PACE require the TSF to authenticate themselves using Chip Authentication, and PACE to communication endpoints of trusted channels.
- The SFR FDP_DAU.2/Att requires the TSF to generate evidence that can be used as a guarantee of the validity of attestation data to external entities.

The security objective for the TOE O.Enc “Confidentiality of user data by means of encryption and decryption” is met by the following SFR:

- The SFR FCS_CKM.1/ECC and FCS_CKM.1/RSA require (long term) key generation for the encryption and decryption security service of the TSF.
- The SFR FCS_CKM.1/AES, FCS_CKM.1/AES_RSA, FCS_CKM.5/ECDHE, and FCS_CKM.1/ECKA-EG, require key generation and FCS_CKM.5/AES, FCS_CKM.5/AES_RSA, FCS_CKM.5/ECKA-EG and FCS_CKM.5/ECC require key derivation for encryption and decryption security service of the TSF. Note the keys must be generated or agreed with the appropriate key type for encryption respectively for decryption or in case of symmetric cryptographic mechanisms for both according to FMT_MSA.1/KM.
- The FCS_COP.1/ED requires encryption and decryption as cryptographic operations for the encryption and decryption security service of the TSF.
- The FCS_COP.1/HDM requires hybrid decryption and the SFR FCS_COP.1/HEM requires hybrid encryption and decryption as cryptographic operations for the encryption and decryption security service of the TSF.
- The SFR FDP_ETC.2 require the TSF to export encrypted user data with reference to the key and data integrity checksums for decryption and FDP_ITC.2/UD require import of encrypted user data with reference to decryption key and data integrity checksums for decryption.
- The SFR FCS_CKM.4 requires the TSF to implement secure key destruction.

- The SFR FMT_MTD.1/RK requires the TSF management of root keys for key hierarchy known to the TSF if used for encryption.
- The SFR FPT_TDC.1/Cert requires the TSF to interpret consistently the security attributes of certificates (including those used for encryption and decryption).
- The SFR FPT_TDC.1/CK requires the TSF to interpret consistently the security attributes of keys (including those used for encryption and decryption).

The security objective for the TOE O.DataAuth "Data authentication by cryptographic mechanisms" is met by the following SFR:

- The SFR FCS_CKM.1/ECC and FCS_CKM.1/RSA require (long term) key generation for the signature security service of the TSF. The SFR FCS_CKM.1/AES, FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA require key generation and FCS_CKM.5/AES_RSA, FCS_CKM.5/ECDHE, FCS_CKM.5/ECC, FCS_CKM.5/ECKA-EG key derivation for MAC generation and verification. Note the keys must be generated or agreed with the appropriate key type for signature-creation, signature-verification or, in case of symmetric cryptographic mechanisms for data authentication according to FMT_MSA.1/KM.
- The SFR FDP_ETC.2 require the TSF to export signed data with and signature and public key reference for signature verification and FDP_ITC.2/UD import of signed data with signature and public key reference for signature verification. The SFR FDP_ETC.1 require the TSF to export successfully MAC verified and decrypted ciphertext as plaintext according to FCS_COP.1/HDM without the user data's associated security attributes:
- The SFR FCS_COP.1/Hash requires the TSF to implement cryptographic primitive hash function used for HMAC, cf. FCS_COP.1/HMAC, digital signature creation, cf. FCS_COP.1/CDS-*and digital signature verification, cf. FCS_COP.1/VDS-*.
- The FCS_COP.1/CDS-ECDSA and FCS_COP.1/CDS-RSA require asymmetric cryptographic mechanisms for signature-creation.
- The SFR FCS_COP.1/VDS-ECDSA and FCS_VDS/RSA require asymmetric cryptographic mechanisms for signature-verification.
- The SFR for keyed hash FCS_COP.1/HMAC and block cipher based MAC FCS_COP.1/MAC require the TSF to provide symmetric data integrity mechanisms.
- The SFR FCS_COP.1/HEM requires hybrid MAC calculation and FCS_COP.1/HDM requires hybrid MAC verification for the ciphertext as security service of the TSF.
- The SFR FPT_ISA.1/Cert requires import of certificates with security attributes and integrity protection according to FPT_TIT.1/Cert.
- The SFR FCS_CKM.4 requires the TSF to implement secure key destruction.
- The SFR FPT_TDC.1/Cert requires the TSF to interpret consistently the security attributes in certificates (including those used for data authentication).
- The SFR FPT_TDC.1/CK requires the TSF to interpret consistently the security attributes keys (including those used for data authentication).

The security objective for the TOE O.RBGS "Random bit generation service" is met directly by the SFR FCS_RNG.1 as providing random bits for the service to the user.

The security objective for the TOE O.TChann "Trusted channel" is met by the following SFR:

- The SFR FTP_ITC.1 requires different types of trusted channel depending on the capability of the other endpoint. The cases are defined in table 4. The remote entity and the TOE may use mutual authentication and key agreement by means of PACE according to FCS_CKM.1/PACE, shall provide integrity protection according to FCS_COP.1/TCM and may support confidentiality of the communication data according to

FCS_COP.1/TCE. The cases 3 requires support of trusted channel with mutual authentication by FIA_API.1/CA, FIA_UAU.5, key agreement TCAP according to FCS_CKM.1/TCAP, encryption and MAC data authentication.

- The TOE authenticate themselves according to FIA_API.1/PACE in case of PACE. It authenticates themselves according to FIA_API.1/CA in case of TCAP as Proximity Integrated Circuit Card (PICC).
- The SFR FMT_MOF.1 limits the configuration of the trusted channel according to FTP_ITC.1.3 to an administrator.
- The SFR FMT_MSA.1/KM describe the requirements for management of key security attributes for these mechanisms.

The security objective for the TOE O.AccCtrl "Access control" is met by the following SFR:

- The SFR FIA_ATD.1 defines the security attributes of individual users including *Role* which is used for access control according to FDP_ACF.1/Oper.
- The SFR FDP_ACC.1/Oper describes the subset access control for the *Cryptographic Operation* SFP.
- The SFR FDP_ACF.1/Oper defines the access control rules of the *Cryptographic Operation* SFP.
- The *Cryptographic Operation* SFP is defined by means of security attributes managed according to the SFR FMT_MSA.1/KM, FMT_MSA.2 and FMT_MSA.3/KM.

The security objective for the TOE O.SecMan "Security management" is met by the following SFR:

- The SFR FIA_ATD.1 defines the security attributes of individual users including *Role* which is used to enforce the *Key Management SFP*.
- The SFR FDP_ACC.1/KM defines subjects, objects and operations of the *Key Management SFP*.
- The SFR FMT_SMF.1 lists the security management functions provided by the TSF.
- The SFR FMT_SMR.1 lists the security role supported by the TOE especially the administrator and – if supported - Crypto-Officer responsible for key management.
- The SFR FCS_CKM.1/AES, FCS_CKM.1/ECC, FCS_CKM.1/ECKA-EG. FCS_CKM.1/PACE, FCS_CKM.1/RSA, FCS_CKM.1/AES_RSA, FCS_CKM.1/TCAP require the TSF to implement key generation function according to the assigned standards.
- The SFR FCS_CKM.5/ECDHE require the TSF to implement key agreement function according to the assigned standards.
- The SFR FCS_CKM.5/AES and FCS_CKM.5/ECKA-EG require the TSF to implement key derivation function according to the assigned standards.
- The SFR FCS_CKM.1/AES_RSA and FCS_CKM.5/AES_RSA require the TSF to implement AES session key generation function with RSA key encryption respective RSA key decryption and AES key derivation according to the assigned standards.
- The SFR FCS_RNG.1 requires the TSF to implement a random number generator for key generation, key agreement functions and cryptographic operations.
- The SFR FCS_COP.1/ED requires the TSF to provide encryption and decryption according to AES which may be used for key management.
- The SFR FCS_COP.1/Hash requires the TSF to implement cryptographic primitive hash function for key derivation, cf. FCS_CKM.5.
- The SFR FPT_ISA.1/CK requires import and FPT_ESA.1/CK the export of cryptographic keys with security attributes and protection of confidentiality according to SFR FPT_TCT.1/CK and integrity protection according to FPT_TIT.1/CK.

- The SFR FPT_ISA.1/Cert requires import of certificates with security attributes and integrity protection according to FPT_TIT.1/Cert.
- The SFR FPT_TDC.1/Cert requires consistent interpretation of certificate's content. The SFR FPT_TDC.1/CK requires consistent interpretation of security attributes imported with the key.
- The SFR FCS_COP.1/KW and FCS_COP.1/KU require the TSF key wrapping and unwrapping for key management.
- The SFR FCS_CKM.4 requires the TSF to implement secure key destruction.
- The SFR FMT_MSA.1/KM and FMT_MSA3/KM limit the setting of default values and specification of alternative initial values for security attributes of cryptographic keys to administrators. The SFR FMT_MSA.1/KM prevents modification or deletion of security attributes of keys.
- FMT_MSA.2 enforce secure values for security attributes.
- The SFR FMT_MTD.1/KM and FMT_MTD.1/RK restricts the management of cryptographic keys espacially the import of root public keys to specifically authorized users.

TOE O.TST "Self-test" is directly met by the SFR FPT_TST.1 and FPT_FLS.1. The TSF shall preserve a secure state if self test fails.

The security objective for the TOE O.PhysProt "Physical protection" is met by the directly met by the SFR FPT_PHP.3. The memory encryption required by FDP_SDC.1, FCS_CKM.1/SDEK and FCS_COP.1/SDE provides additional protection against compromise of information in the stored data. The SFR FPT_FLS.1 requires the TSF to preserve a secure state if exposure to operating conditions occurs which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) or manipulation and physical probing is detected and secure state is reached as response.

The security objective for the TOE O.SecUpCP "Secure import of Update Code Package" is met by the following SFR:

- The SFR FDP_ACC.1/UCP and FDP_ACF.1/UCP requires the TSF to provide access control to enforce SFP *Update*. Note the verification of the authenticity of UCP and decryption of authentic UCP are performed under control of the TSF.
- The SFR FCS_COP.1/VDSUCP requires the verification of digital signature of the Issuer and FCS_COP.1/DecUCP requires decryption of authentic of UCP.
- The SFR FDP_ITC.2/UCP requires the TSF to import UCP as user data with security attributes if the authenticity of UCP is successful verified.
- The SFR FPT_TDC.1/UCP requires the TSF to import consistently the security attributes of the UCP.
- The SFR FMT_MSA.3 requires to provide restrictive initial security attributes to enforce the SFP *Update*.
- The SFR FDP_RIP.1/UCP requires the TSF to remove the received UCP after unsuccessful verification of its authenticity.
- The UCP signature verification key may be updated according to FPT_ISA.1/Cert with integrity protection according to FPT_TIT.1/Cert.
- The UCP decryption key may be updated with confidentiality protection according to FPT_TCT.1/CK with FCS_COP.1/KU.

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 a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

The augmentation 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.

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 and the strength of the corresponding protection measures shall be balanced with respect to the assumed moderate attack potential. Therefore ALC_DVS.2 was augmented.

7 Reference Documentation

ANSI-X9.63 ANSI-X9.63, Key Agreement and Key Transport Using Elliptic Curve Cryptography, , 2011

CC1 Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1, Revision 5, April 2017

CC2 Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017

CC3 Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

FIDO-ECDAA FIDO Alliance, Alliance Proposed Standard FIDO ECDAA Algorithm, https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-ecdaa-algorithm-v1.2-ps-20170411.html, 11 April 2017

FIPS PUB 180-4 NIST, Secure Hash, Standard (SHS), , 2012

FIPS PUB 186-4 NIST, Digital Signature Standard (DSS), , 2013

FIPS197 Federal Information Processing Standards Publication 197 (FIPS PUB 197), Advanced Encryption Standard (AES), , 2001

ICAO Doc9303 ICAO: Machine Readable Travel Documents, ICAO Doc9303, Part 11: Security Mechanisms for MRTDSs, seventh edition, 2015

ISO/IEC 10116 ISO/IEC 10116 Information Technology - Security techniques, Modes of operation for an n-bit block cipher, , 2017

ISO/IEC 14888-2 ISO/IEC 14888-2 Information technology – Security techniques, Digital signatures with appendix – Part 2: Integer factorization based mechanisms, , 2008

ISO/IEC 18033-3 ISO/IEC 18033-3 Information technology - Security techniques, Encryption algorithms - Part 3: Block ciphers, , 2010

ISO/IEC 9797-2 ISO/IEC 9797-2 Information Technology - Security techniques, Message Authentication Codes (MACs), Part 2: Mechanisms using a dedicated hash-function, , 2011

JILGuidance Joint Interpretation Library, Guidance for smartcard evaluation, Version 2.0, February 2010

NIST-SP800-38A NIST, SP800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques, ,

NIST-SP800-38B NIST, SP800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, , May 2005

NIST-SP800-38C NIST, Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, , May 2004

NIST-SP800-38D NIST, SP800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, , November 2007

NIST-SP800-38F NIST , SP800-38F Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, , 2012

NIST-SP800-56C NIST, Recommendation for Key Derivation through Extraction-then-Expansion, Special Publication SP800-56C, , November 2011

PKCS#1 PKCS #1 v2.2: RSA Cryptographic Standard, https://www.emc.com/emc-plus/rsa-labs/pkcs/files/h11300-wp-pkcs-1v2-2-rsa-cryptography-standard.pdf, , 27.10.2012

RFC2104 RFC2104, HMAC: Keyed-Hashing for Message Authentication, ,

RFC5639 RFC5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, http://www.ietf.org/rfc/rfc5639.txt, 2010

RFC5903 RFC5903, Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2 , ,

RFC6954 RFC6954, Using the Elliptic Curve Cryptography (ECC) Brainpool Curves for the Internet Key Exchange Protocol Version 2 (IKEv2), ,

SOGIS IT-TDs SOG-IS, Recognition Agreement Management Committee Policies and Procedures, SOGIS IT-Technical Domains, , February 2011

TPMLib,Part 1 Trusted Platform Module Library, Part 1: Architecture, Family “2.0”, Level 00, Revision 01.38, September 29, 2016

TR-03110	BSI, Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2 - Protocols for electronic IDentification, Authentication and trust Services (eIDAS), Version 2.21, 2016
TR-03111	BSI, Elliptic Curve Cryptography, BSI Technical Guideline TR-03111, Version 2.1, 1.6.2018

Keywords and Abbreviations

Term	Description
authentication reference data	data used by the TOE to verify the authentication attempt of a user
authentication verification data	data used by the user to authenticate themselves to the TOE
authenticity	the property that ensures that the identity of a subject or resource is the one claimed (cf. ISO/IEC 7498-2:1989)
cluster	a system of TOE samples initialized by an administrator and communication through trusted channels in order to manage known users and to share the cryptographic keys
cryptographic key	a variable parameter which is used in a cryptographic algorithm or protocol
data integrity	the property that data has not been altered or destroyed in an unauthorized manner (cf. ISO/IEC 7498-2:1989)
firmware	executable code that is stored in hardware and cannot be dynamically written or modified during execution while operating on a non-modifiable or limited execution platform, cf. ISO/IEC 19790
hardware	physical equipment or comprises the physical components used to process programs and data or to protect physically the processing components, cf. ISO/IEC 19790
Issuer of update code package	Trusted authority issuing an update code package (UCP) and holding the signature private key for signing the UCP and corresponding to the public key implemented in the TOE for verification of the UCP. The issuer is typically the TOE manufacturer. The issuer of an UCP is identified by the security attribute Issuer of the UCP.
private key	confidential key used for asymmetric cryptographic mechanisms like decryption of cipher text, signature-creation or authentication proof, where it is difficult for the adversary to derive the confidential private key from the known public key
public key	public known used for asymmetric cryptographic mechanisms like encryption of cipher text, signature-verification or authentication verification, where it is difficult for the adversary to derive the confidential private key from the known public key
secret key	key of symmetric cryptographic mechanisms, using two identical keys with the same secret value or two different values, where one may be easy calculated from the other one, for complementary operations like encryption / decryption, signature-creation / signature-verification, or authentication proof / authentication verification.

secure channel	a trusted channel which is physically protected and logical separated communication channel between the TOE and the user, or is protected by means of cryptographic mechanisms
software	executable code that is stored on erasable media which can be dynamically written and modified during execution while operating on a modifiable execution platform, cf. ISO/IEC 19790
trusted channel	a means by which a TSF and another trusted IT product can communicate with necessary confidence (cf. CC part 1[CC1], paragraph 97)
update code package	code if implemented changing the TOE implementation at the end of the TOE life time

Table 8: Glossary

Acronym	Term
A.xxx	Assumption
CC	Common Criteria
CSP	cryptographic service provider
ECC	Elliptic curve cryptography
HMAC	Keyed-Hash Message Authentication Code
KDF	Key derivation function
MAC	Message Authentication Code
n. a.	Not applicable
O.xxx	Security objective for the TOE
OE.xxx	Security objective for the TOE environment
OSP.xxx	Organisational security policy
PACE	Password Authenticated Connection Establishment
PKI	Public key infrastructure
PP	Protection profile
SAR	Security assurance requirements
SFR	Security functional requirement
T.xxx	Threat
TOE	Target of Evaluation
TSF	TOE security functionality
UCP	update code package

Table 9: Abbreviations