Federal Office
for Information Security

Common Criteria Protection Profile
Cryptographic Service Provider
BSI-CC-PP-x-y

Document history

Version	Date	Editor	Description
0.1	24.5.2017	km	Document structure
0.2	9.6.2017	km	First draft
0.3	30.6.2017	km	Draft before work on Application-PPs starts
0.4	18.8.2017	km	First intermediate draft aligned with draft of PP CRSMA
0.5	31.8.2017	km	Draft aligned with draft of PP CRSMA, time stamp service and SFR rationale
0.6	22.9.2017	km	Update of full version considering light PP CSPL
0.7	30.10.2017	km	Alignment PP CSP, PP CSPL, PP CRSDA and PP DSCA, SFR for hash function, HMAC, MAC and secret sharing added
0.7.1	6.11.2017	km	Draft for distribution
0.7.2	20.11.2017	Km	DSA key generation, signature generation and signature verification added for TLS cipher suites (necessary?),
0.7.3	30.12.2017	km	FCS_TLS.1: TLS client signature verification only, FCS_TLS_.3: TLS server signature generation only, CBC-MAC removed
0.7.4	29.1.2018	km	Update due to BSI comments
0.7.5	1.2.2018	km	Attestation added (OSP.SecService, OSP.TC, O.AuthTOE, FDP_DAU.2)
0.7.6	23.2.2018	km	Random number generation as security service added in OSP.SecService, O.RBG, FCS_RBG_EXT.6 and rationales.
0.7.7	08.03.2018	km	Due to BSI comments all references to CBC-MAC, PRF, DSA, FCS:CKM.2 removed
0.7.8	13.3.2018	km	Enhanced audit
0.7.9	21.3.2018	km	Time stamp functionality, FIA_API.1/PWT removed
0.8.0	15.5.2018	km	Reset of user attribute Role in FIA_USB.1 and FMT_MTD.1/RAD
0.8.1	13.6.2018	km	Update due to comments, reset of user attribute Role in FMT_SAE.1 (FIA_USB.1, clause 4 removed), consideration of detailed administrator roles, selection and export of auditable events, encryption of stored data in more general form, AES-196 removed, literature reference [21] changed.
0.8.2	19.6.2018	km	Update due to BSI TR-03111, V.2.1
0.8.3	17.07.18	Ae	FCS_CKM.1/DHE removed
0.8.4	02.08.18	ae	Änderungen nach Kommentaren
0.8.5	07.09.18	km	Update due to BSI comments, life cycle description added, clarification of protection of the communication between TOE and application, update of O.PhysProt, OE.Sec.Comm, FMT_MSA.2, FPT_PHP.3, application note to FMT_MOF.1, terminology table and references

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Phone: +49 22899 9582-
E-Mail: @bsi.bund.de
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:	0.8.1
Registration:	BSI-CC-PP-xxxx
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 cryptographic and non-cryptographic security services for users and 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.

The TSF provides a non-cryptographic real time service.

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 [1], 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,

– protected exchange of TSF data in the cluster of CSP samples.

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

The TOE samples may set up a cluster of CSP samples for scalability of performance and availability of security services, cf. [30].

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

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.

The TOE samples may be organized in a cluster in order to manage known users and to share the cryptographic keys. One CSP sample in the cluster is selected as master, the other CSP samples in the cluster are slaves. The Master-CSP communicates with Slave-CSP through trusted channel keeping the confidentiality and integrity of the security attributes of the known users and of the cryptographic keys with their security attributes.

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. [36]). 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 [37].

The TOE sample shall be delivered with attestation keys managed by the TOE manufacturer or another attestation authority in order to enable the attestation as genuine sample of the certified product, cf. chapter 6.1.5. The TOE shall implement authentication keys used for prove of its own identity and managed by the TOE manufacturer, a TOE vendor, a trust center or the TOE owner 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 6.1.12.

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 [2] (security functional components) is CC Part 2 extended.

Conformance of this PP with respect to CC Part 3 [3] (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

The dependencies of AVA_VAN.5 and ALC_DVS.2 are fulfilled by the components of EAL4.

The chapter 5 defines the extended families

- Random bit generation (FCS_RBG_EXT) with extended components FCS_RBG_EXT.1 to FCS_RBG_EXT.6,
- Authentication Proof of Identity (FIA_API) with extended component FIA_API.1,
- Inter-TSF TSF data confidentiality transfer protection (FPT_TCT) with extended component FPT_TCT.1,
- Inter-TSF TSF data integrity transfer protection (FPT_TIT) with extended component FPT_TIT.1,
- TSF data import with security attributes (FPT_ISA) with extended component FPT_ISA.1,
- TSF data export with security attributes (FPT_ESA) with extended component FPT_ESA.1,
- Stored data confidentiality (FDP_SDC) with extended component FDP_SDC.1,

and the extended component

- Cryptographic key derivation (FCS_CKM.5) of the family FCS_CKM.

following the structure of families and components for security functional requirements (SFR) defined in CC part 2.

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,

– *remote entity* exchanging user data and TSF data with the TOE over insecure media,

– *cluster-CSP* being another TOE sample in a cluster with the TOE.

The TOE communicates with

– human user through a secure channel,

– application component through a secure channel,

– remote entities over a trusted channel,

– cluster-CSP in encrypted and integrity protected form.

The subjects as active entities in the TOE perform operations on objects and obtaining 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 reference authentication 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.
  - *Auditor*: role that is allowed to configure the audit functionality, review audit data and export audit trails.
  - *Update Agent*: authorized user for installation of imported and verified as authentic 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).

– *Cluster-CSP*: another TOE sample in a cluster with the TOE with security attribute *Master-CSP* or *Slave-CSP*. This role is bound to the communication through the trusted channel between cluster CSPs established by the administrator.

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.1 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 time stamp service (cf. FDP_DAU.2/TS) by key usage type "*TimeStamp*", 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
  - *Clustering*: distribution of the key in a cluster of TOE samples (i. e. export by TOE as Master-CSP, Import by TOE as Slave-CSP) is allowed or forbidden,
  - *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.

UCP have at least the security attributes

- *Issuer* of the Update Code Package,
- *Version Number* of the Update Code Package.

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. The TSF implementation shall be robust against perturbation.

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

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 according to OSP Secure cryptographic mechanisms only and assigned to the secure cryptographic mechanisms they are intended to be used with and to the entities authorized for their use.

OSP.Audit Audit for key management and cryptographic operations
Security auditing of key management, cryptographic operation, key management and cryptographic operation involves recognizing, recording, storing, and analysing information related to activities controlled by the TSF. The security auditing provides evidence to make users responsible for actions they are authorized for and to protect users against unwarranted accusation. The administrator is allowed to define auditable events.

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.Cluster Cluster of TOE samples
The administrator establishes a cluster of multiple TOE samples that share Authentication Data Records and cryptographic keys for scalability of performance and availability of security services.

OSP.Update Authorized Update Code Packages
Update Code Packages are delivered to the TOE 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 use of authentic Update Code Package to an authorized user.

3.4 Assumptions

A.Cluster Cluster control
The cluster of TOE samples is set up by the administrator by selection of one TOE sample as Master-CSP and transfer of TSF data as security attributes of known users and cryptographic keys with security attributes from the Master-CSP to all other TOE samples of the cluster acting as Slave-CSPs.

A.SecComm Secure communication
Remote entities support trusted channel using cryptographic mechanisms. In case of client-server architecture the

operational environment protects the confidentiality and integrity of communication data by means of a trusted channel using cryptographic mechanisms or a secure channel provided by 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 cryptorgaphic 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 outside the cluster. 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.TimeServices Time services
The TOE provide real time service and time stamp service for the user.

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 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.Audit Audit for cryptographic TSF
The TSF provides security auditing of key management and cryptographic operation by recognizing, recording and storing of selected of auditable events by audit records related to activities controlled by the TSF. The TOE provides the administrator with managements functionality to define the auditable events.

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 download and authorized use of Update Code Package
The TSF verifies the authenticity of received encrypted Update Code Package and decrypts authentic Update Code Package and before it stores the Update Code Package. The TOE allows only authorized administrators in Update Agents role to install Update Code Package for creation of a new CSP.

O.Cluster Cluster
The TSF supports cluster of TOE samples as CSP with distribution of Authentication Data Records and cryptographic keys from Master-CSP to Slave-CSPs through a trusted channel keeping the confidentiality and integrity of the security attributes of the known users and of the cryptographic keys with their security attributes.

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.Audit Review and availability of audit records
The administrator shall ensure the regular audit review and the availability of exported audit records.

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.Cluster Control of the cluster
The administrator builds a cluster only of trustworthy samples of the TOE.

OE.SUCP Signed Update Code Packages
The issuer delivers secure Update Code Packages to the TOE 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.

Security objectives 4

	T.DataCompr	T.DataMani	T.Masqu	T.ServAcc	T.PhysAttack	T.FaUpD	OSP.SecCryM	OSP.SecService	OSP.KeyMan	OSP.Audit	OSP.Cluster	OSP.TC	OSP.Update	A.Cluster	A.SecComm
O.AccCtrl				x											
O.Audit										x					
O.AuthentTOE								x							
O.Cluster											x				
O.DataAuth		x					x	x							
O.Enc	x						x	x							
O.I&A			x	x			x			x					
O.PhysProt					x										
O.RBGS								x							
O.SecMan			x				x		x			x			
O.SecUpCP						x							x		
O.Tchann	x	x	x	x				x							
O.TimeService								x							
OE.AppComp	x	x		x								x			
OE.Audit										x					
OE.Cluster											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.SecChann.

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 outside the cluster 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 over local physically protected communication channel between the TOE. 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.SecChann.

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 reuqiring 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 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 performs self-tests and to enter a secure state if self-test fails or attacks are detected.

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 download and authorized use 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. The TOE allows only authorized administrators to install Update Code Package for creation of a new CSP.

– 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” reuqires 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” and O.TimeServices “Time services” requiring TSF to provide cryptographic and non-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 O.SecMan “Security management”.

The organizational security policy OSP.Audit “Audit for key management and cryptographic operations” is implemented by security objectives for the TOE and the operational environment

– O.I&A requiring identification and authentication of user as prerequisite for audit records and making user responsible for their actions.

– O.Audit requiring security auditing of key management and selected cryptographic operation by recognizing, recording and storing of selected of auditable events by audit records related to activities controlled by the TSF.

– OE.Audit requiring regular audit review and ensures the availability of exported audit records for review.

The organizational security policy OSP.Cluster “Cluster of TOE samples” is implemented by security objectives for the TOE and the operational environment:

– O.Cluster requiring support for cluster of TOE samples as CSPs with distribution of Authentication Data Records and cryptographic keys from Master-CSP to Slave-CSPs through a trusted channel keeping the confidentiality and integrity of the security attributes of the known users and of the cryptographic keys with their security attributes.

– OE.Cluster requiring administrator to build a cluster only of trustworthy samples of the TOE.

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 assumption A.Cluster is directly ensured by OE.Cluster.

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

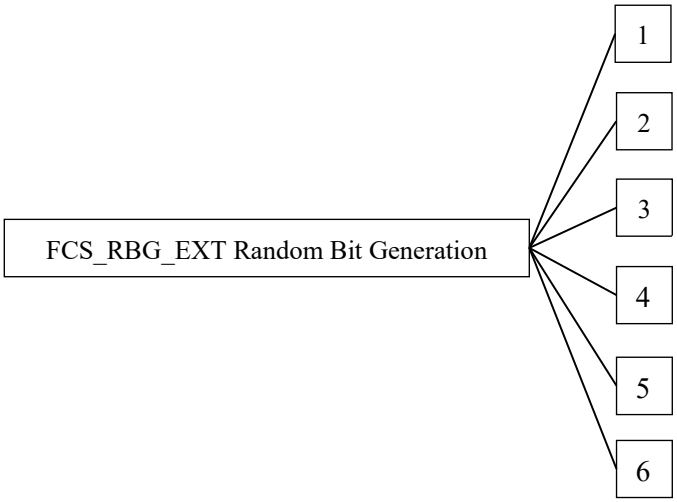
5.1 Random bit generation (FCS_RBG_EXT)

This section describes the functional requirements for the generation of random numbers, which may be used as secrets for cryptographic purposes or authentication. The IT security functional requirements for a TOE are defined in an additional family Random bit generation (FCS_RBG_EXT) of the Class FCS (Cryptographic support).[1]

Family Behaviour

Components in this family address the requirements for random bit/number generation.

Component levelling



FCS_RBG_EXT.1 Random Bit Generation requires random bit generation to be performed in accordance with selected standards.

FCS_RBG_EXT.2 Random Bit Generation seeded by an external (outside the TOE) entropy source.

FCS_RBG_EXT.3 Random Bit Generation seeded by a TSF entropy source.

FCS_RBG_EXT.4 Random Bit Generation seeded by multiple TSF entropy sources.

FCS_RBG_EXT.5 Combining entropy sources – combining multiple entropy sources (multiple internal sources, internal and external).

FCS_RBG_EXT.6 Random Bit Generation Service requires random numbers to be supplied over an external interface as a service to other entities.

Management: FCS_RBG_EXT.1, FCS_RBG_EXT.2, FCS_RBG_EXT.3, FCS_RBG_EXT.4, FCS_RBG_EXT.5, FCS_RBG_EXT.6

There are no management activities foreseen

Audit: FCS_RBG_EXT.1, FCS_RBG_EXT.2

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

1 The family definition follows the draft for CC part 2 SFR components.

a) Minimal: failure of the randomization process

FCS_RBG_EXT.1 Random Bit Generation (RBG)

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.2 and/or FCS_RBG_EXT.3
(No rationale is acceptable for not satisfying one of these dependencies)

FCS_RBG_EXT.1.1 The TSF shall perform deterministic random bit generation services using [assignment: *RBG algorithm*] in accordance with [assignment: *list of standards*] after initialization with a seed.

FCS_RBG_EXT.1.2 The TSF shall use an [selection: *TOE internal, TOE external*] noise source for initialized seeding.

FCS_RBG_EXT.1.3 The TSF shall [selection: *uninstantiate and instantiate, reseed*] the RBG in accordance with [assignment: *list of standards], [selection: on demand, on the condition: [assignment: condition], after [assignment: time], none*].

FCS_RBG_EXT.2 Random Bit Generation (External Seeding)

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1

FCS_RBG_EXT.2.1 The TSF shall be able to accept a minimum input of [assignment: *minimum input length greater than zero*] from an external interface for the purpose of seed generation.

FCS_RBG_EXT.3 Random Bit Generation (Internal Seeding Single Source)

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1

FCS_RBG_EXT.3.1 The TSF shall seed the RBG using a single [selection: *TSF software-based noise source, TSF hardware-based noise source*] with a minimum of [assignment: *number of bits*] bits of min-entropy.

FCS_RBG_EXT.4 Random Bit Generation (Internal Seeding multiple sources)

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1, FCS_RBG_EXT.3

FCS_RBG_EXT.4.1 The TSF shall be able to seed the RBG using [selection: *[assignment: number] TSF software-based noise source(s), [assignment: number] TSF hardware-based noise source(s)*].

FCS_RBG_EXT.5 Random Bit Generation (Combining entropy sources)

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1, FCS_RBG_EXT.2 and/or FCS_RBG_EXT.3

FCS_RBG_EXT.5.1 The TSF shall [assignment: *combining operation*] [selection: *TSF entropy source(s), TOE external entropy source(s)*] to create the entropy input into the derivation function as defined in [assignment: l*ist of standards*], resulting in a minimum of [assignment: *number of bits*] bits of min-entropy.

FCS_RBG_EXT.6 Random Bit Generation (RBG Services)

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1, [FCS_RBG_EXT.2 or FCS_RBG_EXT.3]

Extended component definition 5

FCS_RBG_EXT.6.1 The TSF shall provide a [selection: *hardware, software, [assignment: other interface type]*] interface to make the RBG output, as specified in FCS_RBG_EXT.1, available as a service to entities outside of the TOE.

5.2 Cryptographic key derivation (FCS_CKM.5)

This chapter describes functional requirements 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.

FCS_CKM.5 Requires the TOE to provide key derivation.

Management: FCS_CKM.5

There are no management activities foreseen.

Audit: FCS_CKM.5

There are no actions defined to be auditable.

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

Management: The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: There are no actions defined to be auditable

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.

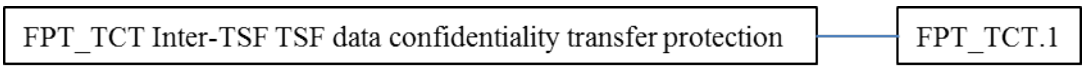
5.4 Inter-TSF TSF data confidentiality transfer protection (FPT_TCT)

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.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 actions defined to be auditable.

FPT_TCT.1 TSF data confidentiality transfer protection

Hierarchical to: No other components.

Dependencies: [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.

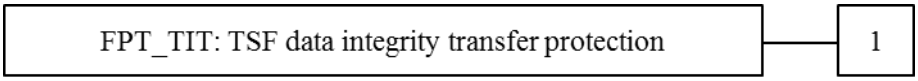
5.5 Inter-TSF TSF data integrity transfer protection (FPT_TIT)

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:



Extended component definition 5

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 actions defined to be auditable.

FPT_TIT.1 TSF data integrity transfer protection

Hierarchical to:	No other components.
Dependencies:	[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.

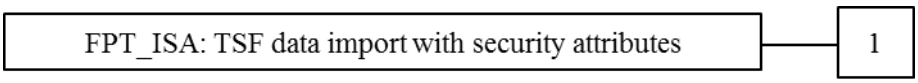
5.6 TSF data import with security attributes (FPT_ISA)

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 actions defined to be auditable.

FPT_ISA.1 Import of TSF data with security attributes

Hierarchical to:	No other components.
Dependencies:	[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*].

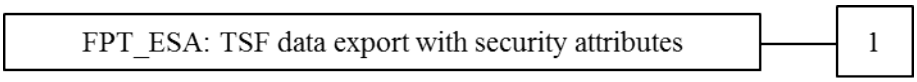
5.7 TSF data export with security attributes (FPT_ESA)

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 actions defined to be auditable.

FPT_ESA.1 Export of TSF data with security attributes

Hierarchical to: No other components.

Dependencies: [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.

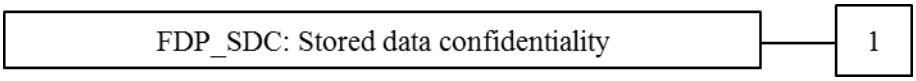
The family “Stored data confidentiality (FDP_SDC)” is specified as follows.

Extended component definition 5

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 actions defined to be auditable.

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 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/KED-RSA, and the symmetric encryption of the data with the data encryption key and data integrity mechanism with message authentication code (MAC) calculation for the cipher text. The receiver reconstructs the data encryption key and the MAC key, cf. FCS_CKM.5/ECKA-EG, FCS_CKM.5/KED-RSA, 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 SFR in chapter 6.1.9 defines the *Clustering SFP* with Administrators (and its refinements Crypto-Officer and User Administrator if supported by the TOE), Application Component, Master-CSP and Slave-CSP (as subjects), Authentication Data Records and cryptographic keys (as objects) and export and import (as operations, cf. to extended components SFR FPT_ESA.1/CL and FPT_ISA.1/CL).

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 [15], TR-03111, section 4.1.3 [10]*
brainpoolP384r1,	*384 bits*	*RFC5639 [15], TR-03111, section 4.1.3 [10]*
brainpoolP512r1	*512 bits*	*RFC5639 [15], TR-03111, section 4.1.3 [10]*
Curve P-256	*256 bits*	*FIPS PUB 186-4 B.4 and D.1.2.3 [16]*
Curve P-384	*384 bits*	*FIPS PUB 186-4 B.4 and D.1.2.4 [16]*
Curve P-521	*512 bits*	*FIPS PUB 186-4 B.4 and D.1.2.5 [16]*

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

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*[2] to restrict the ability to

(1) *change_default*[3] the security attributes *Identity of the key, Key entity of the key, Key type, Key usage type, Key access control rules, Key validity time period*[4] to *[selection: Administrator, Crypto-Officer]*[5],

(2) *modify or delete*[6] the security attributes *Identity of the key, Key entity, Key type, Key usage type, Key validity time period of an existing key*[7] to *none*[8],

(3) *modify independent on key usage*[9] *the security attributes Key usage counter of an existing key*[10] *to none*[11].

(4) *modify*[12] the security attribute *Key access control rules of an existing key*[13] to *[selection: Administrator, Crypto-Officer]*[14],

(5) *query*[15] the security attribute *Key type, Key usage type, Key access control rules, Key validity time period and Key usage counter of an identified key*[16] to *[selection: Administrator, Crypto-Officer, Key Owner]*[17].

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

2 [assignment: *access control SFP, information flow control SFP*]
3 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
4 [assignment: *list of security attributes*]
5 [assignment: *the authorised identified roles*]
6 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
7 [assignment: *list of security attributes*]
8 [assignment: *the authorised identified roles*]
9 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
10 [assignment: *list of security attributes*]
11 [assignment: *the authorised identified roles*]
12 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
13 [assignment: *list of security attributes*]
14 [assignment: *the authorised identified roles*]
15 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
16 [assignment: *list of security attributes*]
17 [assignment: *the authorised identified roles*]

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 and Cryptographic Operation SFP*[18] to provide *restrictive*[19] 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*]**[20] 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*[21] the *cryptographic keys*[22] to **[selection: *Administrator, Crypto-Officer, Key Owner*]**[23],

(2) *import according to FPT_TCT.1/CK, FPT_TIT.1/CK and FPT_ISA.1/CK*[24] the *cryptographic keys*[25] to *[selection: Administrator, Crypto-Officer*][26]**,**

(3) *export according to FPT_TCT.1/CK, FPT_TIT.1/CK and FPT_ESA.1/CK*[27] the *cryptographic keys*[28] to *[selection: Administrator, Crypto-Officer, Key Owner*][29] *if security attribute of the key allows export,***

(4) *delete according to FCS_CKM.4*[30] the *cryptographic keys*[31] to *[selection: Administrator, Crypto-Officer, Key Owner]*[32].

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

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

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

20 [assignment: *the authorised identified roles*]

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

22 [assignment: *list of TSF data*]

23 [assignment: *the authorised identified roles*]

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

25 [assignment: *list of TSF data*]

26 [assignment: *the authorised identified roles*]

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

28 [assignment: *list of TSF data*]

29 [assignment: *the authorised identified roles*]

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

31 [assignment: *list of TSF data*]

32 [assignment: *the authorised identified roles*]

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
MT_MSA.2 Secure security attributes

FCS_COP.1.1/Hash The TSF shall perform *hash generation*[33] in accordance with a specified cryptographic algorithm *SHA-256, SHA-384, SHA-512*[34] and cryptographic key sizes *none*[35] that meet the following: *FIPS 180-4 [17]*[36].

Application note: 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

(1) *create*[37]*, modify, clear and delete*[38] the *root key pair*[39] to **[selection: *Administrator, Crypto-Officer*]**[40].

(2) *import and delete*[41] **a *known as authentic public key of a certification authority in a PKI***[42] **to *[selection: Administrator, Crypto-Officer]***[43].

Application note: 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.

33 [assignment: *list of cryptographic operations*]

34 [assignment: *cryptographic algorithm*]

35 [assignment: *cryptographic key sizes*]

36 [assignment: *list of standards*]

37 “create” denotes initial setting a root key

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

39 [assignment: *list of TSF data*]

40 [assignment: *the authorised identified roles*]

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

42 [assignment: *list of TSF data*]

43 [assignment: *the authorised identified roles*]

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

Hierarchical to: No other components.

Dependencies: [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*[44] to *receive*[45] **certificate** ~~TSF data~~ in a manner protected from *modification and insertion*[46] errors.

FPT_TIT.1.2/Cert The TSF shall be able to determine on receipt of **certificate** ~~TSF data~~ , whether *modification and insertion*[47] has occurred.

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

Hierarchical to: No other components.

Dependencies: [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*[48] 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~~.

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[49].

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*[50] when shared between the TSF and another trusted IT product.

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

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

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

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

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

49 [assignment: *additional importation control rules*]

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*[51]

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

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_RBG_EXT.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, FCS_CKM.5/RSA) 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. FCS_CKM.1/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. The key generation may be combined with encryption, more precisely seed generation, key derivation from seed and seed encryption (cf. FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA). The inverse process comprise decryption of the seed ciphertext and derivation of the keys from the seed (cf. FCS_CKM.5/ECKA-EG, FCS_CKM.5/AES_RSA).

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

The SFR FCS_RBG_EXT.1, FCS_RBG_EXT.3 and FCS_RBG_EXT.6 require the TSF to generate and provide random bits by seeding the deterministic random bit generator by means of an internal noise source. If the TSF provides additional seeding by external noise source(s) the ST shall use FCS_RBG_EXT.2 and FCS_EXT.4 in order to describe the corresponding SFR.

FCS_RBG_EXT.1 Random Bit Generation (RBG)

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.2 or FCS_RBG_EXT.3
(No rationale is acceptable for not satisfying one of these dependencies)

FCS_RBG_EXT.1.1 The TSF shall perform deterministic random bit generation services using [assignment: *RBG algorithm*] in accordance with [assignment: *list of standards*] after initialization with a seed.

FCS_RBG_EXT.1.2 The TSF shall use an [selection: *TOE internal, TOE external*] noise source for initialized seeding.

FCS_RBG_EXT.1.3 The TSF shall [selection: *uninstantiate and instantiate, reseed*] the RBG in accordance with [assignment: *list of standards], [selection: on demand, on the condition: [assignment: condition], after [assignment: time], none*].

Application note: The ST writer shall assign a RBG algorithm meeting DRG.3 or DRG.4 [33] in the element FCS_RBG_EXT.1.1. Examples can be found in [34], chapter 6.

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

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

FCS_RBG_EXT.3 Random Bit Generation (Internal Seeding Single Source)

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1

FCS_RBG_EXT.3.1 The TSF shall seed the RBG using a single ***PTG.2 or higher [33]***[52] *TSF hardware-based noise source*[53] with a minimum of *125*[54] bits of min-entropy.

Application note: 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/KW, FCS_COP.1/HEM and FCS_COP.1/TCE. The minimum min-entropy to be provided as input for seeding meet the intended strength of the cryptographic mechanisms.

FCS_RBG_EXT.6 Random Bit Generation (RBG Services)

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1, [FCS_RBG_EXT.2 or FCS_RBG_EXT.3]

FCS_RBG_EXT.6.1 The TSF shall provide a [selection: *hardware, software, [assignment: other interface type]*] interface to make the RBG output, as specified in FCS_RBG_EXT.1, available as a service to entities outside of the TOE.

Application note: The ST writer shall perform the operation in the element FCS_RBG_EXT.6.1 according to the interface(s) provided by the TOE for the random bit generation service.

FCS_CKM.1/AES Cryptographic key generation – AES 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/AES The TSF shall generate cryptographic AES *key* **[55]** in accordance with a specified cryptographic key algorithms *AES*[56] and key size *128 bits, [*selection: *256 bits, no other key size]*[57] that meet the following: *ISO 18033-3 [28]*[58].

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

FCS_CKM.5/AES Cryptographic key generation – AES 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/AES The TSF shall derive cryptographic AES *key*[59] from [assignment: *input parameters*] in accordance with a specified cryptographic key algorithms AES *key generation using bit string derived from input parameters with KDF*[60] and specified cryptographic key sizes *128 bits, [*selection: *256 bits, no other key size]*[61] that meet the following: *ISO 18033-3 [28]* [62].

52 according to BSI AIS 31

53 [selection: *TSF software-based noise source, TSF hardware-based noise source*]

54 [assignment: number of bits]

55 **[assignment: *key type*]**

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

57 [assignment: *cryptographic key sizes*]

58 [assignment: *list of standards*]

59 **[assignment: *key type*]**

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

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 pair*[63] in accordance with a specified cryptographic key algorithms *ECC key pair generation with [selection: elliptic curves in the table 2]*[64] and cryptographic key sizes *[selection: key size in the table 2]*[65] that meet the following: *[selection: standards in the table 2]*[66].

Application note: 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 generation – 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 pair*[67] from [assignment: *input parameters*] in accordance with a specified cryptographic key algorithms *ECC key pair generation with [selection: elliptic curves in table 2] using bit string derived from input parameters with [assignment: KDF]* [68] and specified cryptographic *key* sizes *[selection: key size in the table 2]*[69] that meet the following: *[selection: standards in the table 2], [9], [21]*[70].

Application note: The elliptic key pair derivation applies a key derivation function (KDF) to the input parameter and uses the output string of KDF instead of the random bit string as input for the ECC key generation algorithm. The KDFs are defined in [9] and [21]. 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.

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*[71] in accordance with a specified cryptographic key algorithms *RSA*[72] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: *[8]*[73].

61 [assignment: *cryptographic key sizes*]

62 [assignment: *list of standards*]

63 **[assignment: *key type*]**

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

65 [assignment: *cryptographic key sizes*]

66 [assignment: *list of standards*]

67 **[assignment: *key type*]**

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

69 [assignment: *cryptographic key sizes*]

70 [assignment: *list of standards*]

71 **[assignment: *key type*]**

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

73 [assignment: *list of standards*]

Application note: 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. The keys generation according to FCS_CKM.1/RSA and key derivation according to FCS_CKM.5/RSA are intended for different key management use cases but the keys itself may be used for same cryptographic operations.

FCS_CKM.5/RSA Cryptographic key generation – RSA 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/RSA The TSF shall derive cryptographic *RSA key pair*[74] from [assignment: *input parameters*] in accordance with a specified cryptographic key algorithms RSA *key pair generation using bit string derived from input parameters with KDF*[75] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: *[8], [9],* [76].

Application note: The RSA key pair derivation applies a KDF to the input parameter and uses the output string of KDF instead of the random bit string as input for the RSA key generation algorithm. 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. The cryptographic key sizes assigned in FCS_CKM.5/RSA must be at least 2000 bits. Cryptographic key sizes of at least 3000 bits are recommended.

FCS_CKM.1/ECDHE Cryptographic key generation – 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.1.1/ECDHE The TSF shall **agree a shared secret** ~~generate~~ **for derivation of ephemeral** cryptographic keys *data encryption key and MAC keys for AES-128, [selection: AES-256, none other]*[77] in accordance with a specified cryptographic key agreement protocol *Elliptic Curve Diffie-Hellman ephemeral key agreement [selection: elliptic curves in table 2] and [selection: DH group in table 3] with SHA-1 [selection: SHA-256, none other]*[78] and specified cryptographic key sizes *128 bits [selection:256 bits, none other]*[79] that meet the following: *[10]*[80].

Application note: The table 2 lists elliptic curves and table 3 lists the Diffie-Hellman Groups for derivation of the shared secret. The SHA-1 shall be used to generate 128 bits AES keys. The SHA-256 shall be selected and used to generate 256 bits AES keys if selected.

74 **[assignment: *key type*]**

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

76 [assignment: *list of standards*]

77 **[assignment: key type]**

78 [assignment: *cryptographic key agreement protocol*]

79 [assignment: *cryptographic key sizes*]

80 [assignment: *list of standards*]

FCS_CKM.1/ECKA-EG Cryptographic key generation – ECKA-EG 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/ECKA-EG The TSF shall generate **and encrypt** cryptographic *data encryption key and MAC keys for AES-128, [selection: AES-256, none other]*[81] in accordance with a specified cryptographic key algorithms *Elliptic Curve Integrated Encryption Scheme with [selection: elliptic curves in table 2], X9.63 Key Derivation Function and AES*[82] and specified cryptographic **symmetric** key sizes *128 bits [selection:256 bits, none other]*[83] that meet the following: *[10], chapter 4.3.2.2*[84].

FCS_CKM.5/ECKA-EG Cryptographic key generation – 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 **decrypt and** derive cryptographic *data encryption key and MAC keys for AES-128, [selection: AES-256, none other]*[85] from *ECC encrypted seed*[86] in accordance with a specified cryptographic key algorithms *X9.63 Key Derivation Function, and Elliptic Curve Integrated Encryption Scheme with [selection: elliptic curves in table 2]*[87] and specified cryptographic **symmetric** key sizes *128 bits [selection:256 bits, none other]*[88] that meet the following: *[10], chapter 4.3.2.2*[89].

Application note: The ECKA-EG according to FCS_CKM.1/ECKA-EG and FCS_CKM.5/ECKA-EG combine generation of a random seed, ECC encryption by the sender and ECC decryption decryption of the seed and derivation of AES key encryption and AES MAC keys from the seed. The static public key and the corresponding domain parameters publicly distributed and can be attributed reliably to the authorised recipient of the message. To send an encrypted (and integrity protected) message, the sender generates a random seed, encrypts the seed with the public key of the receiver, and sends it to the receiver. The receiver decrypts the seed using his private key. The sender and the receiver derive the symmetric data encryption key and the message authentication key from the seed. The selection of elliptic curve, the ECC key size and length of the random seed shall correspond to the selection of AES algorithm and the AES key size, e. g. brainpoolP256r1 and 256 bits seed, ECC key and AES keys.

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** cryptographic *data encryption key and MAC keys for AES-128, [selection: AES-256, none other]*[90] in accordance with a specified cryptographic

81 **[assignment: *key type*]**

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

83 [assignment: *cryptographic key sizes*]

84 [assignment: *list of standards*]

85 **[assignment: *key type*]**

86 [assignment: *input parameters*]

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

88 [assignment: *cryptographic key sizes*]

89 [assignment: *list of standards*]

90 **[assignment: *key type*]**

key algorithm *X9.63 Key Derivation Function and RSA EME-OAEP*[91] and specified cryptographic **symmetric** key sizes *128 bits [selection:256 bits, none other]*[92] that meet the following: *ISO/IEC18033-3 [28], [8], chapter 3.5*[93].

Application note: 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.5/AES_RSA Cryptographic key generation – 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 **decrypt and** derive cryptographic *data encryption key and MAC keys for AES-128, [selection: AES-256, none other]*[94] from *RSA encrypted seed*[95] in accordance with a specified cryptographic key algorithm *RSA EME-OAEP and X9.63 Key Derivation Function*[96] and specified cryptographic **symmetric** key sizes *128 bits [selection:256 bits, none other]*[97] that meet the following: *[11], chapter 3.5*[98].

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]
FMT_MSA.2 Secure security attributes

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.

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

92 [assignment: *cryptographic key sizes*]

93 [assignment: *list of standards*]

94 **[assignment: *key type*]**

95 [assignment: *input parameters*]

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

97 [assignment: *cryptographic key sizes*]

98 [assignment: *list of standards*]

6.1.1.5 Key import and export

FCS_COP.1/KW Cryptographic operation – Key wrap

Hierarchical to: No other components.

Dependencies: [FDP_ETC.1 Export of user data without security attributes, or
FDP_ETC.2 Export of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
MT_MSA.2 Secure security attributes

FCS_COP.1.1/KW The TSF shall perform *key wrap*[99] in accordance with a specified cryptographic algorithm *AES-Keywrap [selection: KW, KWP]*[100] and cryptographic key sizes **of the *key encryption key*** *128 bits [selection:256 bits, none other]*[101] that meet the following: *[29]*[102].

Application note: 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
MT_MSA.2 Secure security attributes

FCS_COP.1.1/KU The TSF shall perform *key unwrap*[103] in accordance with a specified cryptographic algorithm *AES-Keywrap [selection: KW, KWP]*[104] and cryptographic key sizes **of the *key encryption key*** *128 bits [selection:256 bits, none other]*[105] that meet the following:*[29]*[106].

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

Hierarchical to: No other components.

Dependencies: [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*[107] by providing the ability to *transmit and receive*[108] **cryptographic key** ~~TSF data~~ in a manner protected from unauthorised disclosure **according to FCS_COP.1/KW and FCS_COP.1/KU**.

99 [assignment: *list of cryptographic operations*]

100 [assignment: *cryptographic algorithm*]

101 [assignment: *cryptographic key sizes*]

102 [assignment: *list of standards*]

103 [assignment: *list of cryptographic operations*]

104 [assignment: *cryptographic algorithm*]

105 [assignment: *cryptographic key sizes*]

106 [assignment: *list of standards*]

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

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

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

Hierarchical to: No other components.

Dependencies: [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*[109] to *transmit and receive*[110] **cryptographic keys** ~~TSF data~~ in a manner protected from *modification and insertion*[111] errors **according to FCS_COP.1/KW**.

FPT_TIT.1.2/CK The TSF shall be able to determine on receipt of **cryptographic keys** ~~TSF data~~, whether *modification and insertion*[112] 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: [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*[113] 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 ~~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]*[114].

Application note: 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* [115] when shared between the TSF and another trusted IT product.

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

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

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

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

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

114 [assignment: *importation control rules*]

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

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,*

(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*[116]

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: [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*[117] 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: *exportation control rules*].

Application note: 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 User data encryption

FCS_COP.1/ED Cryptographic operation – User 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
MT_MSA.2 Secure security attributes

FCS_COP.1.1/ED The TSF shall perform *data encryption and decryption*[118] 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] mode* [119] and cryptographic key size *128 bits, [*selection: *256 bits, no other key size]*[120] that meet the following: FIPS SP800-38A, *ISO 18033-3 [28], ISO 10116*[121].

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

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

118 [assignment: *list of cryptographic operations*]

119 [assignment: *cryptographic algorithm*]

120 [assignment: *cryptographic key sizes*]

121 [assignment: *list of standards*]

Application note: 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
MT_MSA.2 Secure security attributes

FCS_COP.1.1/HEM The TSF shall perform *hybrid data encryption and MAC calculation*[122] in accordance with a specified cryptographic algorithm *asymmetric key encryption according to [selection: FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA], symmetric data encryption according to AES-128, [selection: AES-256, none other] in [selection: CBC, CCM, GCM] mode with [selection: CMAC, GMAC, HMAC] calculation*[123] and cryptographic **symmetric** key sizes *128 bits,* [selection: *256 bits, no other key size]*[124] that meet the following: *ISO 18033-3, ISO 10116, ISO 19772, [6]*[125].

Application note: The generation and encryption of data encryption keys and MAC keys as well as the AES encryption and MAC calculation are only a steps of the hybrid encryption of user data according to FCS_COP.1.1/HEM. They are not a self-contained security services of the TOE. The hybrid encryption is combined with MAC as data integrity mechanisms for the cipher text, i. e. encrypt-than-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
MT_MSA.2 Secure security attributes

FCS_COP.1.1/HDM The TSF shall perform *hybrid MAC verification and data decryption*[126] in accordance with a specified cryptographic algorithm *asymmetric key decryption according to [selection: FCS_CKM.5/ECKA-EG, FCS_CKM.5/AES_RSA], verification of [selection: CMAC, GCM, HMAC] and symmetric data decryption according to AES with [selection: AES-128, AES-256] in mode [selection: CBC, CCM, GMAC]* [127] and cryptographic **symmetric** key sizes *128*

122 [assignment: *list of cryptographic operations*]

123 [assignment: *cryptographic algorithm*]

124 [assignment: *cryptographic key sizes*]

125 [assignment: *list of standards*]

126 [assignment: *list of cryptographic operations*]

127 [assignment: *cryptographic algorithm*]

bits, [selection: 256 bits, no other key size][128] that meet the following: *ISO 18033-3, ISO 10116, ISO 19772, [6]*[129].

Application note: The decryption of data encryption keys and MAC keys as well as the AES decryption and MAC verification are only a steps of the hybrid decryption of user data. They are not a self-contained security services of the TOE. 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-than-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 message authentication code (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
MT_MSA.2 Secure security attributes

FCS_COP.1.1/MAC The TSF shall perform *MAC generation and verification*[130] in accordance with a specified cryptographic algorithm *AES-128 and [selection: AES-256, none other] CMAC and [selection: GMAC, no other]*[131] and cryptographic key sizes *128 bits [selection: 256 bits, no other key size]*[132] that meet the following: *FIPS SP 800-38B, ISO9797-1, Algorithm 1, Padding 2, FIPS SP 800-38D*[133].

Application note: 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
MT_MSA.2 Secure security attributes

FCS_COP.1.1/HMAC The TSF shall perform *HMAC generation and verification*[134] in accordance with a specified cryptographic algorithm *HMAC-SHA256 and [selection: HMAC-SHA-1, HMAC-SHA384, no*

128 [assignment: *cryptographic key sizes*]

129 [assignment: *list of standards*]

130 [assignment: *list of cryptographic operations*]

131 [assignment: *cryptographic algorithm*]

132 [assignment: *cryptographic key sizes*]

133 [assignment: *list of standards*]

134 [assignment: *list of cryptographic operations*]

other][135] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: *RFC2104, ISO-9797-2 [18]*[136].

Application note: The cryptographic key is a random bit string generated by FCS_RBG_EXT.3 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
MT_MSA.2 Secure security attributes

FCS_COP.1.1/CDS-ECDSA The TSF shall perform *signature-creation*[137] in accordance with a specified cryptographic algorithm *ECDSA with [selection: elliptic curves in the table 2]*[138] *and specified cryptographic key* sizes *[selection: key size in the table 2]*[139] *that meet the following: [selection: standards in the table 2]*[140].

Application note: 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
MT_MSA.2 Secure security attributes

FCS_COP.1.1/VDS-ECDSA The TSF shall perform *signature-verification*[141] in accordance with a specified cryptographic algorithm *ECDSA with [selection: elliptic curves in the table 2]*[142] *and specified cryptographic key* sizes *[selection: key size in the table 2]*[143] *that meet the following: [selection: standards in the table 2]*[144].

135 [assignment: *cryptographic algorithm*]

136 [assignment: *list of standards*]

137 [assignment: *list of cryptographic operations*]

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

139 [assignment: *cryptographic key sizes*]

140 [assignment: *list of standards*]

141 [assignment: *list of cryptographic operations*]

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

143 [assignment: *cryptographic key sizes*]

144 [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
MT_MSA.2 Secure security attributes

FCS_COP.1.1/CDS-RSA The TSF shall perform *signature-creation*[145] in accordance with a specified cryptographic algorithm *RSA and EMSA-PSS*[146] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: ISO/IEC 14888-2, *PKCS #1, v2.2 [8]*[147].

Application note: 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
MT_MSA.2 Secure security attributes

FCS_COP.1.1/VDS-RSA The TSF shall perform *signature-verification*[148] in accordance with a specified cryptographic algorithm *RSA and EMSA-PSS*[149] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: *ISO/IEC 14888-2, PKCS #1, v2.2 [8]*[150].

Application note: 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*[151] **the user data 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*[152] 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: 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-creation operation. The

145 [assignment: *list of cryptographic operations*]

146 [assignment: *cryptographic algorithm*]

147 [assignment: *list of standards*]

148 [assignment: *list of cryptographic operations*]

149 [assignment: *cryptographic algorithm*]

150 [assignment: *list of standards*]

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

152 [assignment: l*ist of subjects*]

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.

FDP_DAU.2/TS Data Authentication with Identity of Guarantor – Signature with time stamp

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_DAU.2.1/TS The TSF shall provide a capability to generate evidence that can be used as a guarantee of the **existence at certain point in time, sequence and** validity of

(a) *user data imported according to FDP_ITC.2/UD,*

(b) *exported audit trails according to FMT_MTD.1 clause (1) and FAU_STG.3 clause (1)*[153]

with

(1) time stamp of the evidence generation according to FPT_STM.1,

(2) Key usage counter of the signature key

by means of digital signature generated according to [selection: *FCS_COP.1/CDS-ECDSA, FCS_COP.1/CDS-RSA*] and keys holding the security attributes Key identity assigned to the TOE sample and Key usage type "Time stamp service".

FDP_DAU.2.2/TS The TSF shall provide [assignment: *list of subjects*] 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: The TSF according to FDP_DAU.2/TS is intended for time stamp service of the TOE for any provided user data and exported audit records. The user data source shall select the security attribute *Key usage type* "*TimeStamp*" of the signature key of the time stamp service. The signature key of exported audit records shall be defined according to FMT_MOF.1 clause (9). The Key usage counter allows to verify the sequence of signed data e. g. in an audit trail. The verification of the evidence requires a certificate showing the identity of the TOE sample and the key usage type of time stamp service. The format of input data and output data shall meet the BSI TR-03151 [31].

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 and PCD role*[154] to prove the identity of the *TOE*[155] to *an* external entity **and establishing a trusted channel according to FTP_ITC.1 case 1 or 2**.

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

154 [assignment: *authentication mechanism*]

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

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 [14] section 3.4*[156] to prove the identity of the *TOE*[157] to *an* external entity **and establishing a trusted channel according to FTP_ITC.1 case 3**.

FIA_API.1/TA Authentication Proof of Identity – Terminal authentication of user

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/TA The TSF shall provide a Terminal *Authentication Version 2 according to [14] section 3.3 [14]*[158] to prove the identity of the *TOE*[159] to an external entity.

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*[160] **by means of [selection: *FCS_COP.1/CDS-RSA, FCS_COP.1/ CDS-ECDSA, ECDAA according to [selection: [24], [25]], [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*[161] 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: 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 [24] or FIDO U2F Authenticators [25].

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 a remote trusted IT product that is **[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 **[selection: *protection of communication data according to the case in table 4*] as required by [selection: *cryptographic operation according to the case in table 4].***

156 [assignment: *authentication mechanism*]

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

158 [assignment: *authentication mechanism*]

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

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

161 [assignment: l*ist of subjects*]

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

FTP_ITC.1.3 The TSF shall

(1) ~~initiate~~ ***allow*** communication via the trusted channel for *the list of functions for which a trusted channel is allowed as configured according to FMT_MOF.1.1 clause (5)*[162]

(2) ~~**initiate**~~ ***enforce*** **communication via the trusted channel for *the list of functions for which a trusted channel is enforced as configured according to FMT_MOF.1 clause (6)***[163].

(3) ~~**initiate**~~ ~~*enforce*~~ **communication via at least one trusted channel for *data in transit between two TOE users as configured according to FMT_MOF.1 clauses (5) and (6).***[164]

Application note: The bullets (2) and (3) are refinements to avoid an iteration of component and therefore printed in bold.

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) or (3), and (6)	FCS_CKM.1/PACE	modification	FCS_COP.1/TCM
2	FIA_API.1/PACE FIA_UAU.5.1 (2) or (3), and (6)	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
4	FIA_API.1/TA FIA_UAU.5.1 (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

Application note: The ST author may select cases to be implemented by the TSF. If only case 1 is required than FCS_COP.1/TCE may be not necessary for trusted channel (but may be required for clustering).

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 ***MAC keys for FCS_COP.1/TCM and if selected encryption keys for FCS_COP.1/TCE***[165] in accordance with a specified cryptographic key **agreement** algorithm *PACE with [selection: elliptic curves in table 2] and Generic Mapping in ICC role*[166] and specified cryptographic key sizes *[selection: 128 bits, 192 bits, 256 bits]*[167] that meet the following: *[5], section 4.4*[168].

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

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

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

165 **[assignment: *key type*]**

166 [assignment: ***cryptographic key agreement protocol***]

167 [assignment: *cryptographic key sizes*]

168 [assignment: *list of standards*]

Application note: 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 encryption and MAC integrity protection of the following communication.

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 ***encryption keys for FCS_COP.1/TCE and MAC keys for FCS_COP.1/TCM***[169] in accordance with a specified cryptographic key **agreement** algorithms *Terminal Authentication version 2 and Chip Authentication Version 2* [170] and specified cryptographic key sizes *[selection: 128 bits, 192 bits, 256 bits]*[171] that meet the following: *[14], section 3.3 and 3.4*[172].

Application note: 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
FMT_MSA.2 Secure security attributes

FCS_COP.1.1/TCE The TSF shall perform *encryption and decryption*[173] in accordance with a specified cryptographic algorithm *AES in [selection: CBC, CCM, GCM] mode*[174] and cryptographic key sizes [*selection: 128 bits, 192 bits, 256 bits]* [175] that meet the following: *ISO18033-3*[176].

169 **[assignment: *key type*]**

170 [assignment: ***cryptographic key agreement protocol***]

171 [assignment: *cryptographic key sizes*]

172 [assignment: *list of standards*]

173 [assignment: *list of cryptographic operations*]

174 [assignment: *cryptographic algorithm*]

175 [assignment: *cryptographic key sizes*]

176 [assignment: *list of standards*]

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
FMT_MSA.2 Secure security attributes

FCS_COP.1.1/TCM The TSF shall perform *MAC calculation and MAC verification*[177] in accordance with a specified cryptographic algorithm *AES [selection: CMAC, GMAC]*[178] and cryptographic key sizes *[selection: 128 bits, 192 bits, 256 bits]*[179] that meet the following: *[26], [27]*[180].

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) *Reference authentication data*,

(3) *Role*.

FMT_MTD.1/RAD Management of TSF data – Reference Authentication 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 [181] the *initial authentication reference data of all authorized users*[182] to *[selection: Administrator, User Administrator]*[183],

(2) *delete*[184] the *authentication reference data of an authorized user*[185] to *[selection: Administrator, User Administrator]*[186],

(3) *modify*[187] the *Reference Authentication Data*[188] to *the corresponding authorized user*[189].

177 [assignment: *list of cryptographic operations*]

178 [assignment: *cryptographic algorithm*]

179 [assignment: *cryptographic key sizes*]

180 [assignment: *list of standards*]

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

182 [assignment: *list of TSF data*]

183 [assignment: *the authorised identified roles*]

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

185 [assignment: *list of TSF data*]

186 [assignment: *the authorised identified roles*]

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

188 [assignment: *list of TSF data*]

189 [assignment: *the authorised identified roles*]

(4) ***create***[190] **the** ***permanently stored session key of trusted channel as Reference Authentication Data***[191] **to** ***[selection: Administrator, User Administrator]***[192]

(5) ***define***[193] **the** ***time in range [assignment: time frame] after which the user security attribute Role is reset according to FMT_SAE.1***[194] ***to [selection: Administrator, User Administrator]***[195]**,**

(6) ***define***[196] **the** ***value [selection: Unidentified user, Unauthenticated user] to which the security attribute Role shall be reset according to FMT_SAE.1***[197] ***to [selection: Administrator, User Administrator]***[198].

Application note: 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*[199] **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 [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*].

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

191 [assignment: *list of TSF data*]

192 [assignment: *the authorised identified roles*]

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

194 [assignment: *list of TSF data*]

195 [assignment: *the authorised identified roles*]

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

197 [assignment: *list of TSF data*]

198 [assignment: *the authorised identified roles*]

199 [assignment: list of TSF data]

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*[200].

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*[201].

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

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

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

(3) *after successful re-authentication of the user for a selected role the user is authorized for the subject attribute Role shall be changed to that role*[202].

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*[203] to *[selection: Administrator, User Administrator]*[204].

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)*[205] after the expiration time for the indicated security attribute has passed.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow

(1) s*elf test according to FPT_TST.1*,

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

(3) *[assignment: list of other TSF-mediated actions]*[206]

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

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

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

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

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

204 [assignment: *the authorised identified roles*]

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

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

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*,

(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]*[207]

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: 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 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 [14] with the TOE in ICC and user in PCD context*,

(4) *version of Terminal Authentication Version 2 with the TOE in ICC context and user in PCD context modified by omitting the certificate chain of the user according to [30]*,

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

(6) *message authentication by MAC verification of received messages*[208]

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 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 external entities with establishment of trusted channel according to FTP_ITC.1*,

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

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

(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) *certificate based Chip Authentication Version 2 with establishment of trusted channel according to FTP_ITC.1 may be used for authentication of users which certificate imported as TSF data,*

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

(8) *[assignment: additional rules]*[209].

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) c*hanging 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]*[210].

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*[211] 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 identification of the encryption key,*

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

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

211 [assignment: *access control SFP*]

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

(2) *user data imported for decryption shall be imported with reference to key decryption key, encrypted data encryption key and data integrity check sum,*

(3) *user data imported for digital signature creation shall be imported with the identification of the private signature key,*

(4) *user data imported for digital signature verification shall be imported with digital signature and identification of the public signature key*[212].

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*[213] 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,*

(2) *user data internally generated and 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*[214].

Application note: 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 (e.g. audit records) 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*[215] when exporting user data **exported 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.

212 [assignment: *additional importation control rules*]

213 [assignment: *access control SFP*]

214 [assignment: *additional exportation control rules*]

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

FDP_ACC.1/Oper Subset access control – Cryptographic operation

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/Oper The TSF shall enforce the *Cryptographic Operation SFP*[216] on

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

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

(3) **operations:** c*ryptographic operation*[217]

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*[218] to objects based on the following:

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

(2) objects:

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

(b) *user data*[219].

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 key management 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]*.[220]

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

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

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

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

216 [assignment: *access control SFP*]

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

218 [assignment: *access control SFP*]

219 [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*]

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

(3) *[assignment: other rules, based on security attributes, that explicitly deny access of subjects to objects]*.[221]

Access control rules for cryptographic operation:

Security attribute of the subject	Security attribute of the cryptographic key	Cryptographic operation referenced by SFR
[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)	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)	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/DS-ECDSA
(any)	Key type: public Key usage type: DS-ECDSA Key validity time period:	FCS_COP.1/DS-ECDSA
Key Owner	Key type: private Key usage type: DS-RSA Key validity time period:	FCS_COP.1/CDS-RSA
(any)	Key type: public Key usage type: DS-RSA Key validity time period:	FCS_COP.1/VDS-RSA

Table 5: Security attributes and access control

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)*,

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

(2) *management of Reference Authentication Data (FMT_MTD.1/Admin, FMT_MTD.1/User),*

(3) *management of audit data (FMT_MTD.1/Audit),*

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

(5) *[assignment: list additional of security management functions to be provided by the TSF]*[222].

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, Auditor, Update Agent] [selection: [assignment: other roles], no other roles]*[223].

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

Application note: The ST author may select the general term 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. **The cryptographic keys shall have**

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

(2) exactly one Key type,

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

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*[224] the functions *password authentication according to FIA_UAU.5.1, clause (1)*[225] to *[selection: Administrator, User Administrator]*[226].

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

223 [assignment: *authorised identified roles*]

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

225 [assignment: *list of functions*]

226 [assignment: *the authorised identified roles*]

(2) ***disable***[227] **the functions** ***password authentication according to FIA_UAU.5.1, clause (1)***[228] **to** ***[selection: Administrator, User Administrator]***[229]**,**

(3) ***determine the entities for which the TSF shall allow*** [230] **the functions** ***trusted channel according to FDP_ITC.1***[231] **to** ***[selection: Administrator, User Administrator]***[232]**,**

(4) ***determine the entities for which the TSF shall enforce***[233] **the functions** ***trusted channel according to FDP_ITC.1***[234] **to** ***[selection: Administrator, User Administrator]***[235]

(5) ***modify the behaviour of***[236] **the functions** ***adjustment of real time clock according to FPT_STM.1 clause (1)***[237] **to** ***Administrator***[238]**,**

(6) ***modify the behaviour of***[239] **the functions** ***adjustment of real time clock according to FPT_STM.1 clause (2)***[240] **to** ***Administrator***[241]**,**

(7) ***determine the behaviour of and modify the behaviour of***[242] **the functions** ***select the auditable events according to FAU_GEN.1***[243] **to** ***[selection: Administrator, Auditor]***[244]**,**

(8) ***determine the behaviour of and modify the behaviour of***[245] **the functions** ***automatic export of audit trails according to FAU_STG.3.2 clause (1)***[246] **to** ***[selection: Administrator, Auditor]***[247]

(9) ***determine the behaviour of and modify the behaviour of***[248] **the functions** ***FDP_DAU.2/TS by selection of signature key used to sign exported audit trails***[249] **to** ***[selection: Administrator, Auditor]***[250]**.**

Application note: The refinements of FMT_MOF.1.1 in bullets (2) to (9) 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).

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

228 [assignment: *list of functions*]

229 [assignment: *the authorised identified roles*]

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

231 [assignment: *list of functions*]

232 [assignment: *the authorised identified roles*]

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

234 [assignment: *list of functions*]

235 [assignment: *the authorised identified roles*]

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

237 [assignment: *list of functions*]

238 [assignment: *the authorised identified roles*]

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

240 [assignment: *list of functions*]

241 [assignment: *the authorised identified roles*]

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

243 [assignment: *list of functions*]

244 [assignment: *the authorised identified roles*]

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

246 [assignment: *list of functions*]

247 [assignment: *the authorised identified roles*]

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

249 [assignment: *list of functions*]

250 [assignment: *the authorised identified roles*]

6.1.9 Clustering

The cluster of TOE samples is set up by the Administrator as Cluster-CSPs by

– selecting one TOE sample of the cluster as Master-CSP, all other TOE samples of the cluster are Slave-CSPs,

– initialization of a secure channel between the Master-CSP and the Slave-CSPs,

– transfer of TSF data as security attributes of known users and cryptographic keys with security attributes from Master-CSP to Slave-CSPs using the application.

FMT_MTD.1/CL Management of TSF data – Authentication Data Records and cryptographic keys

Hierarchical to: No other components.

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

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

(1) *initiate*[251] the *CSP cluster*[252] to *Administrator*[253],

***(2) export according to FPT_ESA.1/CL, FPT_TCT.1/CL and FPT_TIT.1/CL[254]* the *Authentication Data Records from the Master-CSP[255]* to *[selection: Application Component, Administrator, User Administrator][256]*,**

***(3) import according to FPT_ISA.1/CL, FPT_TCT.1/CL and FPT_TIT.1/CL[257]* the *Authentication Data Records into Slave-CSPs[258]* to *[selection: Application Component, Administrator, User Administrator]*[259]**

***(4) export according to FPT_ESA.1/CL, FPT_TCT.1/CL and FPT_TIT.1/CL[260]* the *cryptographic keys from the Master-CSP [261]* to *[selection: Application Component, Administrator, Crypto-Officer][262]*,**

***(5) import according to FPT_ISA.1/CL, FPT_TCT.1/CL and FPT_TIT.1/CL[263]* the *cryptographic keys into Slave-CSPs[264]* to *[selection: Application Component, Administrator, Crypto-Officer][265]*.**

Application note: Authentication Data Records and cryptographic keys are TSF data. [30] describes the export and import of *Authentication Data Records* and *cryptographic keys* by an *Application Component.* The selection in FMT_MTD.1/CL allows for a more detailed separation of duties between the roles if supported by the TOE. The bullets (2) to (5) are refinements to avoid an iteration of the component and therefore printed in bold.

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

252 [assignment: *list of TSF data*]

253 [assignment: *the authorised identified roles*]

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

255 [assignment: *list of TSF data*]

256 [assignment: *the authorised identified roles*]

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

258 [assignment: *list of TSF data*]

259 [assignment: *the authorised identified roles*]

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

261 [assignment: *list of TSF data*]

262 [assignment: *the authorised identified roles*]

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

264 [assignment: *list of TSF data*]

265 [assignment: *the authorised identified roles*]

FTP_ITC.1/CL Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/CL The TSF shall provide a communication channel between TSF and a remote trusted ~~IT~~ **CSP** product that is **[selection: *logically separated from other communication channels, using physical separated ports*]** and provides assured identification of its end points **[selection: *Authentication of TOE and CSP according to the case in table 4*]** and protection of the channel data from **[selection: *Protection of communication data according to the case in table 4*] as required by [selection: *Cryptographic operation according to the case in table 4]***

FTP_ITC.1.2/CL The TSF shall permit [selection: *the TSF, the remote trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3/CL The TSF shall **enforce** communication via the trusted channel for

(1) export of Authentication Data Records and cryptographic keys as Master-CSP according to FMT_MTD.1.1/CL clause (2) and FPT_ESA.1/CL,

(2) import of Authentication Data Records and cryptographic keys as Slave-CSP according to FMT_MTD.1.1/CL clause (3) and FPT_ISA.1/CL.[266]

FCS_CKM.1/CLDH Cryptographic key generation – Diffie-Hellman 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/CLDH The TSF shall generate cryptographic *elliptic curve key pair*[267] in accordance with a specified cryptographic key algorithms *Diffie-Hellman Key Agreement for ECC key pair generation with [selection: elliptic curves in the table 2]*[268] *and specified cryptographic key* sizes *[selection: key size in the table 5]*[269] *that meet the following: [selection: standards in the table 5], [30]*[270].

FPT_TCT.1/CL TSF data confidentiality transfer protection – Cluster

Hierarchical to: No other components.

Dependencies: [FMT_MTD.1 Management of TSF data or
FMT_MTD.3 Secure TSF data]

FPT_TCT.1.1/CL The TSF shall enforce the *Clustering SFP*[271] by providing the ability to *transmit and receive*[272] **Authentication Data Records and cryptographic keys** ~~TSF data~~ in a manner protected from unauthorised disclosure.

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

267 **[assignment: *key type*]**

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

269 [assignment: *cryptographic key sizes*]

270 [assignment: *list of standards*]

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

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

FPT_TIT.1/CL TSF data integrity transfer protection – Cluster

Hierarchical to: No other components.

Dependencies: [FMT_MTD.1 Management of TSF data or
FMT_MTD.3 Secure TSF data]

FPT_TIT.1.1/CL The TSF shall enforce the *Clustering SFP*[273] to *transmit and receive*[274] **Authentication Data Records and cryptographic keys** ~~TSF data~~ in a manner protected from *modification and insertion*[275] errors.

FPT_TIT.1.2/CL The TSF **in role Slave-CSP** shall be able to determine on receipt of **Authentication Data Records and cryptographic keys** ~~TSF data~~, whether *modification and insertion*[276] has occurred.

FPT_ISA.1/CL Import of TSF data with security attributes – Cluster

Hierarchical to: No other components.

Dependencies: [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/CL The TSF shall enforce the *Clustering SFP*[277] when importing **Authentication Data Records and cryptographic keys** ~~TSF data~~, controlled under the SFP, from ~~outside of the TOE~~ **Master-CSP**.

FPT_ISA.1.2/CL The TSF **in role Slave-CSP** shall use the security attributes associated with the imported **Authentication Data Records and cryptographic keys** ~~TSF data~~.

FPT_ISA.1.3/CL The TSF **in role Slave-CSP** shall ensure that the protocol used provides for the unambiguous association between the security attributes and the TSF data received.

FPT_ISA.1.4/CL The TSF **in role Slave-CSP** shall ensure that interpretation of the security attributes of the imported TSF data is as intended by the source of the **Authentication Data Records and cryptographic keys** ~~TSF data~~.

FPT_ISA.1.5/CL The TSF **in role Slave-CSP** shall enforce the following rules when importing **Authentication Data Records and cryptographic keys** ~~TSF data~~ controlled under the SFP from ~~outside of the TOE~~ **Master-CSP**:

(1) *TSF in role Slave-CSP imports an Authentication Data Record with security attributes from Master-CSP,*

(2) *TSF in role Slave-CSP with security attribute slave imports cryptographic keys with security attributes from Master-CSP if the security attribute Clustering of the key allows distribution*[278].

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

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

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

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

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

278 [assignment: *additional importation control rules*]

FPT_ESA.1/CL Export of TSF data with security attributes – Cluster

Hierarchical to: No other components.

Dependencies: [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/CL The TSF shall enforce the *Clustering SFP*[279] when exporting TSF data, controlled under the SFP(s), outside of the TOE.

FPT_ESA.1.2/CL The TSF **in role Master-CSP** shall export the A**uthentication Data Records and cryptographic keys** ~~TSF data~~ with the TSF data's associated security attributes.

FPT_ESA.1.3/CL The TSF **in role Master-CSP** shall ensure that the security attributes, when exported ~~outside the TOE~~ **to Slave-CSP**, are unambiguously associated with the exported A**uthentication Data Records and cryptographic keys** ~~TSF data~~.

FPT_ESA.1.4/CL The TSF **in role Master-CSP** shall enforce the following rules when A**uthentication Data Records and cryptographic keys** ~~TSF data~~ is exported ~~from the TOE~~ **to Slave-CSP**:

(1) *TSF in role Master-CSP exports Authentication Data Records with security attributes to CSP-Slave.*

(2) *TSF in role Master-CSP exports cryptographic key with security attributes to CSP-Slave if the security attribute Clustering of the key allows distribution*[280].

6.1.10 Security audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

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

b) All auditable events for the *not specified*[281] level of audit; and

c) other auditable events

(1) *Start-up after power-up,*

(2) *Maintenance with software download,*

(3) *Establishing cluster with trusted channel according to FMT_MTD.1/CL and FTP_ITC.1/CL,*

(4) *Export of Authentication Data Records and cryptographic keys from the Master-CSP according to FPT_ESA.1/CL,*(3) *Management of Authentication Data Records (FMT_MTD.1): creation and deletion of Authentication Data Record*

(5) Import according to FPT_ISA.1/CL of Authentication Data Records and cryptographic keys into Slave-CSPs according to FPT_ISA.1/CL,

(6) *Authentication failure handling (FIA_AFL.1): the reaching of the threshold for the unsuccessful authentication attempts with claimed Identity of the user,*

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

280 [assignment: *additional exportation control rules*]

281 [selection: *choose one of: minimum, basic, detailed, not specified*]

[selection:

(7) G*eneration of (selected types of) signature key pairs (all FCS_COP.1 instantiations for generation permanent stored keys)*

(8) *Execution of (selected types of) cryptographic operation (all FCS_COP.1 instantiations),*

(9) *Cryptographic key destruction (FCS_CKM.4): permanent stored keys,*

(10) *Failure with preservation of secure state (FPT_FLS.1): entering and exiting secure state,*

(11) *Discrete* a*djustment of the real time clock*

(a) by signed Network Protocol according to FPT_STM.1.1 clause (1) if selected as auditable event,

(b) by Administrator according to FPT_STM.1.1 clause (2) or(3),

(c) failure of adjustment according to FPT_STM.1.1,

(12) *Management of TSF data (FMT_MTD.1/AUDIT): Export, clear and selection of events causing audit data,*

(13) *Management of security functions (FMT_MOF.1),*

(14) *no other event],*

(15) *[assignment: additional specifically defined auditable events]*[282].

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information].

FMT_MTD.1/Audit Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

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

(1) *manual export,*

(2) *clear after manual export,*

(3) *select audited events in*[283]

the *audit records*[284] to *[selection: Administrator, Auditor]*[285].

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

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

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

284 [assignment: *list of TSF data*]

285 [assignment: *the authorised identified roles*]

FAU_STG.1.2 The TSF shall be able to *prevent*[286] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.3 Action in Case of Possible Audit Data Loss

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall

(1) *automatically export audit trails and clear automatically exported audit records*[287] if the audit trail exceeds *an [selection: Administrator, Auditor] defined number of audit records*[288]

(2) *[assignment: actions to be taken in case of possible audit storage failure]* if the audit trail exceeds an *[selection: Administrator, Auditor] settable percentage of storage capacity*[289].

Application note: The ST writer shall perform the open operations in FAU_STG.3.1 element. If the number of number of audit records in clause (1) is set to 1 then the TSF export each audit record automatically. If the number of number of audit records in clause (1) is set higher than maximum number of audit records in the audit trail then the TSF does not export audit records automatically. The assignment of clause (2) may be “no actions” if an appropriate number of audit records is assigned in clause (1).

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps **by means of [selection:**

(1) internal real time clock with automatically adjustment by signed Network Time Protocol,

(2) internal real time clock with adjustment by Administrator if connection with signed Network Time Protocol is not available,

(3) internal real time clock with adjustment by Administrator].

Application note: The signed Network Time Protocol provides a reliable time source for adjustment of the internal real time clock. The time intervals of adjustments in clause (1) may be configured by Administrator. Any adjustment or failure of adjustment of the real time clock is an auditable event according to FAU_GEN.1.1. The refinement with selection defines different cases for real time clocks and therefore printed in bold.

6.1.11 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 [selection: *FCS_COP.1/SDE]*]**.

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

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

288 [assignment: *pre-defined limit*]

289 [assignment: *pre-defined limit*]

Application note: 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.

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*[290] in accordance with a specified cryptographic key algorithms *AES using random bit generation according to FCS_RBG_EXT.3* [291] 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
MT_MSA.2 Secure security attributes

FCS_COP.1.1/SDE The TSF shall perform *stored data encryption and decryption*[292] 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: The generation of data encryption keys and the encryption and decryption are only 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)*[293].

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

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

290 **[assignment: *key type*]**

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

292 [assignment: *list of cryptographic operations*]

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

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*,

(3) *manipulation and physical probing 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 i*nitial start-up, at the request of the authorised user and after power-on*[294] to demonstrate the correct operation of *parts of TSF*[295].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of *TSF data*[296].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of *TSF **implementation***[297].

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* [298] to the *TSF implementation*[299]

(2) *perturbation and environmental stress* [300] to the *TSF*[301]

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: “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

294 [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]*]

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

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

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

298 [assignment: *physical tampering scenarios*]

299 [assignment: l*ist of TSF devices/elements*]

300 [assignment: *physical tampering scenarios*]

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

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.

6.1.12 Import and use of Update Code Package

The TOE imports Update Code Package as user data objects with security attributes according to FDP_ITC.2, 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.

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* [302] 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*[303].

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*[304] 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.*

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

303 [assignment: *additional importation control rules*]

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

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
FMT_MSA.2 Secure security attributes

FCS_COP.1.1/VDSUCP The TSF shall perform *verification of the digital signature of the authorized issuer*[305] 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: 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
FMT_MSA.2 Secure security attributes

FCS_COP.1.1/DecUCP The TSF shall perform *decryption of authentic Update Code Package*[306] 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 – Use of Update code Package

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/UCP The TSF shall enforce the *Update SFP*[307] on

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

(2) **objects:** *Update Code Package*;

(3) **operations**: *import, execute*[308].

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/UCPThe TSF shall enforce the Update *SFP*[309] to objects based on the following:

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

305 [assignment: *list of cryptographic operations*]

306 [assignment: *list of cryptographic operations*]

307 [assignment: *access control SFP*]

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

309 [assignment: *access control SFP*]

(2) **objects**: *Update Code Package with security attributes issuer and Version Number*[310].

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 and store received Update Code Package if authenticity is successful verified according to FCS_COP.1/VDSUCP and decrypted according to FDP_ACC.1/UCP.*

(2)*[selection: Administrator, Update Agent] is allowed to execute stored Update Code Package if the Version Number of the Update Code Package is equal or higher than the Version Number of the TSF.*[311]

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 **rules**

(1) *none user is not allowed to store the Update Code Package if verification of authenticity according to FCS_COP.1/VDSUCP fails*;

(2) [*assignment: other rules, based on security attributes, that explicitly deny access of subjects to objects*].[312]

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***[313] the following objects: *received Update Code Package* [314].

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

310 [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*]

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

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

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

314 [assignment: *list of objects*]

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.

SFR	Dependencies of the SFR	SFR components
FAU_GEN.1	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_STG.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_STG.3	FAU_STG.1 Protected audit trail storage	FAU_STG.1
FCS_CKM.1/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/CLDH	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/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/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.1/ECKA-EG, 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] FMT_MSA.2 Secure security attributes	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 FMT_MSA.2
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/RSA, FCS_CKM.4

SFR	Dependencies of the SFR	SFR components
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/ECKA-EG	FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/HDM and FCS_COP.1/with FCS_CKM.5/ECKA-EG, FCS_CKM.4
FCS_CKM.5/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_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 MT_MSA.2 Secure security attributes	FCS_CKM.1/ECC, FCS_CKM.4, FMT_MSA.2
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 MT_MSA.2 Secure security attributes	FCS_CKM.1/RSA, FCS_CKM.4, FMT_MSA.2
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 FMT_MSA.2 Secure security attributes	Import of UCP decryption key as TSF data with confidentiality protection FPT_TCT.1/CK, FCS_COP.1/KU, FCS_CKM.4, FMT_MSA.2
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 FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
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 MT_MSA.2 Secure security attributes	Hash function do not use keys, it is used for FMT_MSA.2
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 MT_MSA.2 Secure security attributes	FCS_CKM.5/ECKA-EG, FCS_CKM.5/AES_RSA (note deterministic FCS_CKM.5 play the role of randomized FCS_CKM.1) FCS_CKM.4, FMT_MSA.2

SFR	Dependencies of the SFR	SFR components
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 MT_MSA.2 Secure security attributes	FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA FCS_CKM.4, FMT_MSA.2
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 MT_MSA.2 Secure security attributes	FCS_RBG_EXT.1 generates random strings as HMAC keys FCS_CKM.4 FMT_MSA.2
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 MT_MSA.2 Secure security attributes	FCS_CKM.1/ECC, FCS_CKM.1/RSA FCS_CKM.4 FMT_MSA.2
FCS_COP.1/KW	[FDP_ETC.1 Export of user data without security attributes, or FDP_ETC.2 Export 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/ECC, FCS_CKM.1/RSA FCS_CKM.4 FMT_MSA.2
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 FMT_MSA.2
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 FMT_MSA.2 Secure security attributes	FCS_CKM.1/SDEK, FCS_CKM.4, FMT_MSA.2
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 FMT_MSA.2 Secure security attributes	FCS_CKM.1/TCAP, FCS_CKM.1/PACE, FCS_CKM.4, FMT_MSA.2
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 FMT_MSA.2 Secure security attributes	FCS_CKM.1/TCAP, FCS_CKM.1/PACE, FCS_CKM.4, FMT_MSA.2

SFR	Dependencies of the SFR	SFR components
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 FMT_MSA.2 Secure security attributes	FPT_ISA.1/Cert (note keys are TSF data), FCS_CKM.4, FMT_MSA.2
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 MT_MSA.2 Secure security attributes	FPT_ISA.1/Cert (note keys are TSF data), FCS_CKM.4, FMT_MSA.2
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 FMT_MSA.2 Secure security attributes	Import of signature verification key of UCP issuer as TSF data FPT_ISA.1/Cert, FPT_TIT.1/Cert, FCS_CKM.4, FMT_MSA.2
FCS_RBG_EXT.1	FCS_RBG_EXT.2 or FCS_RBG_EXT.3	RCS_RBG_EXT.3
FCS_RBG_EXT.3	RCS_RBG_EXT.1	RCS_RBG_EXT.1
FCS_RBG_EXT.6	FCS_RBG_EXT.1, [FCS_RBG_EXT.2 or FCS_RBG_EXT.3]	RCS_RBG_EXT.1, RCS_RBG_EXT.3
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/KM
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_DAU.2/TS	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

SFR	Dependencies of the SFR	SFR components
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/UCP
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_API.1/TA	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	
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/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/Oper, FDP_ACC.1/Cluster, 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/Audit	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/CL	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

SFR	Dependencies of the SFR	SFR components
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, FPT_STM.1
FMT_SMF.1	No dependencies	
FMT_SMR.1	FIA_UID.1 Timing of identification	
FPT_ESA.1/CK	[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	FMT_MTD.1/KM, FMT_MSA.1/KM (note FPT_TDC.1 must be met by FPT_TDC.1.4)
FPT_ESA.1/CL	[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	FMT_MTD.1/CL, FMT_MSA.1/KM (note TSF data are exported to TOE samples)
FPT_FLS.1	No dependencies	
FPT_ISA.1/Cert	[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	FMT_MTD.1/RK, FMT_MSA.1/KM FPT_TDC.1/Cert
FPT_ISA.1/CK	[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	FMT_MTD.1/RK, FMT_MTD.1/KM FMT_MSA.1/KM FPT_TDC.1/Cert
FPT_ISA.1/CL	[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	FMT_MTD.1/CL FMT_MSA.1/KM (note TSF data are exported to TOE samples)
FPT_PHP.3	No dependencies	
FPT_STM.1	No dependencies	
FPT_TCT.1/CK	[FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]	FMT_MTD.1/CL

SFR	Dependencies of the SFR	SFR components
FPT_TCT.1/CL	[FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]	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/CK	[FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]	FMT_MTD.1/KM
FPT_TIT.1/Cert	[FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]	FMT_MTD.1/RK
FPT_TIT.1/CL	[FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]	FMT_MTD.1/CL
FPT_TIT.1/TC	No dependencies	
FPT_TST.1	No dependencies	
FRU_FLT.2	FPT_FLS.1 Failure with preservation of secure state	FPT_FLS.1
FTP_ITC.1	No dependencies	
FTP_ITC.1/CL	No dependencies	

Table 6: Dependency rationale

6.3.2 Security functional requirements rationale

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

	O.I&A	OT.AuthentTOE	O.Enc	O.DataAuth	O.RBGS	O.Tchann	O.TimeService	O.AccCtrl	O.SecMan	O.Audit	O.PhysProt	O.TST	O.SecUpCP	O,Cluster
FAU_GEN.1										x		x	x	
FAU_STG.1										x				
FAU_STG.3										x				
FCS_CKM.1/SDEK											x			
FCS_CKM.1/AES_RSA			x	x					x					
FCS_CKM.1/CLDH														x
FCS_CKM.1/DHE									x					
FCS_CKM.1/ECC			x	x					x					
FCS_CKM.1/ECDHE									x					
FCS_CKM.1/ECKA-EG			x	x					x					

	O.I&A	OT.AuthentTOE	O.Enc	O.DataAuth	O.RBGS	O.Tchann	O.TimeService	O.AccCtrl	O.SecMan	O.Audit	O.PhysProt	O.TST	O.SecUpCP	O,Cluster
FCS_CKM.1/PACE		x				x			x					
FCS_CKM.1/RSA			x	x					x					
FCS_CKM.1/TCAP		x				x			x					
FCS_CKM.4			x	x					x					
FCS_CKM.5/AES_RSA			x	x					x					
FCS_CKM.5/ECC			x	x					x					
FCS_CKM.5/ECKA-EG			x	x					x					
FCS_CKM.5/RSA			x	x					x					
FCS_COP.1/CDS-ECDSA		x		x			x							
FCS_COP.1/CDS-RSA		x		x			x							
FCS_COP.1/DecUCP													x	
FCS_COP.1/ED			x											
FCS_COP.1/Hash		x		x					x					
FCS_COP.1/HDM		x	x			x								
FCS_COP.1/HEM			x			x								
FCS_COP.1/HMAC				x										
FCS_COP.1/KU									x				x	
FCS_COP.1/KW									x				x	
FCS_COP.1/MAC				x										
FCS_COP.1/SDE											x			
FCS_COP.1/TCE						x								x
FCS_COP.1/TCM						x								x
FCS_COP.1/VDS-ECDSA				x										
FCS_COP.1/VDS-RSA				x										
FCS_COP.1/VDSUCP													x	
FCS_RBG_EXT.1					x				x					
FCS_RBG_EXT.3					x				x					
FCS_RBG_EXT.6					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										

Security requirements 6

	O.I&A	OT.AuthentTOE	O.Enc	O.DataAuth	O.RBGS	O.Tchann	O.TimeService	O.AccCtrl	O.SecMan	O.Audit	O.PhysProt	O.TST	O.SecUpCP	O,Cluster
FDP_ETC.1				x										
FDP_DAU.2/TS				x			x							
FDP_ETC.2			x	x										
FDP_ITC.2/UCP													x	
FDP_ITC.2/UD			x	x			x							
FDP_RIP.1/UCP													x	
FDP_SDC.1			x								x			
FIA_AFL.1	x													
FIA_API.1/CA		x				x								
FIA_API.1/PACE		x				x								
FIA_API.1/TA		x				x								
FIA_ATD.1	x							x						
FIA_UAU.1	x													
FIA_UAU.5	x													
FIA_UAU.6	x													
FIA_UID.1	x													
FIA_USB.1	x													
FMT_MOF.1	x					x				x				
FMT_MSA.1/KM			x	x		x	x	x	x					
FMT_MSA.2								x	x					
FMT_MSA.3/KM								x	x					
FMT_MTD.1/Audit										x				
FMT_MTD.1/CL														x
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_ESA.1/CL														x
FPT_FLS.1											x	x		
FPT_ISA.1/Cert	x			x					x					

	O.I&A	OT.AuthentTOE	O.Enc	O.DataAuth	O.RBGS	O.Tchann	O.TimeService	O.AccCtrl	O.SecMan	O.Audit	O.PhysProt	O.TST	O.SecUpCP	O,Cluster
FPT_ISA.1/CK									x					
FPT_ISA.1/CL														x
FPT_PHP.3											x			
FPT_STM.1							x			x				
FPT_TCT.1/CK									x				x	
FPT_TCT.1/CL														x
FPT_TDC,1/CK									x					
FPT_TDC.1/Cert	x			x					x					
FPT_TDC.1/UCP													x	
FPT_TIT.1/Cert	x			x					x				x	
FPT_TIT.1/CK									x					
FPT_TIT.1/CL														x
FPT_TST.1												x		
FRU_FLT.2											x			
FTP_ITC.1						x								
FTP_ITC.1/CL														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*, *Reference authentication 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.1/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/RSA 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 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 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/ECDHE, FCS_CKM.1/ECK-EG require key generation 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_DAU.2/Sig and FDP_DAU.2/TS requires the TSF to provide two different forms of digital signature mechanisms for cryptographic data authentication. The SFR FDP_DAU.2/Sig requires digital signature generation according to FCS_COP.1/CDS-RSA, FCS_COP.1/CDS-ECDSA for imported user data of the guarantor providing theses data. The SFR FDP_DAU.2/TS requires a time stamp service with signature key usage counter. The guarantor of the time stamp is the TOE itself.

- 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 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 security objective for the TOE O.RBGS “Random bit generation service” is met directly by the SFR FCS_RBG_EXT.6 as providing random bits generated by FCS_RBG_EXT.1 and RBG_EXT.3 as 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 and FIA_API.1/CA in case of TCAP.
- 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.TimeService” is directly met by FPT_STM.1 for the real time service and by by FDP_DAU.1 for time stamp service supported by FCS_COP.1/CDS_ECDSA resp. FCS_COP.1/CDS_RSA for signature creation, FDP_ITC.2 for user data import with security attributes indicating the signature key assigned by FMT_MSA.1/KM.

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

- 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 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.1/ECDHE require the TSF to implement key agreement function according to the assigned standards.
- The SFR FCS_CKM.5/AES, FCS_CKM.5/ECKA-EG and FCS_CKM.5/RSA 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_RBG_EXT.1 and FCS_RBG_EXT.3 requires the TSF to implement internally seeded random bit generator for key generation and key agreement functions.
- The SFR FCS_COP.1/AES 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 cryptographic key import with security attributes and protection of confidentialty 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.

The security objective for the TOE O.Audit “Audit for cryptographic TSF” is met by the following SFR:

- The SFR FAU_GEN.1 requires the TSF to generate the audit records of auditable events.
- The SFR FAU_STG.1 and SFR FAU_STG.3 requires the TSF to protect and to prevent loss of audit records.
- The SFR FMT_MTD.1/Audit restricts the ability to export and to delete exported audit records to an administrator. It prevents undetected deletion of audit records by generation of an audit record about deletion.
- The SFR FDP_DAU.2/TS requires the TSF to provide the capability to export audit trails signed and time stamped.
- The SFR FMT_MOF.1 requires the TSF to provide the capability to define the auditable events in clause (7), with key defined by Administrator according to.
- The SFR FPT_STM.1 requires the TSF to provide time stamps being part of the audit records.

The security objective for the The security objective for the TOE O.Cluster “Cluster” is met by the following SFR:

- The SFR FMT_MTD.1/CL restricts the management of TSF data Authentication Data Records and cryptographic key by initiating the cluster to an administrator, and export and import of TSF data to the Application.
- The SFR FPT_ESA.1/CL and FPT_ISA.1/CL require that export and import of TSF data is perform with security attributes.
- The SFR FPT_TCT.1/CL requires protection of confidentiality and the SFR FPT_TIT.1/CL the protection of integrity of the TSF data when transferred from master CSP to slave CSP trough the trusted channel according to FTP_ITC.1/CL.
- The SFR FCS_CKM.1/CLDH requires the TSF to agree on cryptographic keys as defined in [30].

TOE O.TST “Self-test” is directly met by the SFR FPT_TST.1 and TPT_FLS.1. The TSF shall l preserve a secure state when the following types of failures occur: self test fails, 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, or manipulation and physical probing detected and secure state is reached as response (FPT_PHP.3).

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 security objective for the TOE O.SecUpCP “Secure download and authorized use 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 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

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

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

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

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

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

[6] Federal Information Processing Standards Publication 197 (FIPS PUB 197). Advanced Encryption Standard (AES), 2001

[7] ISO/IEC 18033-2. Information Technology – Security technique – Part 2: Asymmetric Ciphers, 2006

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

[9] ANSI X9.63. Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2011

[10] BSI, Elliptic Curve Cryptography, BSI Technical Guideline TR-03111, Version 2.1, 1.6.2018, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_pdf.html

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

[12] ISO 7498-2:1989 Information processing systems – Open Systems Interconnection – Basic Reference Model-Part 2: Security Architecture

[13] ISO/IEC 21827:2008 Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)

[14] BSI. 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

[15] M. Lochter, J. Merkle. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation (RFC5639), 2010. Available at http://www.ietf.org/rfc/rfc5639.txt.

[16] National Institute of Standards and Technology. FIPS PUB 186-4: Digital Signature Standard (DSS). 2013

[17] National Institute of Standards and Technology. FIPS PUB 180-4: Secure Hash, Standard (SHS). 2012.

[18] ISO/IEC. ISO/IEC 9797-2:2011 – Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function. 2011

[19] Adi Shamir. “How to Share a Secret”. In: Commun. ACM 22.11 (1979), pp. 612–613.

[20] BSI Technical Guideline Cryptographic Mechanisms: Recommendations and Key Lengths, TR-02102, 2017

[21] NIST Special Publication 800-56A Revision 2 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, May 2013

[22] RFC5246 The Transport Layer Security (TLS) Protocol Version 1.2

[23] RFC2631 Diffie-Hellman Key Agreement Method

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

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

[26] National Institute of Standards and Technology Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication May 2005

[27] National Institute of Standards and Technology Special Publication 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November, 2007

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

[29] National Institute of Standards and Technology. Special Publication 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping. 2012.

[30] BSI, Signature Creation Device (SCDev)

[31] Technical Guideline BSI TR3-03151 Secure Element API (SE API), Version 1.0, 5. Juni 2018

[32] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 5: Anwendungen der Secure Element API, Stand 2018, Datum: 5. Juni 2018

[33] BSI AIS 20/31, A proposal for: Functionality classes for random number generators, Version 2.0, 2011

[34] SOG-IS Crypto Working Group: SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.0, May 2016

[35] Joint Interpretation Library: Security requirements for post-delivery code loading, Version 1.0, February 2016

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

[37] Joint Interpretation Library: Guidance for smartcard evaluation, Version 2.0, February 2010

Keywords and Abbreviations

Term	**Description**
authentication reference data	data used by the TOE to verify the authentication attempt of a user
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 and holding the signature private key for signing the update code package and corresponding to the public key implemented in the TOE for verification of the update code package; the issuer is typically the TOE manufacturer
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 [1], paragraph 97)
update code package	code if implemented changing the TOE implementation at the end of the TOE life time
verification data	data used by the user to authenticate themselves to the TOE

Table 8: Glossary

Acronym	***Term***
A.xxx	Assumption
CC	Common Criteria
CSP	cryptographic service provider component
n. a.	Not applicable
PACE	Password Authenticated Connection Establishment,
O.xxx	Security objective for the TOE
OE.xxx	Security objective for the TOE environment
OSP.xxx	Organisational security policy
SAR	Security assurance requirements
SCM	Secure cryptographic mechanisms
SFR	Security functional requirement
T.xxx	Threat
TOE	Target of Evaluation
TSF	TOE security functions

Table 9: Abbreviations