CryptoServer CSPLight

Security Target Lite for CryptoServer CSPLight

utimaco®

Imprint

Copyright 2021	Utimaco IS GmbH Germanusstr. 4 52080 Aachen Germany
Phone	+49 (0)241 / 1696-200
Fax	+49 (0)241 / 1696-199
Internet	http://hsm.utimaco.com
e-mail	hsm@utimaco.com
Document Number	2019-0029
Document Version	1.0.2
Date	18th March 2021
Status	Released

Table of Contents

1 Introduction

1.1 Change History

Version	Date	Description
1.0.0	19th February 2021	First release of Security Target Lite, based on full Security Target with same version
1.0.1	23rd February 2021	▪One item in Table 1 TOE deliverables is updated
1.0.2	18th March 2021	▪Guidance document versions are updated in Table 1 TOE deliverables ▪CryptoServer_ErrorReference.pdf is removed from Table 2: List of Non-TOE Hardware/Software/Firmware

1.2 Document Introduction

This Security Target (ST) was developed based on the Protection Profile Configuration "Cryptographic Service Provider Light – Time Stamp Service, Audit and Clustering" [PPC-CSPLight-TS-Au-Cl], which uses the Common Criteria Protection Profile "Cryptographic Service Provider Light - BSI-CC-PP-0111-2019" [PP-CSPLight] as base Protection Profile and includes two Protection Profile-Modules:

1) Protection Profile-Module CSPLight Clustering [PPM-Cl] which is contained in the [PPC-CSPLight-TS-Au-Cl] Protection Profile Configuration document,
2) Protection Profile-Module CSPLight Time Stamp Service and Audit [PPM-TS-Au] which is contained in the [PPC-CSPLight-TS-Au-Cl] Protection Profile Configuration document.

The following subchapters provide some information for the further understanding of this document and introduce the reader to some used conventions.

1.2.1 Acknowledgement

The author would like to acknowledge the significant contributions of the Protection Profile Configuration "Cryptographic Service Provider Light" [PP-CSPLight], the Protection Profile-Module "CSPLight Clustering" [PPM-Cl] and Protection Profile-Module "CSPLight Time Stamp Service and Audit" [PPM-TS-Au].

1.2.2 Notations

The notation, formatting, and conventions used in this ST are consistent with those used in the Common Criteria, Version 3.1, Revision 5, April 2017 [CC1], [CC2], [CC3].

The Common Criteria allow several operations to be performed on security requirements: refinement, selection, assignment and iteration are defined in Section C.2 of [CC1].

- **Refinement:** The refinement operation is used to add details to a requirement, and thus further restricts a requirement.
- **Selection:** The selection operation occurs where a given component contains an element where a choice from several items has to be made by the PP/ST author. Whenever an element within a PP contains a selection, the PP author could leave the selection uncompleted, restrict the selection by removing some of the choices (but leaving two or more) or complete the selection by choosing one or more items. Whenever an element within an ST contains a selection, the ST author has to complete that selection. If a selection was already completed in the PP, the PP text is shown in *non-underlined italic letters*. If a selection is completed by the ST author the text is shown in *underlined italicized letters*.
- **Assignment:** The assignment operation is used to assign a specific value to an unspecified parameter (e.g. the length of a password). Whenever an element in a PP contains an assignment, the PP author could leave the assignment uncompleted, complete the assignment, narrow the assignment, to further limit the range of values that is allowed or transform the assignment to a selection, thereby narrowing the assignment. Whenever an element in an ST contains an assignment, the ST author has to complete that assignment, the PP text is also given within a footnote where the original text is given. If an assignment was already completed in the PP, the PP text is shown in *non-underlined italic letters*. If an assignment is completed by the ST author the text is shown in *underlined italicized letters*.
- **Iteration:** The iteration operation is used when a component is repeated with varying operations. Iterations within Base PP [PP-CSPLight] and the PP Modules [PPM-CI] or [PPM-TS-Au] are denoted by showing a slash “/” and an iteration indicator after the CC component identifier. Iterations within the ST are denoted by showing a double-slash “//” and an iteration indicator after the PP component and the CC component, respectively, identifier.

1.2.3 Abbreviations

Assumptions, threats, organisational security policies and security objectives (for TOE and environment) are assigned with a unique label for easy reference as follows:

T.<xxx>	Threats
P.<xxx>	Organisational security policies
A.<xxx>	Assumptions about the TOE security environment
OT.<xxx>	Security objectives for the TOE
OE.<xxx>	Security objectives for the operating environment

1.2.4 References

References in this document are specified with the help of brackets (e.g.: [<Reference>]). A list of all referenced documents can be found in chapter 10.2 “References”.

1.2.5 Terminology

A complete list of used terms and abbreviations can be found in chapter 10.1 “Glossary and Acronyms”. Thereby Common Criteria and IT technology terms relevant for this ST are described. Most of the definitions are taken out of the Base PP [PP-CSPLight] as well as from the Common Criteria.

2 Security Target Introduction

2.1 ST and TOE Reference

Title:	Security Target Lite for CryptoServer CSPLight
ST Version:	1.0.2
ST Date:	18th March 2021
Author:	Utimaco IS GmbH
Developer:	Utimaco IS GmbH
Product:	CryptoServer CSPLight
TOE-name long:	CryptoServer CSPLight
TOE-name short:	CryptoServer CSPLight
TOE-version:	CryptoServer CSPLight 1.0.0
Product Type:	Cryptographic module
Certification Authority:	Federal Office for Information Security – BSI Germany
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 [CC1], [CC2], [CC3]
Keywords:	Cryptographic module, Cryptographic Service Provider, electronic signature, digital signature, secure messaging, trusted channel, Cash Box Register, Kassensicherungsverordnung

2.2 Related Documents

All related documents can be found in chapter 10.2 “References”.

2.3 Organisation

The main chapters of this ST are Security Target Introduction with the description of the TOE (Target of Evaluation), Conformance claims, Security problem definition, Security objectives, Extended components definition, Security requirements and TOE summary specification as well as annexes. This document is structured according to the Security Target requirements of [CC1].

- **Chapter 2:** The TOE description provides general information about the TOE, its generic structure and boundaries.
- **Chapter 3:** The ST conformance claims section states conformance to Protection Profiles.
- **Chapter 4**: The security problem definition describes security aspects of the environment in which the TOE is intended to be used and the manner in which it is intended to be employed. The security problem definition includes threats relevant to secure TOE operation (section 4.3), organisational security policies (section 4.4), which must be complied by the TOE, and assumptions regarding the TOE's intended usage and environment of use (section 4.5).

- **Chapter 5:** The statement of security objectives defines the security objectives for the TOE (section 5.1) and for its environment (section 5.2). The rationale (section 8.1) presents evidence that the security objectives satisfy the threats and policies.
- **Chapter 6:** This chapter defines the extended components.
- **Chapter 7:** The security requirements are subdivided into TOE Security Functional Requirements (section 7.2) and Security Assurance Requirements (section7.3).
- **Chapter 8:** The rationale (section 8.2) explains how the set of requirements is complete relative to the security objectives.
- **Chapter 9:** The TOE summary specification provides a description of the TOE security functionality in narrative form.

The **annex** offers a glossary and acronyms as well as relevant references.

2.4 TOE Overview

The Fiscal Code of Germany [FCG] section146a requires an electronic record-keeping system to protect the accounts and the records by a certified technical security system, for later cash inspections. The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik - BSI) defines requirements for the components of the certified technical security system, i. e. for the security module in form of Common Criteria Protection Profiles, and for the storage medium and the unified digital interface in form of Federal Office's technical guidelines (cf. [KSV] section 5). The security module consists of the Security Module Application and the Cryptographic Service Provider or Cryptographic Service Provider Light (CSPLight). The TOE implements such a CSPLight and the Security Target in hand defines security requirements of the CSPLight based on the Protection Profile Configuration [PPC-CSPLight-TS-Au-Cl].

Although it is first emerged together with the electronic record-keeping system application, the CSPLight is a generic cryptographic service provider which can also provide its services to potential other Security Module Applications (SMA). In the case of the ERS, the Security Module Applications called Security Module Application for Electronic Record-keeping Systems (SMAERS) which fulfills the security requirements from [PP-SMAERS] as well as "Technische Richtlinie BSI TR-03153 - Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme" [TR-03153].

Major security functionalities of the TOE are:

- Cryptographic key management: *key generation, key derivation, key agreement, key import, key export, key destruction;*
  - *AES key generation, derivation for 128 bits and 256 bits of key lengths,*
  - *ECC key pair generation with brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, Curve P-256, Curve P-384 and Curve P-521 elliptic curves,*
  - *ECC key pair derivation with the elliptic curve of brainpoolP256r1,*
  - *RSA key generation of 2048 bits, 3072 bits, or 4096 bits of modulus size,*
  - *Elliptic Curve Diffie-Hellman ephemeral key agreement for AES-128,*
  - *ECKA-EG key generation (brainpoolP256r1) with ECC encryption with 256 bits,*
  - *ECKA-EG key derivation (brainpoolP256r1) for AES-128,*
  - *key destruction by zeroization,*
- Random number generation for internal purposes, e. g. for key generation, but also provided as a security service of the TOE,

- Digital signature generation with time stamp and key usage counter;
  - *ECDSA signature generation and verification with brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, Curve P-256, Curve P-384 and Curve P-521 elliptic curves,*
  - *RSA digital signature generation and verification using 2048 bits, 3072 bits, and 4096 bits of keys,*
- Confidentiality and integrity protection of stored user data and TSF data;
  - *Data encryption and decryption using AES-128 and AES-256,*
  - *Data integrity protection – MAC using AES-128 and AES-256,*
- Authentication and attestation of the TOE to external entities,
- PACE authentication to Security Module Application (SMA),
- Chip Authentication with establishment of a trusted channel,
- Certificate based Terminal Authentication,
- User Identification and authentication services,
- certificate management;
  - *export of a public key in form of a certificate,*
  - *Import of a certificate for a public key,*
  - *Import and deletion of a public key of a trusted CA Root key (root certificate),*
- Security management, time stamp and security audit,
- Secure SW update of the TOE,
- Clustering of the TOE samples.

2.5 TOE Description

This chapter contains the following sections:

- TOE configuration and TOE environment (section 2.5.1)
- TOE boundary (section 2.5.2)

2.5.1 TOE Configuration and TOE Environment

The TOE, CryptoServer CSPLight, is a cryptographic service provider which is composed of software modules running on a dedicated server platform, provided by Utimaco. The server together with the TOE form the network-attached appliance CryptoServer CSPLight as seen in Figure 1. The server itself is not part of the TOE, but it is seen as a hardware platform where the TOE runs on, and where the TOE relies on functionality provided e.g. by the operating system of the server. The server furthermore fulfills also the requirements in the Appendix “Appendix: Operational Requirements for CSPLight” of [PP-SMAERS]. CryptoServer CSPLight provides the security services as required by the Security Module Applications, such as SMAERS, which is either integrated into a cash register or running on a back-office server to which cash registers are connected. The TOE provides also time services, time stamp services and secure auditing services.

Figure 1: CryptoServer CSPLight

When the application component (SMA) is SMAERS, the main function of the TOE is to create digital signatures over the transaction data imported from the cash registers, provide time stamp service, securely store and manage the signature keys and manage a signature counter enumerating the signatures created for Log messages. The signing and time stamping service provided by the TOE is required by the SMAERS to generate verifiable sequences of transaction data and log messages for cash inspection (cf. [FCG] section146b).

The TOE and the SMA are physically separated components interacting with each other through a trusted channel. The application component (in client role) uses the security services of the TOE (in server role). For this purpose, CryptoServer CSPLight provides a cryptographically protected trusted channel to any SMA via the PACE protocol as depicted in Figure 2. The PACE Protocol is used to setup a MAC Key and an encryption key in order to sign and optionally encrypt all messages transferred from and to the TOE. CryptoServer CSPLight supports also periodic transfer of log messages to an external storage medium.

In order to enable the set-up of a CSPLight-cluster of TOE samples for scalability of performance and availability of security services, the TOE provides the functionality to synchronize a Slave-CSPLight with a Master-CSPLight in a secure manner (see Figure 2). For this, the TOE provides security functionality for an encrypted and integrity-protected export of the sensitive data from a TOE in the role of a Master-CSPLight, as well as the security functionality for decryption and integrity-verification during import of these data into a TOE which is in the role of a Slave-CSPLight.

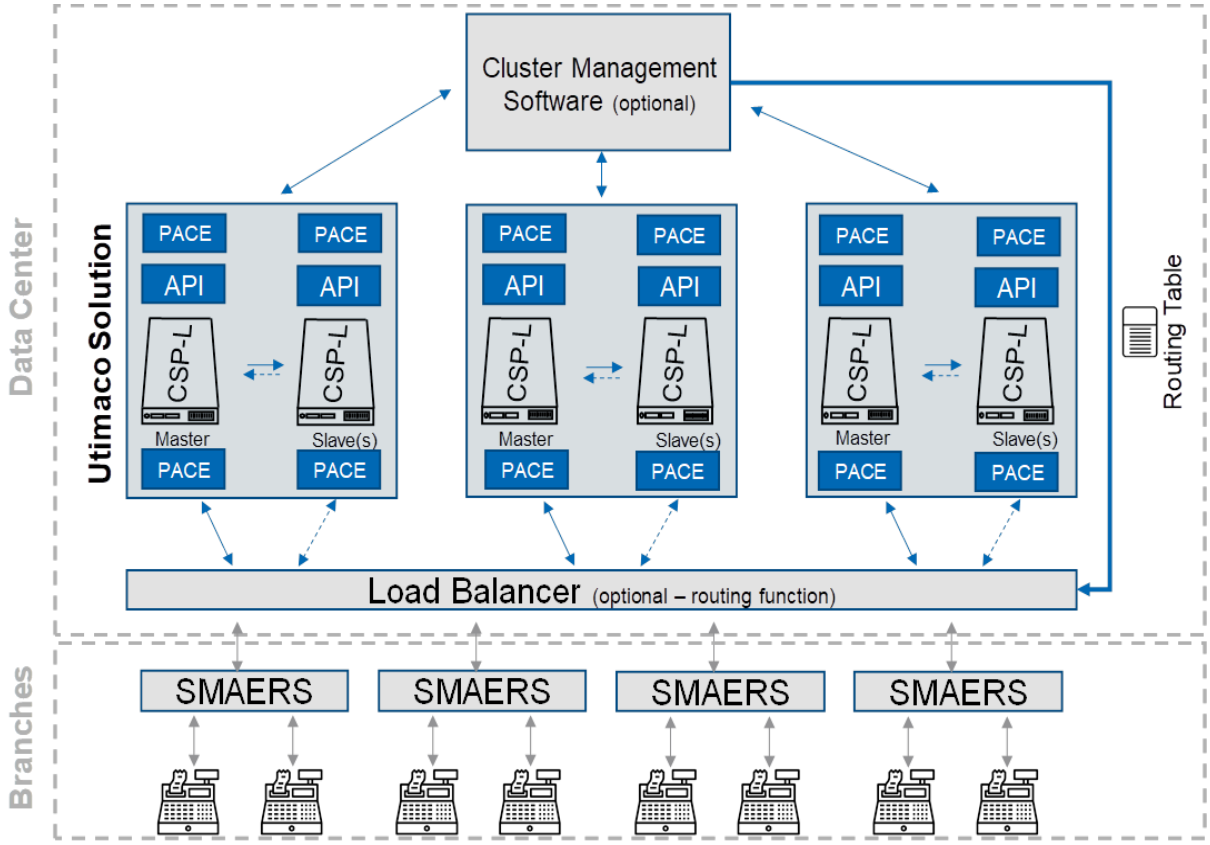


Figure 2 Architectural Overview of the TOE in a technical solution environment for SMAERS

In Figure 2, a technical solution environment involving clustering of the TOE for SMAERS is demonstrated. The same solution can be considered for other SMAs as well. CSP-L in the figure represents CryptoServer CSPLight.

The TOE furthermore provides additional TOE security functionality in order to enable time service, time stamp service and secure auditing service. The time service allows the user to query the internal time and hence provides users with reliable time as known to the TOE. The time stamp service provides evidence that user data were presented to the TOE and exported audit data (transaction logs in the sense of the ERS for cash inspections) were generated at certain point in time and in a verifiable sequence. The validity and authenticity of these user data and audit records can be verified.

The audit functionality generates audit records on selected user activities and security events of the TOE. The audit records can be exported in a signed and time stamped form.

Cryptographic functions, key and certificate management functions, and other functions of the TOE that can be called by a SMA are implemented as a REST API. Cryptographic keys, which are used by functions that are available to SMA, are generated, stored and used inside the TOE. The TOE furthermore provides the security functionality for a secure update of its source code (Update Code Package), in encrypted and integrity-protected form.

2.5.2 TOE Boundary

The overview of all deliverables associated to the TOE are listed in Table 1. The developer documentation in the list describes the Application Protocol Interfaces (APIs), the internal versions of which are assigned to the TOE version 1.0.0.

TOE deliverable	Type/Form, Name		Exact reference
Software	SW	CryptoServer CSPLight	CryptoServer CSPLight, Version 1.0.0
Guidance Documentation	Doc	CryptoServer CSPLight Betriebsanleitung	Dokument No. 2020-0011, Version 1.0.1
	Doc	CryptoServer CSPLight Administration Manual	Document No. 2020-0016, Version 1.0.0
Developer Documentation	Doc	CryptoServer CSPLight Clustering API	Document No. 2020-0022, Version 1.4.0
	Doc	CryptoServer CSPLight Core API	Document No. 2020-0021, Version 1.6.0
	Doc	CryptoServer CSPLight Crypto API	Document No. 2020-0020, Version 1.2.0
	Doc	CryptoServer CSPLightUI-Logic-API	Document No. 2020-0019, Version 1.5.0

Table 1: TOE deliverables

2.6 Required Non-TOE Hardware/Software/Firmware

The following hardware and software which do not belong to the TOE is required for the operating environment and is always delivered together with the TOE:

Additional deliverables	Type/Form		Exact reference
CryptoServer CSPLight Server	HW	19” appliance (together with rack rails)	CryptoServer CSPLight Server
CryptoServer CSPLight System software	SW	– Operating system of Server – Operating system of the Virtual Machines – Other software tools	CryptoServer CSPLight System SW 1.0.0.
PIN Pad	HW	smartcard reader with keypad	Utimaco cyberJack one
Ten Smart cards	HW	Ten smartcards are provided to support the administration of the CryptoServer CSPLight.	Javacard J2A081 Javacard J2E081
Network cable	HW	1.5 – 2m length network cable to connect the server to a terminal application (accessed via SSH) on a host computer.	
Two power supply cables	HW		
Two rack rails	HW		
Four physical keys	HW	Keys to lock the front lid of the CryptoServer CSPLight server	
One cable management arm	HW		
License information document in PDF format	DOC	CryptoServer – License Texts/Utimaco IS GmbH	2009-0005
Declaration of Conformity	DOC	Declaration_of_Conformity_CSPLight.pdf	

Table 2: List of Non-TOE Hardware/Software/Firmware

3 Conformance Claims

3.1 CC Conformance Claim

This ST claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017 [CC1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017 [CC2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017 [CC3]

as follows

- **CC Part 2 extended**
- **CC Part 3 conformant**

The

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

  has to be taken into account.

3.2 PP Claim

This Security Target claims strict conformance to Common Criteria Protection Profile Configuration “Cryptographic Service Provider Light – Time Stamp Service and Audit – Clustering” [PPC-CSPLight-TS-Au-Cl], which uses the Common Criteria Protection Profile “Cryptographic Service Provider Light - BSI-CC-PP-0111-2019” [PP-CSPLight] as base Protection Profile.

3.3 Package Claim

The assurance level for this Security Target is EAL2 augmented with ALC_CMS.3 and ALC_LCD.1.

3.4 Conformance Rationale

This Security Target claims strict conformance with the Protection Profile Configuration [PPC-CSPLight-TS-Au-Cl] which consists of one Base-PP together with two PP-Modules.

- Base-PP: Common Criteria Protection Profile Cryptographic Service Provider Light, version 1.0 [PP-CSPLight]
- PPM-Cl: Protection Profile-Module CSPLight Clustering, version 1.0 [PPM-Cl], defined in chapter 3 to 9 of the Protection Profile Configuration document [PPC-CSPLight-TS-Au-Cl].
- PPM-TS-Au: Protection Profile-Module CSPLight Time Stamp Service and Audit, version 1.0 [PPM-TS-Au]

4 Security Problem Definition

This chapter contains the following sections:

- Assets (section 4.1)
- Subjects (section 4.2)
- Threats (section 4.3)
- Organisational Security Policy (section 4.4)
- Assumptions (section 4.5)

4.1 Assets

The assets of the TOE are

- user data, whose integrity and confidentiality shall be protected,
- cryptographic services and keys which shall be protected against unauthorized use or misuse, and whose integrity shall be protected
- update code packages (UCP), whose integrity and confidentiality shall be protected.
- additional TSF-data (e.g. security flags), whose integrity and/or confidentiality shall be protected,
- other TOE resources, whose unauthorized use and misuse shall be prevented
- The TSF data the security attributes of the known users and the cryptographic keys with their security attributes transferred between Master-CSPLight and Slave-CSPLight (for clustering purposes) shall be protected.
- user data and time stamps shall be integrity-protected,
- time services which time base shall be protected against manipulation.

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. The audit records are TSF data generated by the TSF and exported to the user.

4.2 Subjects, Objects and Security Attributes

4.2.1 Users and subjects

The TOE knows external entities (users) as

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

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

The TOE communicates with

- human user through a secure channel,
- application component through a secure channel,

- remote entities over a trusted channel using cryptographic mechanisms including mutual authentication,
- cluster-CSPLight in encrypted and integrity-protected form.

The subjects as active entities in the TOE perform operations on objects. Objects obtain their associated security attributes from the authenticated users, or the security attributes are defined by default values.

4.2.2 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 that are imported and stored in the TOE until they are used to create an updated version of the CSPLight. 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, or the security attributes of the known users and the cryptographic keys with their security attributes transferred between Master-CSPLight and Slave-CSPLight.

Cryptographic keys, including the keys used by the time stamp service and clustering operations, are objects of the key management.

4.2.3 Security attributes

A Role is a set of certain access rights and permissions. By defining roles, and associating users with roles (“a user or a subject takes a role”) it is immediately clear, what access rights and permissions this user is granted.

The security attributes of users 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 TOE knows the following roles that can be taken by a user or a subject:

- **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**: a successfully authenticated user in this role is allowed to access the TOE in order to perform management functions, including device management, user management and key management. It is taken by a human user or a subject acting on behalf of a human user after successful authentication as an Administrator.
- **Auditor**: a successfully authenticated user in this role is allowed to configure the audit functionality, review audit data and export and clear audit trails.
- **Timekeeper**: a successfully authenticated user in this role is allowed to adjust the internal time and configure the secure NTP service.
- **Key Owner**: a successfully authenticated user in this role is allowed to perform cryptographic operation with his 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 being authenticated as a human user (e. g. exporting and importing of wrapped keys). This role may be assigned to an entity communicating through a trusted channel (which requires assured identification of its end points), as done e. g. by the SMAERS.
- **Cluster-CSPLight**: another TOE sample in the same cluster with the TOE with security attribute *Master-CSPLight* or *Slave-CSPLight*. This role is bound to the communication through the trusted channel between cluster CSPLights established by the administrator.

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

- human user authentication by knowledge, where the authentication verification data is a password and the authentication reference data is the hash value of the password,
- cryptographic entity authentication mechanisms where the authentication verification data is a PIN value and the authentication reference data is a PUK value.

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

The TOE is delivered with initial Authentication Data Records for administrator roles. The roles are not exclusive, i. e. a user or subject may be in more than one role, e. g. a human user may claim the Administrator and Key Owner role at the same time.

Cryptographic keys have at least the security attributes

- Key identity, i. e. an attribute that uniquely identifies the key,
- Key Owner, i. e. the identity of the owner this key is assigned to,
- Key type, i. e. whether the key is as secret key, a private key, or a public key,
- Key usage type, an attribute that identifies the cryptographic mechanism or services the key can be used for. For example, a private signature key may be used by a digital signature-creation mechanism (cf. FCS_COP.1/CDS-ECDSA or FCS_COP.1/CDS-RSA); and depending on the corresponding certificate (cf.

FDP_DAU.2/Sig) be used for signing data, or for device-attestation,

- Key access control attributes, i. e. a list of combinations of the identity of the user, the role for which the user is authenticated, and the allowed key management functions or cryptographic operations. This includes that
  - the import of the key is allowed or forbidden,
  - the export of the key is allowed or forbidden,
  - Clustering: transfer of the key in a cluster of TOE samples (i.e. export by TOE as Master-CSPLight and import by TOE as Slave-CSPLight) is allowed or forbidden.

and may have further security attributes

- Key validity time period, i. e. the time period for operational use of the key: The key must not be used before or after a defined time slot. Note that exceptions could be required: For example, it might be required that an expired root certificate can be updated with a valid link certificate to a new valid root certificate.

The Update Code Package (UCP) has at least the security attributes

- issuer of the UCP,
- version number of the UCP.

4.3 Threats

T.DataCompr Compromise of communication data

An unauthorized entity gets knowledge of information that are stored on media controlled by the TSF, or an unauthorized entity gets knowledge of information that are transferred between the TOE and an authenticated external entity.

T.DataMani Unauthorized generation or manipulation of communication data

An unauthorized entity generates or manipulates user data that are stored on media controlled by the TSF or transferred between the TOE and an authenticated external entity, and manipulates such data so that they are accepted as valid by the recipient.

T.Masqu Masquerade authorized user

A threat agent masquerades 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

An attacker gets unauthorized access to security services of the TOE.

T.PhysAttack Physical attacks

An attacker gets physical access to the underlying hardware platform that the TOE is running on 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 and installs a faulty update code package. Thus attacks against the integrity of the TSF implementation, and against the confidentiality and integrity of user data and TSF data becomes possible.

4.4 Organisational Security Policies

OSP.SecCryM Secure cryptographic mechanisms

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

OSP.SecService Security services of the TOE

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

OSP.KeyMan Key Management

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

OSP.TC Trust centre

Trust centres provide secure certificates for trustworthy certificate holders 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. In particular, this includes key management and attestation.

OSP.Update Authorized Update Code Packages

Update Code Packages are delivered in encrypted form, and are signed by the authorized issuer. The TOE verifies the authenticity of the received Update Code Package using the CSPLight before storing any update data in the TOE. The TOE restricts the storage of authentic Update Code Package to authorized users.

OSP.Cluster Cluster of the TOE Samples

The administrator establishes and manages a cluster of multiple TOE samples for secure transfer of the security attributes of the known users and the cryptographic keys as necessary for scalability of performance and availability of security services.

OSP.TimeService Time Service and Time stamp service

The TOE provides non-cryptographic time service and cryptographic time stamp service for user data and TSF data. The time stamp service provides evidence that user data were presented to the TSF and exported audit data were generated at certain point in time and in a verifiable sequence.

OSP.Audit Audit for key management and cryptographic operations

The TOE provides security auditing related to activities controlled by the TSF and security critical events. 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 select auditable events.

4.5 Assumptions

A.SecComm Secure communication
Remote entities support trusted channels by cryptographic mechanisms. The operational environment shall protect the local communication channels by trusted channels using cryptographic mechanisms, or by secure channels using non-cryptographic security measures. The operational environment must be subject to a security audit that verifies that the communication between the TOE and the application is indeed protected.

A.ClusterAppl Cluster management by application
The application using the security services of the TOE transfers security attributes of the known users and cryptographic keys with their security attributes between Master-CSPLight and Slave-CSPLight as necessary for scalability of performance and availability of security services.

5 Security Objectives

This section identifies and defines the security objectives for the TOE and its operational environment.
Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organisational security policies and assumptions.

5.1 Security Objectives for the TOE

The following security objectives describe security functions to be provided by the TOE.

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

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

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 provides cryptographically secure random bit generation for the users.

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

Note that the TSF can establish the trusted channel by means of secure cryptographic mechanisms only if the other external entity supports these secure cryptographic mechanisms as well. If the trusted channel cannot be established by means of secure cryptographic mechanisms – i.e . due to missing security functionality on the user side – then the operational environment shall provide a secure channel that protects the communication by non-cryptographic security mechanisms, cf. A.SecComm and OE.SecComm.

O.I&A Identification and authentication of users
The TOE shall uniquely identify users and verify the claimed identity of the user before providing access to any controlled resources; The TOE shall authenticate IT entities using secure cryptographic mechanisms.

O.AccCtrl Access control
The TOE provides access control of security services, operations on user data, and 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 certificates. The TSF generates, derives, agrees, imports and exports cryptographic keys as a security service for users and for internal use. The TSF shall destruct unprotected secret or private keys in such a way that any previous information content of the resource is made unavailable.

O.TST Self-test
The TSF performs self-tests during initial start-up, and after power-on. The TSF enters a secure state if the self-test fails or if attacks are detected. It relies on the underlying hardware platform and operating system (cf. OE.SecPlatform) to implement this functionality.

O.SecUpCP Secure import of Update Code Packages
The TSF verifies the authenticity of a received encrypted Update Code Package, decrypts the Update Code Package if it is verified to be authentic, and installs it after verifying that it is suitable for the TOE and does not downgrade the TOE's firmware to a previous version.

O.Cluster Cluster
The TSF supports cluster of TOE samples by secure transfer of the security attributes of the known users and the cryptographic keys with their security attributes between Master-CSPLight and Slave-CSPLight in encrypted and integrity protected form.

O.Audit Audit
The TSF provides security auditing of selected user activities controlled by the TSF and security critical events. The Administrator is allowed to select auditable events, to manage the audit functionality and the export of audit records.

O.TimeService Time services
The TOE provides an internal time service and time stamp service for the user.

5.2 Security Objectives for the Operational Environment

The following security objectives relate to the TOE environment.

OE.CommInf Communication infrastructure
The operational environment shall provide a public key infrastructure for entities in the relevant communication networks. Trust centres must generate secure certificates for trustworthy certificate holders with correct security attributes. They must distribute their certificate signing public key securely such that a verification of the digital signature of the generated certificates is possible. Trust centres should further operate 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 centres.

OE.SecManag Security management

The operational environment shall implement appropriate security management functionality for secure use of the TOE. This includes user management as well as key management. It ensures secure key management outside of the TOE and uses the trust centre's services to determine the validity of certificates. Cryptographic keys and cryptographic key components shall be assigned to the secure cryptographic mechanisms they are intended to be used with, and to the entities authorized for their use.

OE.SecComm Protection of communication channel

Remote entities shall support establishing trusted channels with the TOE by using cryptographic mechanisms. The operational environment shall protect the local communication channels by trusted channels using cryptographic mechanisms, or by secure channels using non-cryptographic security measures. In the latter case, the operational environment must be subject to a security audit that verifies that the communication between the TOE and the application is indeed protected.

OE.SUCP Signed Update Code Packages

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

OE.SecPlatform Secure Hardware Platform

The TOE runs on a secure hardware platform. The hardware platform and its operating system support the implementation of the TSF; this in particular includes the protection of the confidentiality and integrity of user data, TSF data and its correct operation against physical attacks and environmental stress.

OE.ClusterCtrl Control of the cluster

The administrator establishes and manages a cluster only of trustworthy samples of the TOE as necessary for scalability of performance and availability of security services.

OE.TSFdataTrans Transfer of TSF data within the CSPLight cluster

The administrator and the application using the security services of the TOE transfer the security attributes of the known users and the cryptographic keys with their security attributes between Master-CSPLight and Slave-CSPLight as necessary for scalability of performance and availability of security services.

OE.Audit Review and availability of audit records

The Administrator shall ensure the regular audit review and the availability of exported audit records.

OE.TimeSource External time source

The operational environment provides reliable external time source for the adjustment of the TOE internal time source.

6 Extended Components Definition

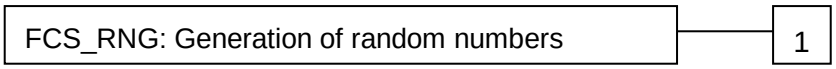
6.1 Generation of Random Numbers (FCS_RNG)

This family describes the functional requirements for random number generation used for cryptographic purposes.

Family behaviour:

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

Component levelling:



Management:FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no auditable events foreseen.

FCS_RNG.1 Generation of random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

6.2 Cryptographic key derivation (FCS_CKM.5)

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

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

Management: FCS_CKM.5

There are no management activities foreseen

Audit: FCS_CKM.5

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ ST: a) Minimal: Success and failure of the activity. b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).

FCS_CKM.5 Requires the TOE to provide key derivation.

FCS_CKM.5 Cryptographic key derivation

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.5.1	The TSF shall derive cryptographic keys [assignment: key type] from [assignment: input parameters] in accordance with a specified cryptographic key derivation algorithm [assignment: cryptographic key derivation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

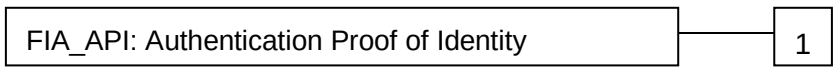
6.3 Authentication Proof of Identity (FIA_API)

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: FIA_API.1

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

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

Audit: FIA_API.1

There are no auditable events foreseen.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

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

Family Behaviour

This family requires confidentiality protection of exchanged TSF data.

Component levelling:

FPT_TCT: Inter-TSF TSF data confidentiality transfer protection	1

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

Management: FPT_TCT.1

There are no management activities foreseen.

Audit: FPT_TCT.1

There are no auditable events foreseen.

FPT_TCT.1 TSF data confidentiality transfer protection

Hierarchical to: No other components.

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

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

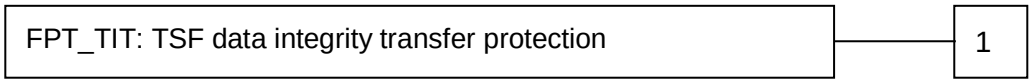
6.5 Inter-TSF TSF data integrity transfer protection (FPT_TIT)

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

Family Behaviour

This family requires integrity protection of exchanged TSF data.

Component levelling:



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

Management: FPT_TIT.1

There are no management activities foreseen.

Audit: FPT_TIT.1

There are no auditable events foreseen.

FPT_TIT.1 TSF data integrity transfer protection

Hierarchical to: No other components.

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

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

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

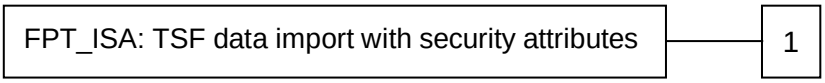
6.6 TSF data import with security attributes (FPT_ISA)

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

Family Behaviour

This family requires TSF data import with security attributes.

Component levelling:



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

Management: FPT_ISA.1

There are no management activities foreseen.

Audit: FPT_ISA.1

There are no auditable events foreseen.

FPT_ISA.1 Import of TSF data with security attributes

Hierarchical to: No other components.

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

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

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

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

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

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

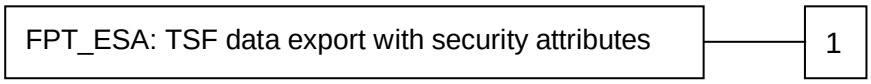
6.7 TSF data export with security attributes (FPT_ESA)

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

Family Behaviour

This family requires TSF data export with security attributes.

Component levelling:



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

Management: FPT_ESA.1 There are no management activities foreseen.

Audit: FPT_ESA.1 There are no auditable events foreseen.

FPT_ESA.1 Export of TSF data with security attributes

Hierarchical to: No other components.

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

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

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

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

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

7 Security Requirements

This chapter gives the security functional requirements (SFR) and the security assurance requirements (SAR) for the TOE and the environment.
Security functional requirements components given in section 7.2 are drawn from Common Criteria part 2 [CC2]. Some security functional requirements represent extensions to [CC2], with a reasoning given in section 6. Operations for assignment, selection and refinement have been made.

The TOE security assurance requirements statements given in section 7.3 “Security Assurance Requirements” are drawn from the security assurance components from Common Criteria part 3 [CC3].

7.1 Typographical Conventions

The following conventions have been used by the Protection Profile [PP-CSPLight] in the definitions of the SFRs and SARs:

- Refinements are denoted in one of two ways, depending on whether they add detail to an SFR or SAR (‘explanatory refinements’) or update the text of an SFR or SAR element (‘element refinements’). Explanatory refinements follow the SFR/SAR that they update and are marked by the word “**Refinement**” in **bold** followed by text describing the refinement. Element refinements are indicated by **bold** text within an SFR/SAR element, with the original text indicated in a footnote.
- Selections and assignments made in the PP are *italicized*, and the original text is indicated in a footnote. Selections and assignments that are left to be filled in by the Security Target author appear in square brackets with an indication that a selection or assignment is to be made, [selection:] or [assignment:], and the description of selection options or assignment description are *italicized*.

If an Application Note e. g. to an SFR was added by the Protection Profile, this is denoted by “**Application Note <nn> (PP)**”, with <nn> being the number of the Application Note as given in the Protection Profile. If an additional Application Note was added by the Security Target writer, this is denoted by “**Application Note <nn> (ST)**”.

7.2 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 establishment and random number generation.

The TOE enforces the Cryptographic Operation SFP for protection of theses cryptographic services. Corresponding 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 a cryptographic security service of the TOE. The encryption FCS_COP.1/HEM combines the generation of a data encryption key and message authentication code (MAC) key, the asymmetric encryption of the data encryption key with an asymmetric key encryption key, cf. FCS_CKM.1/ECKA-EG, FCS_CKM.1/RSA, and the symmetric encryption of the data with the data encryption key and data integrity

mechanism with MAC calculation for the cipher text. The receiver reconstructs the data encryption key and the MAC key, cf. FCS_CKM.5/ECKA-EG, calculates the MAC for the cipher text and compares it with the received MAC. If the integrity of the cipher text is determined, then 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 passwords, cf. FIA_UAU.5.1 clause 1 (1-Factor Authentication). But a human user may also authenticate himself to a token and the token authenticates to the TOE (2-Factor Authentication). 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). Chapter 5.3 describes SFRs 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 a 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. the 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, where the latter is usually closely linked to the claimed identity by means of a certificate. Depending on the security attributes of the cryptographic keys – e.g. encoded in the certificate (cf. FPT_ISA.1/Cert) –, the same cryptographic mechanisms for digital signature generation (FCS_COP.1/CDS-*) and signature verification (cf. FCS_COP.1/VDS-*) may be used for entity authentication, data authentication and nonrepudiation as well.

A trusted channel requires mutual authentication of both endpoints with a key exchange of a key agreement, and the protection of confidentiality by encryption and cryptographic data integrity protection.

The TSF provide security management for user and TSF data, including cryptographic keys. Key management comprises administration and use of keying material in accordance with a security policy. This includes generation, derivation, registration, certification, deregistration, distribution, installation, storage, archival, revocation and destruction of keying material. The key management functionality 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 all cryptographic keys (as data objects of TSF data) and key management services (as operation, cf. to SFR of the FMT class) provided for Administrators, Crypto-Officers, and Key Owners. Note that the cryptographic keys will be used for cryptographic operations under the Cryptographic Operation SFP as well.

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

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

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

Table 3: Elliptic curves, key sizes and standards

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 4: Recommended groups for the Diffie-Hellman key exchange

The individual security functional requirements are specified in the sections below.

7.2.1 Key Management

7.2.1.1 Management of security attributes

FDP_ACC.1/KM Subset access control – Cryptographic operation

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

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

(1) *subjects: Administrator*[2]*, Key Owner;*

(2) *objects: operational cryptographic keys;*

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

[1] [PP-CSPLight] [assignment: *access control SFP*]

[2] *[selection: Administrator, Crypto-Officer]*

[3] [PP-CSPLight] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

FMT_MSA.1/KM Management of security attributes – Key security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/KM The TSF shall enforce the *Key Management SFP and Cryptographic Operation SFP*[4] to restrict the ability to

(1) set and change default values for[5] *the security attributes Identity of the key, Key owner of the key, Key type, Key usage type, Key access control attributes, Key validity time period*[6] to *Administrator*[7,8],

***(2) modify or delete*[9] the security attributes *Identity of the key, Key owner, Key type, Key usage type, Key validity time period of an existing key*[10] to *none*[11],**

***(3) modify independent on key usage*[12] the security attributes *Key usage counter of an existing key*[13] to *none*[14].**

***(4) modify*[15] the security attributes *Key access control attribute of an existing key*[16] to *Administrator*[17,18],**

***(5) query*[19] the security attributes *Key type, Key usage type, Key access control attributes, Key validity time period and Key usage counter of an identified key*[20] to *Administrator, Key Owner*[21,22]**

[4] [PP-CSPLight] [assignment: *access control SFP, information flow control SFP*]

[5] [PP-CSPLight] [selection: *change_default, query, modify, delete, [assignment: other operations]*]

[6] [PP-CSPLight] [assignment: *list of security attributes*]

[7] [PP-CSPLight] [assignment: *the authorised identified roles*]

[8] *[selection: Administrator, Crypto-Officer]*

[9] [PP-CSPLight] [selection: *change_default, query, modify, delete, [assignment: other operations]*]

[10] [PP-CSPLight] [assignment: *list of security attributes*]

[11] [PP-CSPLight] [assignment: *the authorised identified roles*]

[12] [PP-CSPLight] [selection: *change_default, query, modify, delete, [assignment: other operations]*]

[13] [PP-CSPLight] [assignment: *list of security attributes*]

[14] [PP-CSPLight] [assignment: *the authorised identified roles*]

[15] [PP-CSPLight] [selection: *change_default, query, modify, delete, [assignment: other operations]*]

[16] [PP-CSPLight] [assignment: *list of security attributes*]

[17] [PP-CSPLight] [assignment: *the authorised identified roles*]

[18] ***[selection: Administrator, Crypto-Officer, Key Owner]***

[19] [PP-CSPLight] [selection: *change_default, query, modify, delete, [assignment: other operations]*]

[20] [PP-CSPLight] [assignment: *list of security attributes*]

[21] [PP-CSPLight] [assignment: *the authorised identified roles*]

[22] ***[selection: Administrator, Crypto-Officer, KeyOwner]***

Application note 1 ([PP-CSPLight])

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

FMT_MSA.3/KM Static attribute initialisation – Key management

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1/KM	The TSF shall enforce the *Key Management SFP*, *Cryptographic Operation SFP and Update SFP*[23] to provide *restrictive*[24] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/KM	The TSF shall allow the *Administrator*[25,26] 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*[27] the *cryptographic keys*[28] to *Administrator*[29,30], **(2) *import according to FPT_TCT.1/CK, FPT_TIT.1/CK and FPT_ISA.1/CK*[31] the *cryptographic keys*[32] to *Administrator*[33,34],**

[23] [PP-CSPLight] [assignment: *access control SFP, information flow control SFP*]

[24] [PP-CSPLight] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

[25] [PP-CSPLight] [assignment: *the authorised identified roles*]

[26] [selection: *Administrator, Crypto-Officer*]

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

[28] [PP-CSPLight] [assignment: *list of TSF data*]

[29] [PP-CSPLight] [assignment: *the authorised identified roles*]

[30] [selection: *Administrator, Crypto-Officer, Key Owner*]

[31] [PP-CSPLight][selection: change_default, query, modify, delete, clear, [assignment: other operations]]

[32] [PP-CSPLight] [assignment: *list of TSF data*]

[33] [PP-CSPLight] [assignment: *the authorised identified roles*]

[34] ***[selection: Administrator, Crypto-Officer,Key Owner]***

(3) ***export according to FPT_TCT.1/CK, FPT_TIT.1/CK and FPT_ESA.1/CK[35] the cryptographic keys[36] to Administrator[37,38] if security attribute of the key allows export (keys with security attribute Key Usage Counter must never be exported),***

(4) ***delete according to FCS_CKM.4[39] the cryptographic keys[40] to Administrator[41,42]***

Application note 2 ([PP-CSPLight])

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

7.2.1.2 Hash based functions

FCS_COP.1/Hash Cryptographic operation – Hash

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/Hash	The TSF shall perform hash generation[43] in accordance with a specified cryptographic algorithm *SHA-256, SHA-384, SHA-512*[44] and cryptographic key sizes *none*[45] that meet the following: *FIPS 180-4* ***[FIPS PUB 180-4]***[46]*.*

Application note 3 ([PP-CSPLight])

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.

[35] [PP-CSPLight] [selection: *change_default, query, modify, delete, clear,[assignment: other operations]*]

[36] [PP-CSPLight] [assignment: *list of TSF data*]

[37] [PP-CSPLight] [assignment: *the authorised identified roles*]

[38] ***[selection: Administrator, Crypto-Officer, Key Owner]***

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

[40] [PP-CSPLight] [assignment: *list of TSF data*]

[41] [PP-CSPLight] [assignment: *the authorised identified roles*]

[42] ***[selection: Administrator, Crypto-Officer, Key Owner]***

[43] [PP-CSPLight] [assignment: *list of cryptographic operations*]

[44] [PP-CSPLight] [assignment: *cryptographic algorithm*]

[45] [PP-CSPLight] [assignment: *cryptographic key sizes*]

[46] [PP-CSPLight] [assignment: *list of standards*]

7.2.1.3 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*[47]*, modify, clear and delete*[48] the *root key pair*[49] to *Administrator*[50],[51]. **(2) *import and delete*[52] a *known as authentic public key of a certification authority in a PKI*[53] to *Administrator*[54,55].**

Application note 4 ([PP-CSPLight])

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 being an authentic certificate signing key. The PKI may be used for user authentication, key management and signature-verification. The second bullet is a refinement to avoid an iteration of component and therefore printed in bold.

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]
FPT_TIT.1.1/Cert	The TSF shall enforce the *Key Management SFP*[56] to *receive*[57] **a certificate ~~TSF data~~** in a manner protected from *modification and insertion*[58] errors.
FPT_TIT.1.2/Cert	The TSF shall be able to determine on receipt of **a certificate ~~TSF data~~**, whether *modification and insertion*[59] has occurred.

[47] [PP-CSPLight] “create” denotes initial setting a root key

[48] [PP-CSPLight][selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

[49] [PP-CSPLight] [assignment: *list of TSF data*]

[50] [PP-CSPLight] [assignment: *the authorised identified roles*]

[51] [selection: *Administrator, Crypto-Officer*]

[52] [PP-CSPLight][selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

[53] [PP-CSPLight] [assignment: *list of TSF data*]

[54] [PP-CSPLight] [assignment: *the authorised identified roles*]

[55] **[*selection: Administrator, Crypto-Officer]***

[56] [PP-CSPLight] [assignment: *access control SFP, information flow control SFP*]

[57] [PP-CSPLight] [selection: *transmit, receive, transmit and receive*]

[58] [PP-CSPLight] [selection: *modification, deletion, insertion, replay*]

[59] [PP-CSPLight] [selection: *modification, deletion, insertion, replay*]

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency
FPT_ISA.1.1/Cert	The TSF shall enforce the *Key management SFP*[60] 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 **the** 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 it is known as an authentic certificate according to FMT_MTD.1/RK.* (2) *The validity verification of the certificate shall include* *(a) except for root certificates, the verification of the digital signature of the certificate issuer and* *(b) a verification that the security attributes in the certificate pass the interpretation according to FPT_TDC.1*[61]*.*

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 the identity of the certificate issuer*[62] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2/Cert	The TSF shall use **the following rules:**

[60] [PP-CSPLight] [assignment: *access control SFP, information flow control SFP*]

[61] [PP-CSPLight] [assignment: *additional importation control rules*]

[62] [PP-CSPLight] [assignment: *list of TSF data types*]

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

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

(3) *the identity of the certificate issuer shall meet the identity of the signer of the certificate*[63]

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

Application note 5 ([PP-CSPLight]***)***

The security attributes assigned to a certificate holder and the cryptographic key in the certificate are used as TSF data of the TOE. The certificate is imported from a trust centre directory service but must be verified by the TSF (i.e. if it is verified successfully that the source is the trust centre's directory server of the trusted IT product).

7.2.1.4 Key generation, agreement and destruction

Key generation (cf. FCS_CKM.1/ECC, FCS_CKM.1/RSA) is a randomized process which uses random secrets (cf. FCS_RNG.1), applies key generation algorithms and defines security attributes depending on the intended use of the keys. It has the property that it is computationally infeasible to deduce the output without prior knowledge of the secret input. *Key derivation* (cf. FCS_CKM.5/ECC) is a deterministic process by which one or more keys are calculated from a pre-shared key or shared secret or other information. It allows repeating the key generation if the same input is provided. *Key agreement* (cf. FCS_CKM.5/ECDHE) is a key-establishment procedure process for establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key independently of the other party's contribution. Key agreement allows each participant to enforce the cryptographic quality of the agreed key. The component FCS_CKM.1 was refined for key agreement because it normally uses random bits as input. Hybrid cryptosystems (FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA) are a combination of a public key cryptosystem with an efficient symmetric key cryptosystem.

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

FCS_RNG.1 Random number generation

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a *hybrid deterministic*[64] random number generator that implements: *RNG class DRG.4 of [AIS 20/31] chapter 4.9*[65].

[63] [PP-CSPLight] [assignment: *list of interpretation rules to be applied by the TSF*]

[64] [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*]

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

(DRG.4.1) The internal state of the RNG shall use PTRNG of class PTG.2 as random source[66].

(DRG.4.2) The RNG provides forward secrecy.

(DRG.4.3) The RNG provides backward secrecy even if the current internal state is known.

(DRG.4.4) The RNG provides enhanced forward secrecy on condition[67] that 1000 requests for pseudo random bits have been made after last entropy input during instantiation or reseeding[68]

(DRG.4.5) The internal state of the RNG is seeded by an PTRNG of class PTG.2[69]

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

(DRG.4.6) The RNG generates output for which $7 \cdot 10^7$ [70] strings of bit length 128 are mutually different with probability 0.9998.[71]

(DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A[72,73]

Application note 6 ([PP-CSPLight]**)**

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

FCS_CKM.1/AES Cryptographic key generation – AES key

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/AES	The TSF shall generate cryptographic **AES** keys in accordance with a specified cryptographic key generation algorithm *AES*[74] and specified cryptographic key sizes *128 bits, 256 bits*[75,76] that meet the following: *ISO 18033-3[ISO/IEC 18033-3]*[77].

[66] [AIS 20/31]: [selection: *use PTRNG of class PTG.2 as random source, have [assignment: work factor], require [assignment: guess work]*]

[67] [AIS 20/31]: [selection: *on demand, on condition [assignment: condition], after [assignment: time]*]

[68] [AIS 20/31]: [*condition*]

[69] [AIS 20/31]: [selection: *selection: internal entropy source, PTRNG of class PTG.2, PTRNG of class PTG.3, [other selection]*]

[70] [AIS 20/31]: [assignment: *number of strings*]

[71] [AIS 20/31]: [assignment: *probability*]

[72] [AIS 20/31]: [assignment: *additional test suites*]

[73] [assignment: *a defined quality metric*]

[74] [PP-CSPLight] [assignment: *cryptographic key generation algorithm*]

[75] [PP-CSPLight] [assignment: *cryptographic key sizes*]

[76] [selection: *256 bits, [assignment: additional cryptographic key sizes > 128 bits]*]

[77] [PP-CSPLight] [assignment: *list of standards*]

Application note 7 ([PP-CSPLight]**)**

The cryptographic key(s) may be also used together with FCS_COP.1/ED, e. g. for internal purposes.

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

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.5.1/AES	The TSF shall derive cryptographic *AES* keys[78] from *a byte string*[79] in accordance with a specified cryptographic key derivation algorithms *AES key generation using a bit string derived from input parameters with a KDF*[80] and specified cryptographic key sizes *128 bits, 256 bits*[81,82] that meet the following: *NIST SP800-56C [NIST-SP800-56C]*[83].

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** keys ~~-~~ **pairs** in accordance with a specified cryptographic key generation algorithm *ECC key pair generation with all elliptic curves in Table 3*[84,85] and specified cryptographic key sizes *all key sizes in Table 3*[86,87] that meet the following: *all standards in Table 3*[88,89].

Application note 8 ([PP-CSPLight]**)**

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

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

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or

[78] [PP-CSPLight] [assignment: *key type*]

[79] [assignment: *input parameters*]

[80] [PP-CSPLight] [assignment: *cryptographic key derivation algorithm*]

[81] [PP-CSPLight] [assignment: cryptographic key sizes]

[82] [selection: *256 bits, [assignment: additional cryptographic key sizes > 128 bits]*]

[83] [PP-CSPLight] [assignment: *list of standards*]

[84] *[selection: elliptic curves in Table 3]*

[85] [PP-CSPLight] [assignment: *cryptographic key generation algorithm*]

[86] [PP-CSPLight] [assignment: *cryptographic key sizes*]

[87] *[selection: key size in Table 3]*

[88] [PP-CSPLight] [assignment: *list of standards*]

[89] *[selection: standards in Table 3]*

	FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.5.1/ECC	The TSF shall derive cryptographic *elliptic curve* keys *pairs*[90] from *a bit string*[91] in accordance with a specified cryptographic key derivation algorithm *ECC key pair generation with brainpoolP256r1*[92] *using bit string derived from input parameters with ANSI X9.63 Key Derivation Function*[93,94] and specified cryptographic key sizes *256 bits*[95,96] that meet the following: *RFC5639 [RFC5639], TR-03111, section 4.1.3*[97], *[TR-03111]*[98].

Application note 9 ([PP-CSPLight]**)**

The elliptic key pair derivation applies a key derivation function (KDF), e.g. *from [TR-03111] (Section 4.3.3.)* to the input parameter. It uses the output string of a KDF instead of the random bit string as input for the ECC key generation algorithm *([TR-03111], Section 4.1.1, Algorithms 1 or 2)*. The input parameters shall include a secret of the length of 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 **pairs** in accordance with a specified cryptographic key generation algorithm *RSA*[99] and specified cryptographic key sizes *2048 bits, 3072 bits, or 4096 bits modulus size* [100] that meet the following: *PKCS #1 v2.2 [PKCS#1]*[101].

Application note 10 ([PP-CSPLight]**)**

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 SFR FCS_CKM.1/RSA assigns given security attributes *Key identity* and *Key owner*.

[90] [PP-CSPLight] [assignment: *key type*]

[91] *[assignment: input parameters]*

[92] *[selection: elliptic curves in Table 3]*

[93] [PP-CSPLight] [assignment: *cryptographic key derivation algorithm*]

[94] *[assignment: KDF]*

[95] [PP-CSPLight] [assignment: *cryptographic key sizes*]

[96] *[selection: key size in Table 3]*

[97] *[selection: standards in Table 3]*

[98] [PP-CSPLight] [assignment: *list of standards*]

[99] [PP-CSPLight] [assignment: *cryptographic key generation algorithm*]

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

[101] [PP-CSPLight] [assignment: *list of standards*]

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

Hierarchical to: No other components.

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

FCS_CKM.5.1/ECDHE The TSF shall derive cryptographic *ephemeral keys*[102] **for data encryption and MAC with AES-128, *AES-256***[103] from an *agreed shared secret*[104] in accordance with a specified cryptographic key derivation algorithm *Elliptic Curve Diffie Hellman ephemeral key agreement brainpoolP256r1*[105] *and 256-bit random ECP group with IANA assigned ID value of 19 as specified in section 8.1 of [RFC5903]*[106] *with a key derivation from the shared secret according to ANS X9.63 Key Derivation Function*[107,108] and specified cryptographic key sizes *128 bits, 256 bits*[109,110] that meet the following: *TR-03111 [TR-03111]*[111].

Application note 11 ([PP-CSPLight]**)**

The input parameters for key derivation is an agreed shared secret established by means of Elliptic Curve Diffie-Hellman. Table 3 lists elliptic curves and Table 4 lists Diffie-Hellman Groups for the agreement of the shared secret. SHA-1 shall be supported for generation of 128 bits AES keys. SHA-256 shall be selected and used to generate 256 bits AES keys.

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

Hierarchical to: No other components.

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

FCS_CKM.1.1/ECKA-EG The TSF shall generate **ephemeral** cryptographic **elliptic curve** key **pairs for** ECK~~G~~A-EG *[TR-03111], (sender role*) in accordance with a specified cryptographic key generation algorithm *ECC key pair generation with brainpoolP256r1*[112,113] and specified

---

[102] [PP-CSPLight] [assignment: *key type*]

[103] **[selection: *AES-256, none other*]**

[104] [PP-CSPLight] [assignment: *input parameters*]

[105] *[selection: elliptic curves in Table 3]*

[106] *[selection: DH group in Table 4]*

[107] [PP-CSPLight] [assignment: *cryptographic key derivation algorithm*]

[108] *[assignment: key derivation function]*

[109] [PP-CSPLight] [assignment: *cryptographic key sizes*]

[110] *[selection:256 bits, none other]*

[111] [PP-CSPLight] [assignment: *list of standards*]

[112] [PP-CSPLight] [assignment: *cryptographic key generation algorithm*]

[113] *[selection: elliptic curves in Table 3]*

cryptographic key sizes *256 bits*[114,115] that meet the following: *RFC5639[RFC5639], TR-03111, section 4.1.3[TR-03111]*[116,117].

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

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.5.1/ECKA-EG	The TSF shall derive cryptographic *data encryption and MAC keys for AES-128, AES-256*[118,119] from *a private and a public ECC key*[120] in accordance with a specified cryptographic key derivation algorithm *ECKGA-EG[TR-03111] brainpoolP256r1*[121] *and X9.63 Key Derivation Function*[122] and specified cryptographic **symmetric** key sizes *128 bits, 256 bits*[123,124] that meet the following: *TR03111[TR-03111], chapter 4.3.2.2*[125].

Application note 12 ([PP-CSPLight]**)**

FCS_CKM.5/ECKA-EG is used by both the sender (encryption) and the recipient (decryption) to compute a secret point SAB on an elliptic curve and derived a shared secret ZAB. The shared secret is then used as the input to the key derivation function to derive two symmetric keys: the encryption key and the MAC key. These are then used to encrypt or decrypt messages according to FCS_COP.1/HEM or FCS_COP.1/HDM, respectively. Sender and recipient use however different inputs to FCS_CKM.5/ECKA-EG. The sender first generates an ephemeral ECC key pair according to FCS_CKM.1/ECKA-EG and uses the generated ephemeral private key and the static public key of the recipient as input. The recipient first extracts the ephemeral public key from the message and uses the ephemeral public key and the static private key (cf. FCS_CKM.1/ECC for key generation) as the input to derive the symmetric keys. The selection of the elliptic curve, the ECC key size and length of the shared secret shall correspond to the selection of the AES key size, e. g. brainpoolP256r1 and 256 bits seed for ECC key and AES keys. FCS_CKM.1/ECKA-EG and FCS_CKM.5/ECKA-EG do not provide self-contained security services for the user but are necessary steps for FCS_COP.1/HEM and FCS_COP.1/HDM (refer to the next section 7.2.3).

---

114 [PP-CSPLight] [assignment: *cryptographic key sizes*]

115 *[selection: key size in Table 3]*

116 [PP-CSPLight] [assignment: *list of standards*]

117 *[selection: standards in Table 3]*

118 [PP-CSPLight] [assignment: *key type*]

119 *[selection: AES-256, none other]*

120 [PP-CSPLight] [assignment: *input parameters*]

121 *[selection: elliptic curves in Table 3]*

122 [PP-CSPLight] [assignment: *cryptographic key derivation algorithm*]

123 [PP-CSPLight] [assignment: *cryptographic key sizes*]

124 *[selection:256 bits, none other]*

125 [PP-CSPLight] [assignment: list of standards]

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** a **seed, derive** cryptographic keys **from the seed for data encryption and MAC with AES-128, *AES-256*[126]** in accordance with a specified cryptographic key generation algorithm *X9.63 Key Derivation Function [ANSI-X9.63] and RSA EME-OAEP [PKCS#1]*[127] and specified cryptographic **symmetric** key sizes *128 bits, 256 bits*[128,129] that meet the following: *ISO/IEC18033-3 [ISO/IEC 18033-3], PKCS #1 v2.2 [PKCS#1]*[130].

Application note 13 ([PP-CSPLight]**)**

The asymmetric cryptographic key sizes used in FCS_CKM.1/AES_RSA must be at least 2000 bits. Cryptographic key sizes of at least 3000 bits are recommended. FCS_CKM.1/AES_RSA and FCS_CKM.5/AES_RSA do not provide self-contained security services for the user but they are only necessary steps for FCS_COP.1/HEM respective FCS_COP.1/HDM (refer to the next section 7.2.3).

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

Hierarchical to: No other components.

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

FCS_CKM.5.1/AES_RSA The TSF shall derive cryptographic *data encryption* keys *and MAC keys for AES-128, AES-256*[131,132] from **a decrypted** *RSA encrypted seed*[133] in accordance with a specified cryptographic key derivation algorithm *RSA EME-OAEP [PKCS#1] and X9.63 [ANSI-X9.63] Key Derivation Function*[134] and specified cryptographic **symmetric** key sizes *128 bits, 256 bits*[135,136] that meet the following: *ISO/IEC 14888-2 [ISO/IEC 14888-2]*[137].

---

[126] **[selection: *AES-256, none other*]**

[127] [PP-CSPLight] [assignment: *cryptographic key generation algorithm*]

[128] [PP-CSPLight] [assignment: *cryptographic key sizes*]

[129] *[selection:256 bits, none other]*

[130] [PP-CSPLight] [assignment: *list of standards*]

[131] [PP-CSPLight] [assignment: *key type*]

[132] *[selection: AES-256, none other]*

[133] [PP-CSPLight] [assignment: *input parameters*]

[134] [PP-CSPLight] [assignment: *cryptographic key derivation algorithm*]

[135] [PP-CSPLight] [assignment: *cryptographic key sizes*]

[136] *[selection: 256 bits, none other]*

[137] [PP-CSPLight] [assignment: *list of standards*]

FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting the key by zeroising in case of secret or private keys*[138] that meets the following: *none*[139].

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.

7.2.1.5 Key import and export

FCS_COP.1/KW Cryptographic operation – Key wrap

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/KW	The TSF shall perform *key wrap*[140] in accordance with a specified cryptographic algorithm *AES-Keywrap KWP*[141,142] and cryptographic key sizes **of the key encryption key** *128 bits, 256 bits*[143,144] that meet the following: *NIST SP800-38F [NIST-SP800-38F]*[145].

Application note 14 ([PP-CSPLight]**)**

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

[138] [assignment: *cryptographic key destruction method*]

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

[140] [PP-CSPLight] [assignment: *list of cryptographic operations*]

[141] [PP-CSPLight] [assignment: *cryptographic algorithm*]

[142] *[selection: KW, KWP]*

[143] [PP-CSPLight] [assignment: *cryptographic key sizes*]

[144] *[selection: 256 bits, none other]*

[145] [PP-CSPLight] [assignment: *list of standards*]

FCS_COP.1.1/KU	The TSF shall perform *key unwrap*[146] in accordance with a specified cryptographic algorithm *AES-Keywrap* *KWP*[147,148] and cryptographic key sizes **of the *key encryption key*** *128 bits, 256 bits*[149,150] that meet the following: *NIST SP800-38F [NIST-SP800-38F]*[151].

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]
FPT_TCT.1.1/CK	The TSF shall enforce the *Key Management SFP*[152] by providing the ability to *transmit and receive*[153] **a cryptographic key** ~~TSF data~~ in a manner protected from unauthorised disclosure **according to FCS_COP.1/KW and FCS_COP.1/KU**.

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]
FPT_TIT.1.1/CK	The TSF shall enforce the *Key Management SFP*[154] to *transmit and receive*[155] **cryptographic keys** ~~TSF data~~ in a manner protected from *modification and insertion*[156] 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*[157] has occurred **according to FCS_COP.1/KU**.

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or

[146] [PP-CSPLight] [assignment: *list of cryptographic operations*]

[147] [PP-CSPLight] [assignment: *cryptographic algorithm*]

[148] *[selection: KW, KWP]*

[149] [PP-CSPLight] [assignment: *cryptographic key sizes*]

[150] *[selection:256 bits, none other]*

[151] [PP-CSPLight] [assignment: *list of standards*]

[152] [PP-CSPLight] [assignment: *access control SFP, information flow control SFP*]

[153] [PP-CSPLight] [selection: *transmit, receive, transmit and receive*]

[154] [PP-CSPLight] [assignment: *access control SFP, information flow control SFP*]

[155] [PP-CSPLight] [selection: *transmit, receive, transmit and receive*]

[156] [PP-CSPLight] [selection: *modification, deletion, insertion, replay*]

[157] [PP-CSPLight] [selection: *modification, deletion, insertion, replay*]

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

FPT_ISA.1.1/CK	The TSF shall enforce the *Key Management SFP*[158] when importing **cryptographic key** ~~TSF data~~, controlled under the SFP, from outside of the TOE.
FPT_ISA.1.2/CK	The TSF shall use the security attributes associated with the imported **cryptographic key** ~~TSF data~~.
FPT_ISA.1.3/CK	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the **cryptographic key** ~~TSF data~~ received.
FPT_ISA.1.4/CK	The TSF shall ensure that interpretation of the security attributes of the imported **cryptographic key** ~~TSF data~~ is as intended by the source of the **cryptographic key** ~~TSF data~~.
FPT_ISA.1.5/CK	The TSF shall enforce the following rules when importing **a 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 the verification of the digital signature of the issuer and the validity time period.* (2) *No further rules*[159,160]*.*

Application note 15 ([PP-CSPLight]**)**

The operational environment is obligated to use trust centre 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*[161] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2/CK	The TSF shall use **the following rules**: (1) *the TOE reports about conflicts between the Key identity of stored cryptographic keys and cryptographic keys to be imported,* (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*[162]

[158] [PP-CSPLight] [assignment: *access control SFP, information flow control SFP*]

[159] [PP-CSPLight] [assignment: *importation control rules*]

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

[161] [PP-CSPLight] [assignment: *list of TSF data types*]

[162] [PP-CSPLight] [assignment: *list of interpretation rules to be applied by the TSF*]

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

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency
FPT_ESA.1.1/CK	The TSF shall enforce the *Key Management SFP*[163] when exporting **a 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 **a cryptographic key** ~~TSF data~~ is exported from the TOE: *For keys with the security attribute "Key Usage Counter", the TSF must ensure that decreasing the counter importing an older version of the key is impossible. Additionally no further rules*[164,165].

Application note 16 ([PP-CSPLight]**)**

W.r.t. to FPT_ESA.1.4/CK note the following naive attack: 1) A user exports a key having the attribute "Key Usage Counter". 2) The key is then re-imported and used several times. 3) The key is exported again and 4) the exported version of 1) instead of the one of 3.) is re-imported, thus effectively decreasing the attribute "Key Usage Counter". A straight-forward way to counter this is to prohibit keys with the attribute "Key Usage Counter" from being exported.

Keys with the security attribute "Key Usage Counter" are never transferred from TOE into any non-TOE entity. They are only transferred between one TOE sample and another TOE sample in a cluster (master to slave) or between different partitions when the SMA is moved from one partition to another one. Following security measures make it impossible to modify the signature counter or use an older version of the signature key during the transfer of keys avoiding a similar naive attack as described above.

1. Private cryptographic keys with security attribute "Timestamp" are not allowed to be transferred into a non-TOE environment. They can only be transferred in the context of the synchronisation between Master and Slave CSPLight in a cluster.

[163] [PP-CSPLight] [assignment: access control SFP, information flow control SFP]

[164] [PP-CSPLight] [assignment: additional exportation control rules]

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

2. Master CSPLight communicates with the Slave CSPLight over a PACE secure channel.
3. Signature keys, bundled with their signature counters, are encrypted with a Master Backup Key (MBK) before being stored in a database inside the CryptoServer CSPLight or transferred to another TOE sample.
4. During a synchronisation between Master and Slave CSPLight in a cluster, any request of service from a Security Module Application involving the use of signature keys is locked until the synchronisation is complete.

7.2.2 Data encryption

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ED	The TSF shall perform *data encryption and decryption*[166] in accordance with a specified cryptographic algorithm *symmetric data encryption according to AES-128 and AES-256*[167] *in CBC and no other*[168] *mode*[169] and cryptographic key size *128 bits, 256 bits*[170,171] that meet the following: *NIST-SP800-38A[NIST-SP800-38A], ISO 18033-3 [ISO/IEC 18033-3], ISO 10116 [ISO/IEC 10116]*[172].

Application note 17 ([PP-CSPLight]**)**

Data encryption and decryption should be combined with data integrity mechanisms in Encrypt-then-MAC order, i. e. the MAC is calculated over the ciphertext and verified before decryption. The modes of operation should combine encryption with data integrity mechanisms into authenticated encryption, e. g. 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 7.2.3.

7.2.3 Hybrid encryption with MAC for user data

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

Hierarchical to:	No other components.

166 [PP-CSPLight] [assignment: *list of cryptographic operations*]

167 *[selection: AES-256, no other algorithm]*

168 *[selection: CRT, OFB, CFB, no other]*

169 [PP-CSPLight] [assignment: *cryptographic algorithm*]

170 [PP-CSPLight] [assignment: *cryptographic key sizes*]

171 *[selection: 256 bits, no other key size]*

172 [PP-CSPLight] [assignment: *list of standards*]

Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/HEM	The TSF shall perform *hybrid data encryption and MAC calculation*[173] in accordance with a specified cryptographic algorithm *asymmetric key encryption according to FCS_CKM.1/AES_RSA*[174]*, symmetric data encryption according to AES-128, AES-256*[175] *[FIPS PUB 197] in CBC [NIST-SP800-38A]*[176] *mode with CMAC [NIST-SP800-38B]*[177] *calculation*[178] and cryptographic **symmetric** key sizes *128 bits*, *256 bits*[179,180] that meet the following: *the referenced standards above according to the chosen selection*[181].

Application note 18 ([PP-CSPLight]**)**

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

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/HDM	The TSF shall perform *hybrid MAC verification and data decryption*[182] in accordance with a specified cryptographic algorithm *asymmetric key decryption according to FCS_CKM.5/AES_RSA*[183]*, verification of CMAC [NIST-SP800-38B]*[184] *and symmetric data decryption according to AES with AES-128, AES-256*[185] *[FIPS PUB 197] in mode CBC*

[173] [PP-CSPLight] [assignment: *list of cryptographic operations*]

[174] *[selection: FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA, FCS_CKM.5/ECDHE]*

[175] *[selection: AES-256, none other]*

[176] *[selection: CBC [NIST-SP800-38A], CCM [NIST-SP800-38C], GCM [NIST-SP800-38D]]*

[177] *[selection: CMAC [NIST-SP800-38B], GMAC [NIST-SP800-38D], HMAC [RFC2104]]*

[178] [PP-CSPLight] [assignment: *cryptographic algorithm*]

[179] [PP-CSPLight] [assignment: *cryptographic key sizes*]

[180] [selection: *256 bits, no other key size*]

[181] [PP-CSPLight] [assignment: *list of standards*]

[182] [PP-CSPLight] [assignment: *list of cryptographic operations*]

[183] *[selection: FCS_CKM.5/ECDHE, FCS_CKM.5/ECKA-EG, FCS_CKM.5/AES_RSA]*

[184] *[selection: CMAC [NIST-SP800-38B], GCM [NIST-SP800-38D], HMAC [RFC2104]]*

[185] *[selection: AES-128, AES-256]*

[NIST-SP800-38A][186,187] and cryptographic **symmetric** key sizes *128 bits*, *256 bits*[188,189] that meet the following: *the referenced standards above according to the chosen selection*[190].

Application note 19 ([PP-CSPLight]**)**

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

7.2.4 Data integrity mechanisms

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

FCS_COP.1/MAC Cryptographic operation – MAC using AES

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/MAC	The TSF shall perform *MAC generation and verification*[191] in accordance with a specified cryptographic algorithm *AES-128 and AES-256*[192] *[FIPS PUB 197] CMAC [NIST-SP800-38B] and no other*[193,194] and cryptographic key sizes *128 bits, 256 bits*[195,196] that meet the following: *the referenced standards above according to the chosen selection*[197].

Application note 20 ([PP-CSPLight]**)**

186 [PP-CSPLight] [assignment: *cryptographic algorithm*]

187 *[selection: CBC [NIST-SP800-38A], CCM [NIST-SP800-38C], GMAC [NIST-SP800-38D]]*

188 [PP-CSPLight] [assignment: *cryptographic key sizes*]

189 *[selection: 256 bits, no other key size]*

190 [PP-CSPLight] [assignment: *list of standards*]

191 [PP-CSPLight] [assignment: *list of cryptographic operations*]

192 *[selection: AES-256, none other]*

193 [PP-CSPLight] [assignment: *cryptographic algorithm*]

194 *[selection: GMAC[NIST-SP800-38D], no other]*

195 [PP-CSPLight] [assignment: *cryptographic key sizes*]

196 *[selection: 256 bits, no other key size]*

197 [PP-CSPLight] [assignment: *list of standards*]

The MAC may be applied to plaintexts and cipher texts. The algorithm AES-128 CMAC is mandatory.

FCS_COP.1/HMAC Cryptographic operation – HMAC

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/HMAC The TSF shall perform *HMAC generation and verification*[198] in accordance with a specified cryptographic algorithm *HMAC-SHA256 and no other*[199,200] and cryptographic key sizes *512 bits*[201] that meet the following*: RFC2104[RFC2104], ISO 9797-2[ISO/IEC 9797-2]*[202].

Application note 21 ([PP-CSPLight]**)**

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

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

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/CDS-ECDSA The TSF shall perform *signature-creation*[203] in accordance with a specified cryptographic algorithm *ECDSA with all elliptic curves in Table 3*[204,205] and cryptographic key sizes *all key sizes in Table 3*[206,207] that meet the following: *all reference standards in Table 3*[208,209].

198 [PP-CSPLight] [assignment: *list of cryptographic operations*]

199 [PP-CSPLight] [assignment: *cryptographic algorithm*]

200 *[selection: HMAC-SHA-1, HMACSHA384, no other]*

201 [assignment: *cryptographic key sizes*]

202 [PP-CSPLight] [assignment: *list of standards*]

203 [PP-CSPLight] [assignment: *list of cryptographic operations*]

204 [PP-CSPLight] [assignment: *cryptographic key generation algorithm*]

205 *[selection: elliptic curves in Table 3]*

206 [PP-CSPLight] [assignment: *cryptographic key sizes*]

207 *[selection: key size in Table 3]*

208 [PP-CSPLight] [assignment: *list of standards*]

209 *[selection: standards in Table 3]*

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

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/VDS-ECDSA The TSF shall perform *signature-verification*[210] in accordance with a specified cryptographic algorithm *ECDSA with all elliptic curves in Table 3*[211,212] and cryptographic key sizes *all key sizes in Table 3*[213,214] that meet the following: *all reference standards in Table 3*[215,216].

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

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/CDS-RSA The TSF shall perform *signature-creation*[217] in accordance with a specified cryptographic algorithm *RSA and EMSA-PSS*[218] and cryptographic key sizes *2048 bits, 3072 bits, and 4096 bits*[219] that meet the following: *ISO/IEC 14888-2 [ISO/IEC 14888-2], PKCS #1, v2.2 [PKCS#1]*[220].

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

---

[210] [PP-CSPLight] [assignment: *list of cryptographic operations*]

[211] [PP-CSPLight] [assignment: *cryptographic key generation algorithm*]

[212] *[selection: elliptic curves in Table 3]*

[213] [PP-CSPLight] [assignment: *cryptographic key sizes*]

[214] *[selection: key size in Table 3]*

[215] [PP-CSPLight] [assignment: *list of standards*]

[216] *[selection: standards in Table 3]*

[217] [PP-CSPLight] [assignment: *list of cryptographic operations*]

[218] [PP-CSPLight] [assignment: *cryptographic algorithm*]

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

[220] [PP-CSPLight] [assignment: *list of standards*]

FCS_COP.1.1/VDS-RSA The TSF shall perform *signature-verification*[221] in accordance with a specified cryptographic algorithm *RSA and EMSA-PSS*[222] and cryptographic key sizes *2048 bits, 3072 bits, and 4096 bits*[223] that meet the following: *ISO/IEC 14888-2 [ISO/IEC 14888-2] , PKCS #1, v2.2 [PKCS#1]*[224].

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*[225] **imported according to FDP_ITC.2/UD by means of *FCS_COP.1/CDS-ECDSA*[226] and keys holding the security attribute Key identity assigned to the guarantor and Key usage type "digitalSignature".**
FDP_DAU.2.2/Sig	The TSF shall provide *external entities*[227] 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 22 ([PP-CSPLight]**)**

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 owner* of the guarantor and *Key usage type "digitalSignature"* 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 verification of the evidence requires a certificate showing the identity of the key owner.

7.2.5 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 *PACE in ICC role*[228] to prove the identity of the *TOE*[229] to an external entity **and to establish a trusted channel according to FTP_ITC.1 case 1 or 2.**

[221] [PP-CSPLight] [assignment: *list of cryptographic operations*]

[222] [PP-CSPLight] [assignment: *cryptographic algorithm*]

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

[224] [PP-CSPLight] [assignment: *list of standards*]

[225] [PP-CSPLight] [assignment: *list of objects or information types*]

[226] **[selection: *FCS_COP.1/CDS-RSA*, *FCS_COP.1/CDS-ECDSA*]**

[227] [PP-CSPLight] [assignment: *list of subjects*]

[228] [PP-CSPLight] [assignment: *authentication mechanism*]

[229] [PP-CSPLight] [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 *Chip Authentication Version 2 according to [TR-03110] section 3.4*[230] to prove the identity of the *TOE*[231] to an external entity **and to establish a trusted channel according to FTP_ITC.1 case 3.**

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

Hierarchical to:	FDP_DAU.1 Basic Data Authentication
Dependencies:	FIA_UID.1 Timing of identification
FDP_DAU.2.1/Att	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of *attestation data*[232] **by means of *FCS_COP.1/CDS-ECDSA*[233] and keys holding the security attributes Key identity assigned to the TOE sample, and Key usage type "contentCommitment".**
FDP_DAU.2.2/Att	The TSF shall provide *external entities*[234] 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 23 ([PP-CSPLight]**)**

The attestation data shall represent the TOE sample as a 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, the hash value of the TSF implementation and some TSF data as result of a 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. a digital signature, a group signature or a direct anonymous attestation mechanism as e.g. used for Trusted Platform Modules [TPMLib,Part 1] or FIDO U2F Authenticators [FIDO-ECDAA].

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1	The TSF shall provide a communication channel between TSF and another trusted IT product that is ~~logically distinct from other communication channels~~ ***logically separated from other***

[230] [PP-CSPLight] [assignment: *authentication mechanism*]

[231] [PP-CSPLight] [assignment: *object, authorized user or role*]

[232] [PP-CSPLight] [assignment: *list of objects or information types*]

[233] **[selection: *FCS_COP.1/CDS-RSA, FCS_COP.1/CDS-ECDSA, ECDAA according to [selection: [TPMLib,Part 1] [FIDO-ECDAA]], [assignment: other cryptographic authentication mechanisms]*]**

[234] [PP-CSPLight] [assignment: *list of subjects*]

communication channels, or using physical separated ports[235] and provides assured identification of its end points ***according to the case 1 in Table 5***[236] and protection of the channel data from modification or disclosure ***according to the case 1 in Table 5***[237] **as required by *cryptographic operation FCS_COP.1/TCM according to the case 1 in Table 5***[238]**.**

FTP_ITC.1.2 The TSF shall permit *the remote trusted IT product*[239] **determined according to FMT_MOF.1.1 clause (3)** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *communication with entities defined according to FMT_MOF.1 clause (4)*[240].

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

Table 5: Operation in SFR for trusted channel

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

Hierarchical to: No other components.

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

FCS_CKM.1.1/PACE The TSF shall generate cryptographic keys ***for MAC with for FCS_COP.1/TCM and if selected encryption keys for FCS_COP.1/TCE*** in accordance with a specified cryptographic key ~~generation~~ **agreement** algorithm *PACE with brainpoolP256r1*[241] *and*

[235] **[selection: *logically separated from other communication channels, using physical separated ports*]**

[236] **[selection: *Authentication of the TOE and remote entity according to the case in Table 5*]**

[237] **[assignment: *according to the case in Table 5*]**

[238] **[selection: *cryptographic operation according to the case in Table 5*]**

[239] [PP-CSPLight] [selection: *the TSF, the remote trusted IT product*]

[240] [PP-CSPLight] [assignment: *list of functions for which a trusted channel is required*]

[241] *[selection: elliptic curves in Table 3]*

Generic Mapping in ICC role[242] and specified cryptographic key sizes *256 bits*[243,244] that meet the following: *ICAO Doc9303*, *Part 11, section 4.4 [ICAO Doc9303]*[245].

Application note 24 ([PP-CSPLight]**)**

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

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

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/TCAP	The TSF shall generate cryptographic keys ***for encryption according to FCS_COP.1/TCE and MAC according to FCS_COP.1/TCM*** in accordance with a specified cryptographic key ~~generation~~ **agreement** algorithms *Terminal Authentication version 2 and Chip Authentication Version 2*[246] and specified cryptographic key sizes *256 bits*[247,248] that meet the following: *BSI TR-03110 [TR-03110], section 3.3 and 3.4*[249].

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/TCE	The TSF shall perform *encryption and decryption*[250] in accordance with a specified cryptographic algorithm *AES in CBC [NIST-SP800-38A]*[251]

[242] [PP-CSPLight] [assignment: *cryptographic algorithm*]

[243] [PP-CSPLight] [assignment: *cryptographic key sizes*]

[244] *[selection: 128 bits, 192 bits, 256 bits]*

[245] [PP-CSPLight] [assignment: *list of standards*]

[246] [PP-CSPLight] [assignment: *cryptographic algorithm*]

[247] [PP-CSPLight] [assignment: *cryptographic key sizes*]

[248] *[selection: 128 bits, 192 bits, 256 bits]*

[249] [PP-CSPLight] [assignment: *list of standards*]

[250] [PP-CSPLight] [assignment: *list of cryptographic operations*]

[251] *[selection: CBC[NIST-SP800-38A], CCM[NIST-SP800-38C], GCM[NIST-SP800-38D]]*

mode[252] and cryptographic key sizes *256 bits*[253,254] that meet the following:*[FIPS PUB 197]*[255].

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/TCM	The TSF shall perform *MAC calculation and MAC verification*[256] in accordance with a specified cryptographic algorithm *AES CMAC[NIST-SP800-38B]*[257,258] and cryptographic key sizes *256 bits*[259,260] that meet the following: *[FIPS PUB 197]*[261]*.*

7.2.6 User identification and authentication

FIA_ATD.1 User attribute definition – Identity based authentication

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: (1) *Identity,* (2) *Authentication reference data,* (3) *Role.*

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

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

[252] [PP-CSPLight] [assignment: *cryptographic algorithm*]

[253] [PP-CSPLight] [assignment: *cryptographic key sizes*]

[254] *[selection: 128 bits, 192 bits, 256 bits]*

[255] [PP-CSPLight] [assignment: *list of standards*]

[256] [PP-CSPLight] [assignment: *list of cryptographic operations*]

[257] [PP-CSPLight] [assignment: *cryptographic algorithm*]

[258] *[selection: CMAC[NIST-SP800-38B], GMAC[NIST-SP800-38D]]*

[259] [PP-CSPLight] [assignment: *cryptographic key sizes*]

[260] *[selection: 128 bits, 192 bits, 256 bits]*

[261] [PP-CSPLight] [assignment: *list of standards*]

(1) *create*[262] *the initial Authentication reference data of all authorized users*[263] to *Administrator*[264,265],

(2) *delete*[266] *the Authentication reference data of an authorized user*[267] to *Administrator*[268,269],

(3) *modify*[270] *the Authentication reference data*[271] to *the corresponding authorized user*[272].

(4) *create*[273] *the permanently stored session key of a trusted channel as Authentication reference data*[274] to *Administrator*[275,276]

(5) *define*[277] *the time in range 30 minutes to 48 hours of inactivity*[278] *after which the user security attribute Role of the authentication data record is reset according to FMT_SAE.1*[279] to *Administrator*[280,281],

(6) *define*[282] *the value Unidentified user*[283] *to which the security attribute Role of the authentication data record shall be reset according to FMT_SAE.1*[284] to *Administrator*[285,286].

---

[262] [PP-CSPLight] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

[263] [PP-CSPLight] [assignment: *list of TSF data*]

[264] [PP-CSPLight] [assignment: *the authorised identified roles*]

[265] *[selection: Administrator, User Administrator]*

[266] [PP-CSPLight] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

[267] [PP-CSPLight] [assignment: *list of TSF data*]

[268] [PP-CSPLight] [assignment: *the authorised identified roles*]

[269] ***[selection: Administrator, User Administrator]***

[270] [PP-CSPLight] [selection: *change_default, query, modify, delete, clear,[assignment: other operations]*]

[271] [PP-CSPLight] [assignment: *list of TSF data*]

[272] [PP-CSPLight] [assignment: *the authorised identified roles*]

[273] [PP-CSPLight] [selection: *change_default, query, modify, delete, clear,[assignment: other operations]*]

[274] [PP-CSPLight] [assignment: *list of TSF data*]

[275] [PP-CSPLight] [assignment: *the authorised identified roles*]

[276] ***[selection: Administrator, User Administrator]***

[277] [PP-CSPLight] [selection: *change_default, query, modify, delete, clear [assignment: other operations]*]

[278] **[assignment: *time frame*]**

[279] [PP-CSPLight] [assignment: *list of TSF data*]

[280] [PP-CSPLight] [assignment: *the authorised identified roles*]

[281] ***[selection: Administrator, User Administrator]***

[282] [PP-CSPLight] [selection: *change_default, query, modify, delete, clear [assignment: other operations]*]

[283] ***[selection: Unidentified user, Unauthenticated user]***

[284] [PP-CSPLight] [assignment: *list of TSF data*]

[285] [PP-CSPLight] [assignment: *the authorised identified roles*]

[286] ***[selection: Administrator, User Administrator]***

Application note 25 ([PP-CSPLight]**)**

The Administrator is responsible for user management. The Administrator creates and revokes a user as a known authorized user of the TSF by creating resp. deleting authentication data records and additionally authentication reference data for the user identities in these records, 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 an 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 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*[287] **by enforcing a change of initial passwords to a different operational password on the first successful authentication of the user**

FIA_AFL.1/PINPUK Authentication failure handling

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1/PINPUK	The TSF shall detect when *three*[288] unsuccessful authentication attempts occur related to *consecutive failed authentication attempts*[289] .
FIA_AFL.1.2/PINPUK	When the defined number of unsuccessful authentication attempts has been *met*[290], the TSF shall *enforce the reset of user authentication data (PIN) via a PUK*[291].

FIA_AFL.1/PASSWORD Authentication failure handling

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication

[287] [PP-CSPLight] [assignment: *list of TSF data*]

[288] [selection: [assignment: *positive integer number*], ~~*an administrator*~~ ***[selection: Administrator, User Administrator]*** *configurable positive integer within [assignment: range of acceptable values]*]

[289] [assignment: *list of authentication events*]

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

[291] [assignment: *list of actions*]

FIA_AFL.1.1/PASSWORD The TSF shall detect when *one* [292] unsuccessful authentication attempts occur related to *consecutive failed authentication attempts*[293] .

FIA_AFL.1.2 /PASSWORD When the defined number of unsuccessful authentication attempts has been *surpassed*[294], the TSF shall *wait for an exponentially increasing period of time between each authentication attempt* [295].

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*[296]*.*
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*[297].
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: (1) *after successful identification of the user, the attribute Role of the subject shall be changed from Unidentified user to Unauthenticated user;* (2) *after successful authentication of the user for a selected role, the attribute Role of the subject shall be changed from Unauthenticated User to that role;* (3) *after successful re-authentication of the user for a selected role, the attribute Role of the subject shall be changed to that role*[298]*.*

FMT_SAE.1 Time-limited authorisation

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FPT_STM.1 Reliable time stamps

[292] [selection: [assignment: *positive integer number*], ~~*an administrator*~~ ***[selection: Administrator, User Administrator]*** *configurable positive integer within [assignment: range of acceptable values]*]

[293] [assignment: *list of authentication events*]

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

[295] [assignment: *list of actions*]

[296] [PP-CSPLight] [assignment: *list of user security attributes*]

[297] [PP-CSPLight] [assignment: *rules for the initial association of attributes*]

[298] [PP-CSPLight] [assignment: *rules for the changing of attributes*]

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for *a Role*[299] to *Administrator*[300,301].

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

Application note 26 ([PP-CSPLight]**)**

The TSF shall implement means to handle an expiration time for the roles within a session (i.e. between power-up and power-down of the TOE) which may not necessarily meet the requirements for a reliable time stamp as required by FPT_STM.1. As the security target requires FPT_STM.1 (e.g. as the PP-module "Time Stamp and Audit" is claimed), this time stamp is used to meet FMT_SAE.1.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow

(1) *self test according to FPT_TST.1,*
(2) *identification of the TOE to the user,*
(3) *no other TSF-mediated action*[303,304]

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

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

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow

(1) *self test according to FPT_TST.1,*
(2) *authentication of the TOE to the user after authentication of the user to the TOE,*
(3) *identification of the user to the TOE and selection of a set of role*[305] *for authentication,*

[299] [PP-CSPLight] [assignment: *list of security attributes for which expiration is to be supported*]

[300] [PP-CSPLight] [assignment: *the authorised identified roles*]

[301] *[selection: Administrator, User Administrator]*

[302] [PP-CSPLight] [assignment: *list of actions to be taken for each security attribute*]

[303] [PP-CSPLight] [assignment: *list of TSF mediated actions*]

[304] *[assignment: list of other TSF-mediated actions]*

[305] *[selection: a role, a set of role]*

(4) *reception of the request for PACE from another trusted IT product*[306].[307]

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 27 ([PP-CSPLight]**)**

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 the TOE in ICC and the user in PCD context with the establishment of trusted channel according to FTP_ITC.1,*
(3) *certificate based Terminal Authentication Version 2 according to section 3.3 in [TR-03110] with the TOE in ICC and the user in PCD context,*
(4) *Terminal Authentication Version 2 with the TOE in ICC context and user in PCD context modified by omitting the verification of the certificate chain (simplified TA2),*
(5) *Chip Authentication Version 2 with establishment of a trusted channel according to FTP_ITC.1,*
(6) *message authentication by MAC verification of received messages*[308]

to support user authentication.

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

(1) *password authentication shall be used for authentication of human users if enabled according to FMT_MOF.1.1, clause (1),*
(2) *PACE shall be used for authentication of human users using terminals with the establishment of a trusted channel according to FTP_ITC.1,*
(3) *PACE may be used for authentication of IT entities with the establishment of a trusted channel according to FTP_ITC.1,*
(4) *certificate based Terminal Authentication Version 2 may be used for authentication of users whose certificate is imported as TSF data,*

[306] [PP-CSPLight] [assignment: *list of TSF mediated actions*]

[307] *[assignment: list of other TSF mediated actions]*

[308] [PP-CSPLight] [assignment: *list of multiple authentication mechanisms*]

(5) *the simplified version of Terminal Authentication Version 2 may be used for authentication of identified users associated with a known user's public key,*
(6) *message authentication by MAC verification of received messages shall be used after initial authentication of a remote entity according to clauses (2) or (3) for a trusted channel according to FTP_ITC.1,*
(7) *no further rules*[309,310]*.*

FIA_UAU.6 Re-authenticating

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions (1) *changing to a role not selected for the current valid authentication session,* (2) *power on or reset,* (3) *every message received from entities after establishing trusted channel according to FIA_UAU.5.1, clause (2), (3) or (6),* (4) *after an explicit logoff of the user*[311,312]*.*

7.2.7 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*[313] 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 the interpretation of the security attributes of the imported user data is as intended by the source of the user data.

309 [PP-CSPLight] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

310 *[assignment: additional rules]*

311 [PP-CSPLight] [assignment: *list of conditions under which re-authentication is required*]

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

313 [PP-CSPLight] [assignment: *access control SFP, information flow control SFP*]

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 the attribute Key identity of the key and the identification of the requested cryptographic operation,*
(2) *user data imported for encryption according to FCS_COP.1/HEM shall be imported with the attribute Key identity of the public key encryption key or key agreement method,*
(3) *user data imported for decryption according to FCS_COP.1/HDM shall be imported with the attribute Key identity of the asymmetric decryption key, encrypted seed and data integrity check sum,*
(4) *user data imported for digital signature creation shall be imported with the attribute Key identity of the private signature key,*
(5) *user data imported for digital signature verification shall be imported with digital signature and Key identity of the public signature key*[314]*.*

Application note 28 ([PP-CSPLight]**)**

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

FDP_ETC.2 Export of user data with security attributes

Hierarchical to: No other components.

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

FDP_ETC.2.1 The TSF shall enforce the *Cryptographic Operation SFP*[315] 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 the key decryption key, encrypted data encryption key and data integrity check sum,*
(2) *user data exported as plaintext according to FCS_COP.1/HDM shall be exported only if the MAC verification confirmed the integrity of the ciphertext,*
(3) *user data exported as signed data according to FCS_COP.1/CDS-ECDSA or FCS_COP.1/CDS-RSA shall be exported with a digital signature and Key identity of the used signature-creation key*[316]*.*

Application note 29 ([PP-CSPLight]**)**

[314] [PP-CSPLight] [assignment: *additional importation control rules*]

[315] [PP-CSPLight] [assignment: *access control SFP, information flow control SFP*]

[316] [PP-CSPLight] [assignment: *additional exportation control rules*]

In case of internally generated data exported as signed data, the Key identity of the used key should be exported as well in order to identify the corresponding signature-verification key. Note that 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*[317] when exporting user data **as plaintext according to FCS_COP.1/HDM**, controlled under the SFP(s), outside of the TOE.
FDP_ETC.1.2	The TSF shall export the ~~user data~~ **successfully MAC verified and decrypted ciphertext as plaintext according to FCS_COP.1/HDM** without the user data's associated security attributes.

FDP_ACC.1/Oper Subset access control – Cryptographic operation

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/Oper	The TSF shall enforce the *Cryptographic Operation SFP*[318] on (1) *subjects: Administrator*[319]*, Key Owner, no other roles*[320]*;* (2) *objects: operational cryptographic keys, user data;* (3) *operations: cryptographic operation*[321]

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*[322] to objects based on the following: (1) *subjects: subjects with security attribute Role Administrator*[323]*, Key Owner, no other roles*[324]*;* (2) *objects:*

317 [PP-CSPLight] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

318 [PP-CSPLight] [assignment: *access control SFP*]

319 *[selection: Administrator, Crypto-Officer]*

320 *[assignment: other roles]*

321 [PP-CSPLight] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

322 [PP-CSPLight] [assignment: *access control SFP*]

323 *[selection: Administrator, Crypto-Officer]*

324 *[assignment: other roles]*

(a) *cryptographic keys with security attributes: Identity of the key, Key owner, Key type, Key usage type, Key access control attributes, Key validity time period;*
(b) *user data*[325]*.*

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) A *Subject in Administrator*[326] *role is allowed to perform cryptographic operations on cryptographic keys in accordance with their security attributes.*
(2) The *Subject Key Owner is allowed to perform cryptographic operations on user data with cryptographic keys in accordance with the security attribute Key owner, Key type, Key usage type, Key access control attributes and Key validity time period;*
(3) *No further rules*[327,328]*.*

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

(1) *subjects with the security attribute Role are allowed to perform cryptographic operations on user data and cryptographic keys with security attributes as shown in the rows of Table 6.*
(2) *No further rules*[329]*.*

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

(1) *No subject is allowed to use cryptographic keys by cryptographic operation other than those identified in the security attributes Key usage type and the Key access control attributes;*
(2) *No subject is allowed to decrypt ciphertext according to FCS_COP.1/HDM if MAC verification fails.*
(3) *No further rules.*[330,331]

Access control rules for cryptographic operation:

[325] [PP-CSPLight] [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*]

[326] *[selection: Administrator, Crypto-Officer]*

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

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

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

[330] [PP-CSPLight] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

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

Security attribute Role of the subject	Security attribute of the cryptographic key	Cryptographic operation referenced by SFR allowed for the subject on user data with the cryptographic key
Administrator[332]	Key type: symmetric Key usage type: Key wrap Key validity time period:	FCS_COP.1/KW
Administrator[333]	Key type: symmetric Key usage type: Key unwrap Key validity time period:	FCS_COP.1/KU
(any authenticated user)	Key type: public Key usage type: ECKA-EG Key validity time period: as in certificate	FCS_COP.1/HEM, FCS_CKM.1/ECKA-EG
Key Owner	Key type: private Key usage type: ECKA-EG Key validity time period:	FCS_COP.1/HDM FCS_CKM.5/ECKA-EG
(any authenticated user)	Key type: public Key usage type: RSA_ENC Key validity time period: as in certificate	FCS_COP.1/HEM FCS_CKM.1/AES_RSA
Key Owner	Key type: private Key usage type: RSA_ENC Key validity time period: as in certificate	FCS_COP.1/HDM FCS_CKM.5/AES_RSA
Key Owner	Key type: private Key usage type: DS-ECDSA Key validity time period:	FCS_COP.1/CDS-ECDSA
(any authenticated user)	Key type: public Key usage type: DS-ECDSA Key validity time period:	FCS_COP.1/VDS-ECDSA
Key Owner	Key type: private Key usage type: DS-RSA Key validity time period:	FCS_COP.1/CDS-RSA
(any authenticated user)	Key type: public Key usage type: DS-RSA Key validity time period:	FCS_COP.1/VDS-RSA

Table 6: Security attributes and access control

7.2.8 Security Management

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

[332] [selection: Administrator, Crypto-Officer, Key Owner]

[333] [selection: Administrator, Crypto-Officer, Key Owner]

FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: (1) *management of security functions behaviour (FMT_MOF.1),* (2) *management of Authentication reference data (FMT_MTD.1/RAD),* (3) *management of security attributes of cryptographic keys (FMT_MSA.1/KM, FMT_MSA.2, FMT_MSA.3/KM),* (4) *none*[334,335]*.*

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, Administrator*[336]*, Auditor, and Time keeper*[337,338]*.*
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Application note 30 ([PP-CSPLight]**)**
The ST selects more detailed administrator roles, *Administrator*, *Auditor* and *Time keeper*, as supported by the TOE.

FMT_MSA.2 Secure security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for *security attributes* (1) *Key identity,* (2) *Key type,* (3) *Key usage type,* (4) *None other*[339,340]*.* **The cryptographic keys shall have** **(1) a Key identity uniquely identifying the key among all keys implemented in the TOE,**

334 [PP-CSPLight] [assignment: *list of management functions to be provided by the TSF*]

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

336 *[selection: Administrator, Crypto-Officer, User Administrator, Update Agent]*

337 [PP-CSPLight] [assignment: *authorised identified roles*]

338 *[selection: [assignment: other roles], no other roles]*

339 [PP-CSPLight] [assignment: *list of security attributes*]

340 *[assignment: additional security attributes]*

(2) the Key type defined as exactly one of secret key, private key, or public key,

(3) a Key usage type identifying at least one cryptographic mechanism the key can be 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*[341] the functions *password authentication according to FIA_UAU.5.1, clause (1)*[342] to *Administrator*[343,344]. **(2) *disable*[345] the functions *password authentication according to FIA_UAU.5.1, clause (1)*[346] to *Administrator*[347,348],** **(3) *determine the behavior of*[349] the functions *trusted channel according to FDP_ITC.1.2*[350] by defining the remote trusted IT products permitted to initiate communication via the trusted channel to *Administrator*[351,352],** **(4) *determine the behavior of*[353] the functions *trusted channel according to FDP_ITC.1.3*[354] by defining the entities for which the TSF shall enforce communication via the trusted channel to *Administrator*[355,356].**

Application note 31 ([PP-CSPLight]**)**

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

---

341 [PP-CSPLight] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

342 [PP-CSPLight] [assignment: *list of functions*]

343 [PP-CSPLight] [assignment: *the authorised identified roles*]

344 *[selection: Administrator, User Administrator]*

345 [PP-CSPLight] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

346 [PP-CSPLight] [assignment: *list of functions*]

347 [PP-CSPLight] [assignment: *the authorised identified roles*]

348 ***[selection: Administrator, User Administrator]***

349 [PP-CSPLight] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

350 [PP-CSPLight] [assignment: *list of functions*]

351 [PP-CSPLight] [assignment: *the authorised identified roles*]

352 ***[selection: Administrator, User Administrator]***

353 [PP-CSPLight] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

354 [PP-CSPLight] [assignment: *list of functions*]

355 [PP-CSPLight] [assignment: *the authorised identified roles*]

356 ***[selection: Administrator, User Administrator]***

7.2.9 Protection of the TSF

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) *none other*[357].

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

FPT_TST.1 TSF testing

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests *during initial start-up and after power-on*[358] to demonstrate the correct operation of *integrity of TOE software and correct operation of cryptographic services*[359,360].
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of *TSF data*[361].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of *TSF **implementation***[362].

7.2.10 Import and verification of Update Code Package

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

[357] [*assignment*: list of types of additional failures]

[358] [PP-CSPLight] [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]*]

[359] [PP-CSPLight] [selection: *[assignment: parts of TSF], the TSF*]

[360] [assignment: *parts of TSF*]

[361] [PP-CSPLight] [selection: *[assignment: parts of TSF data], TSF data*]

[362] [PP-CSPLight] [selection: *[assignment: parts of TSF], TSF*]

	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*[363] 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) *encrypted Update Code Package are stored only after successful verification of authenticity according to FCS_COP.1/VDSUCP,* (2) *authentic Update Code Package are decrypted according to FCS_COP.1/DecUCP*[364]*.*

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*[365] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2/UCP	The TSF shall use **the following rules:** (1) *the Issuer must be identified and known,* (2) *the Version Number must be identified* when interpreting the TSF data from another trusted IT product.

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/VDSUCP The TSF shall perform *verification of the digital signature of the authorized Issuer*[366] in accordance with a specified cryptographic algorithm *ECDSA with*

[363] [PP-CSPLight] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[364] [PP-CSPLight] [assignment: *additional importation control rules*]

[365] [PP-CSPLight] [assignment: *list of TSF data types*]

[366] [PP-CSPLight] [assignment: *list of cryptographic operations*]

brainpoolP256r1[367] and cryptographic key sizes *256 bits*[368] that meet the following: *[RFC5639], [TR-03111] section 4.1.3*[369]

Application note 32 ([PP-CSPLight]**)**

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 the public key of the authorized Issuer shall be used for the verification of the digital signature of the Update Code Package.

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/DecUCP	The TSF shall perform *decryption of authentic encrypted Update Code Package*[370] in accordance with a specified cryptographic algorithm *AES block cipher in CBC mode with PKCS#5 padding*[371] and cryptographic key sizes *256 bits*[372] that meet the following: *[NIST-SP800-38A] chapter 6.2, [FIPS PUB 197]chapter 5 (AES block cipher in CBC mode)*[373].

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

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/UCP	The TSF shall enforce the *Update SFP*[374] on (1) *subjects: Administrator*[375]*;* (2) *objects: Update Code Package;* (3) *operations: import, store*[376]*.*

[367] [assignment: *cryptographic algorithm*]

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

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

[370] [PP-CSPLight] [assignment: *list of cryptographic operations*]

[371] [assignment: *cryptographic algorithm*]

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

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

[374] [PP-CSPLight] [assignment: *access control SFP*]

[375] *[selection: Administrator, Update Agent]*

[376] [PP-CSPLight] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

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

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/UCP	The TSF shall enforce the *Update SFP*[377] to objects based on the following: (1) *subjects: Administrator*[378]*;* (2) *objects: Update Code Package with security attributes Issuer and Version Number*[379]*.*
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) *Administrator*[380] *is allowed to import Update Code Package according to FDP_ITC.2/UCP.* (2) *Administrator*[381] *is allowed to store a Update Code Package if* *(a) authenticity is successfully verified according to FCS_COP.1/VDSUCP and the Update Code Package is decrypted according to FCS_COP.1/DecUCP* (b) *the Version Number of the Update Code Package is equal or higher than the Version Number of the TSF*[382]*.*
FDP_ACF.1.3/UCP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *no further rules*[383].
FDP_ACF.1.4/UCP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *no further rules*[384].

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***

[377] [PP-CSPLight] [assignment: *access control SFP*]

[378] *[selection: Administrator, Update Agent]*

[379] [PP-CSPLight] [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*]

[380] *[selection: Administrator, Update Agent]*

[381] *[selection: Administrator, Update Agent]*

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

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

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

Issuer according to FCS_COP.1/VDSUCP[385] the following objects: *received Update Code Package* [386].

7.2.11 Clustering

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

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

– initialization of secure channel between the Master-CSPLight and the Slave-CSPLight,

– transfer of TSF data as security attributes of known users and cryptographic keys with security attributes between Master-CSPLight and Slave-CSPLight using the application.

FDP_ACC.1/CL Subset access control – Clustering

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/CL	The TSF shall enforce the *Clustering SFP*[387] on (1) *subjects: Administrator;* (2) *objects: cluster keys, Authentication Data Records, cryptographic keys;* (3) *operations: generation, export, import*[388]*.*

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) *generate according to FCS_CKM.5/CLDH*[389] *the cluster keys*[390] to *Administrator*[391],

[385] [PP-CSPLight] [selection: *allocation of the resource to, deallocation of the resource from*]

[386] [PP-CSPLight][assignment: *list of objects*]

[387] [PPM-Cl][assignment: *access control SFP*]

[388] [PPM-Cl][assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

[389] [PPM-Cl][selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

[390] [PPM-Cl][assignment: *list of TSF data*]

[391] [PPM-Cl] [assignment: *the authorised identified roles*]

(2) ***export from the Master-CSPLight according to FPT_ESA.1/CL, FPT_TCT.1/CL and FPT_TIT.1/CL[392] the Authentication Data Records[393]*** **to** ***Application Component, Administrator[394,395]*****,**

(3) ***import into Slave-CSPLights according to FPT_ISA.1/CL, FPT_TCT.1/CL and FPT_TIT.1/CL[396] the Authentication Data Records[397]*** **to** ***Application Component, Administrator[398,399]***

(4) ***export from the Master-CSPLight according to FPT_ESA.1/CL, FPT_TCT.1/CL and FPT_TIT.1/CL[400] the cryptographic keys[401]*** **to** ***Application Component, Administrator[402,403]*****,**

(5) ***import into Slave-CSPLights according to FPT_ISA.1/CL, FPT_TCT.1/CL and FPT_TIT.1/CL[404] the cryptographic keys [405]*** **to** ***Application Component, Administrator[406,407].***

Application note 1 ([PPM-Cl]**)**

Authentication Data Records and cryptographic keys are TSF data. 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 further iterations of the component FMT_MTD.1.1/CL and therefore printed in bold.

FCS_CKM.5/CLDH Cryptographic key derivation – Cluster keys

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/CLDH	The TSF shall derive cryptographic *cluster keys*[408] from an agreed *shared secret*[409] in accordance with a specified cryptographic key derivation algorithm *anonymous DiffieHellman Key Agreement for*

[392] [PPM-Cl] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

[393] [PPM-Cl] [assignment: *list of TSF data*]

[394] [PPM-Cl] [assignment: *the authorised identified roles*]

[395] ***[selection: Application Component, Administrator, User Administrator]***

[396] [PPM-Cl] [selection: *change_default, query, modify, delete, clear,[assignment: other operations]*]

[397] [PPM-Cl] [assignment: *list of TSF data*]

[398] [PPM-Cl] [assignment: *the authorised identified roles*]

[399] ***[selection: Application Component, Administrator, User Administrator]***

[400] [PPM-Cl] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

[401] [PPM-Cl] [assignment: *list of TSF data*]

[402] [PPM-Cl] [assignment: *the authorised identified roles*]

[403] ***[selection: Application Component, Administrator, Crypto-Officer]***

[404] [PPM-Cl] [selection: *change_default, query, modify, delete, clear,[assignment: other operations]*]

[405] [PPM-Cl] [assignment: *list of TSF data*]

[406] [PPM-Cl] [assignment: *the authorised identified roles*]

[407] ***[selection: Application Component, Administrator, Crypto-Officer]***

[408] [PPM-Cl] [assignment: *key type*]

[409] [PPM-Cl] [assignment: *input parameters*]

ECC key pair generation with brainpoolP256r1[410,411] and specified cryptographic key sizes *256 bits*[412,413] that meet the following: *RFC5639[RFC5639], TR-03111, section 4.1.3[TR-03111] 256-bit random ECP group with IANA assigned ID value of 19 as specified in section 8.1 of [RFC5903]*[414,415].

Application note 2 ([PPM-Cl]**)**

The cryptographic cluster keys shall be used for encryption according to FCS_COP.1/ED (cf. Base-PP [PP-CSPLight]) and FPT_TCT.1/CL and MAC protection according to FCS_COP.1/MAC (cf. Base-PP) and FPT_TIT.1/CL during transfer of Authentication Data Records and the cryptographic keys between Master-CSPLight and Slave-CSPLight.

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]
FPT_TCT.1.1/CL	The TSF shall enforce the *Clustering SFP*[416] by providing the ability to *transmit and receive*[417] **Authentication Data Records and cryptographic keys** ~~TSF data~~ in a manner protected from unauthorised disclosure according to FCS_COP.1/ED.

Application note 3 ([PPM-Cl]**)**

FCS_COP.1/ED is defined in the Base-PP.

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]
FPT_TIT.1.1/CL	The TSF shall enforce the *Clustering SFP*[418] to *transmit and receive*[419] **Authentication Data Records and cryptographic keys** ~~TSF data~~ in a

[410] [PPM-Cl] [assignment: *cryptographic key derivation algorithm*]

[411] *[selection: elliptic curves in the Table 3[PP-CSPLight]]*

[412] [PPM-Cl] [assignment: *cryptographic key sizes*]

[413] *[selection: key size in the Table 3 [PP-CSPLight]]*

[414] [PPM-Cl] [assignment: *list of standards*]

[415] [selection: *standards in the Table 3 and Table 4[[PP-CSPLight],[TR-03111]]*

[416] [PPM-Cl] [assignment: *access control SFP, information flow control SFP*]

[417] [PPM-Cl] [selection: *transmit, receive, transmit and receive*]

[418] [PPM-Cl] [assignment: *access control SFP, information flow control SFP*]

[419] [PPM-Cl] [selection: *transmit, receive, transmit and receive*]

manner protected from *modification*[420] errors **according to FCS_COP.1/MAC**.

FPT_TIT.1.2/CL The TSF **in role Slave-CSPLight** shall be able to determine on receipt of **Authentication Data Records and cryptographic keys** ~~TSF data~~, whether *modification*[421] has occurred **according to FCS_COP.1/MAC**.

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

Hierarchical to: No other components.

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

FPT_ISA.1.1/CL The TSF **in role Slave-CSPLight** shall enforce the *Clustering SFP*[422] when importing **Authentication Data Records and cryptographic keys** ~~TSF data~~**,** controlled under the SFP, from ~~outside of the TOE~~ **Master-CSPLight**.

FPT_ISA.1.2/CL The TSF **in role Slave-CSPLight** 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-CSPLight** shall ensure that the protocol used provides for the unambiguous association between the security attributes and the **Authentication Data Records and cryptographic keys** ~~TSF data~~ received.

FPT_ISA.1.4/CL The TSF **in role Slave-CSPLight** shall ensure that interpretation of the security attributes of the imported **Authentication Data Records and cryptographic keys** ~~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-CSPLight** 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-CSPLight**:

(1) *TSF in role Slave-CSPLight always imports Authentication Data Records with security attributes from Master-CSPLight.*
(2) *TSF in role Slave-CSPLight imports cryptographic keys with security attributes from Master-CSPLight only if the security attribute Clustering of the key allows transfer*[423]*.*

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

Hierarchical to: No other components.

---

[420] [PPM-Cl] [selection: *modification, deletion, insertion, replay*]

[421] [PPM-Cl] [selection: *modification, deletion, insertion, replay*]

[422] [PPM-Cl] [assignment: *access control SFP, information flow control SFP*]

[423] [PPM-Cl] [assignment: *additional importation control rules*]

Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency
FPT_ESA.1.1/CL	The TSF **in role Master-CSPLight** shall enforce the *Clustering SFP*[424] when exporting **Authentication Data Records and cryptographic keys** ~~TSF data~~, controlled under the SFP(s), ~~outside of the TOE~~ **to Slave-CSPLight**.
FPT_ESA.1.2/CL	The TSF **in role Master-CSPLight** shall export the **Authentication 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-CSPLight** shall ensure that the security attributes, when exported ~~outside the TOE~~ **to Slave-CSPLight**, are unambiguously associated with the exported **Authentication Data Records and cryptographic keys** ~~TSF data~~.
FPT_ESA.1.4/CL	The TSF **in role Master-CSPLight** shall enforce the following rules when **Authentication Data Records and cryptographic keys** ~~TSF data~~ is exported ~~from the TOE~~ **to Slave-CSPLight**: (1) *TSF in role Master-CSPLight exports Authentication Data Records with security attributes to any Slave-CSPLight.* (2) *TSF in role Master-CSPLight exports cryptographic key with security attributes to Slave-CSPLight only if the security attribute Clustering of the key allows transfer*[425]*.*

FPT_TDC.1/CL Inter-TSF basic TSF data consistency – Clustering

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TDC.1.1/CL	The TSF shall provide the capability to consistently interpret *Authentication Data Records and cryptographic keys with their security attributes*[426] when shared between the TSF and **TOE sample in the cluster** ~~another trusted IT product~~.
FPT_TDC.1.2/CL	The TSF shall use the following rules: (1) *the TSF in Slave-CSPLight role shall interpret the imported Authentication Data Records with their security attributes in the same way as it interprets the Authentication Data Records when it exports them in Master-CSPLight role,* (2) *the TSF in Slave-CSPLight role shall interpret the imported cryptographic keys with their security attributes in the same way as it interprets the Authentication Data Records when it exports them in Master-CSPLight role,*[427]

[424] [PPM-Cl] [assignment: *access control SFP, information flow control SFP*]

[425] [PPM-Cl] [assignment: *additional exportation control rules*]

[426] [PPM-Cl] [assignment: *list of TSF data types*]

[427] [PPM-Cl][assignment: *list of interpretation rules to be applied by the TSF*]

when interpreting the **Authentication Data Records and cryptographic keys** ~~TSF data~~ from **Master-CSPLight** ~~another trusted IT product.~~

7.2.12 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*[428] level of audit; and c) *Discrete adjustment of the real time clock* (1) *by automatic adjustment of the clock according to FPT_STM.1.1 clause (2) if selected as auditable event,* (2) *by Administrator according to FPT_STM.1.1 clause (1) or (2),* (3) *failure of adjustment according to FPT_STM.1.1,* d) *other auditable events* (1) *Start-up after power-up,* (2) *Import of UCP (FDP_ITC.2/UCP),* (3) *Authentication failure handling (FIA_AFL.1/PINPUK, FIA_AFL.1/PASSWORD): the reaching of the threshold for the unsuccessful authentication attempts with claimed Identity of the user,* *(10)No other event*[429,430]*.*
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 (if applicable), 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, *none other*[431].

[428] [PPM-TS-Au] [selection: *choose one of: minimum, basic, detailed, not specified*]

[429] [PPM-TS-Au] [assignment: *other specifically defined auditable events*]

[430] *[selection:*

(4) *Generation of (selected types of) signature key pairs (all FCS_CKM.1 instantiations for generation of permanent stored keys)*
(5) *Execution of (selected types of) cryptographic operation (all FCS_COP.1 instantiations),*
(6) *Cryptographic key destruction (FCS_CKM.4) of permanent stored keys,*
(7) *Failure with preservation of secure state (FPT_FLS.1): entering and exiting secure state,*
(8) *Management of security functions (FMT_MOF.1, FMT_MOF.1/TSA),*
(9) *Management of TSF data (FMT_MTD.1/AUDIT): Export, clear and selection of events causing audit data],*
(10) *No other event,*
(11) *[assignment: additional specifically defined auditable events].*

[431] [assignment: *other audit relevant information*]

Application note 6 ([PPM-TS-Au]**)**

The SFR FDP_ITC.2/UCP, FIA_AFL.1, FCS_CKM.1, FCS_COP.1, FCS_CKM.4, FPT_FLS.1 and FMT_MOF.1 are defined in the Base-PP. The SFR FPT_STM.1, FMT_MOF.1/TSA and FMT_MTD.1/Audit are defined in [PPM-TS-Au].

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 FAU_GEN.1,* (4) *define the number of audit records causing automatic export and clearing of exported audit records according to FAU_STG.3.1 clause(1),* (5) *define the percentage of storage capacity of audit records if actions are assigned in FAU_STG.3.1 clause (2)*[432] the *audit records*[433] to *Administrator*[434,435].

Application note 7 ([PPM-TS-Au]**)**

The selection of auditable events according to FMT_MTD.1.1/Audit, clause (3) enables or disables or specifies the generation of audit records as defined in FAU_GEN.1. The role *Administrator* may be selected only if it is selected in FMT_SMR.1 in the Base-PP and any conflict of duties is prevented (cf. application note to FMT_SMR.1/TSA).

FAU_STG.1 Protected audit trail storage

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to *prevent*[436] 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.

[432] [PPM-TS-Au] [selection: *change_default, query, modify, delete, clear,[assignment: other operations]*]

[433] [PPM-TS-Au] [assignment: *list of TSF data*]

[434] [PPM-TS-Au] [assignment: *the authorised identified roles*]

[435] *[selection: Auditor, Administrator]*

[436] [PPM-TS-Au] [selection, *choose one of: prevent, detect*]

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*[437] if the audit trail exceeds *an* *Administrator* [438] *defined number of audit records within* *1 to 1 days* [439,440] (2) *delete exported audit records older than 90 days* [441] **if the audit trail exceeds an *Administrator* [442] *settable percentage of storage capacity*[443]*.***

Application note 8 ([PPM-TS-Au]**)**

Since the number of audit records in clause (1) is set to 1 day, the TSF export each audit record automatically every day. Before reaching the defined percentage of storage capacity a warning is issued to an Administrator.

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** **(2) *internal clock with accuracy 3 seconds*[444] *with automatic adjustment of the clock by an externally trustable source in a cryptographically verifiable manner (e.g. by signed Network Time Protocol) and the ability of adjustment of the clock by the Timekeeper*[445]*.***

Application note 9 ([PPM-TS-Au]**)**

The external trustable source (e.g. signed Network Time Protocol) provides a reliable time source for adjustment of the internal clock. The time intervals of adjustments in clause (2) may be configured by the Administrator. Any adjustment or failure of adjustment of the internal clock is an auditable event according to FAU_GEN.1.1. The refinement with selection defines different cases for internal clocks and are therefore printed in bold.

Note that it is not expected that the internal clock continues to operate when the TOE is switched off. An implementation that e.g. counts CPU ticks with sufficient accuracy while switched on would suffice to fulfil the requirements, provided that all auditable events are logged properly.

---

[437] [PPM-TS-Au] [assignment: *actions to be taken in case of possible audit storage failure*]

[438] *[selection: Administrator, Auditor]*

[439] [PPM-TS-Au] [assignment: *pre-defined limit*]

[440] *[assignment: pre-defined range]*

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

[442] ***[selection: Administrator, Auditor]***

[443] [PPM-TS-Au] [assignment: *pre-defined limit*]

[444] ***[assignment: approximate deviation]***

[445] ***[selection: Administrator, Timekeeper]***

FPT_TIT.1/Audit TSF data integrity transfer protection – Audit functionality

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]
FPT_TIT.1.1/Audit	The TSF shall enforce the *Update SFP, Cryptographic Operation SFP*[446,447] to *transmit*[448] TSF data **audit records** in a manner protected from *modification, deletion, insertion and replay*[449] *errors.*
FPT_TIT.1.2/Audit	The TSF shall be able to determine on receipt of TSF data **time**, whether *modification*[450] has occurred.

Application note 10 ([PPM-TS-Au]**)**

The Update SFP is enforced by the export of audit records about import of UCP, cf. FAU_GEN.1.1 clause d) (2). The selection of the Key Management SFP or Cryptographic Operation SFP depends on the selection of auditable events of key management, cryptographic operations and adjustment of the internal clock (e. g. used for verification of validity time period) in FAU_GEN.1.1 clause c). The TSF transmits audit records and receives time as TSF data for security audit. The TSF protects the audit records by means of digital signature against modification and by means of time stamps and key usage counter of the signature key as part of the signature against deletion, insertion and replay as required in FPT_TIT.1.1.

FAU_GEN.1/CL Audit data generation

Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps
FAU_GEN.1.1/CL	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*[451] level of audit; and *c) other auditable events* (1) *Generation of cluster keys for the secure channel according to FMT_MTD.1/CL and FCS_CKM.5/CLDH,* (2) *Export of Authentication Data Records and cryptographic keys from the Master-CSPLight according to FPT_ESA.1.3/CL,Management of Authentication Data Records (FMT_MTD.1/RAD): creation and deletion of Authentication Data Record,*

[446] [PPM-TS-Au] [assignment: *access control SFP*]

[447] *[selection: Key Management SFP, Cryptographic Operation SFP]*

[448] [PPM-TS-Au] [selection: *transmit, receive, transmit and receive*]

[449] [PPM-TS-Au] [selection: *modification, deletion, insertion, replay*]

[450] [PPM-TS-Au] [selection: *modification, deletion, insertion, replay*]

[451] [PPM-Cl][selection: *choose one of: minimum, basic, detailed, not specified*]

(3) *Import according to FPT_ISA.1/CL of Authentication Data Records and cryptographic keys into Slave-CSPLight.*[452].

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, *none other*[453].

Application note 5 ([PPM-Cl]**)**

The SFR FAU_GEN.1/CL adds auditable events to FAU_GEN.1 required by [PPM-TS-Au]. The SFR FPT_STM.1 is required by [PPM-TS-Au].

7.2.13 Time Stamp

FDP_DAU.2/TS Data Authentication with Identity of Guarantor – Signature with time stamp and optional key usage counter

Hierarchical to: FDP_DAU.1 Basic Data Authentication

Dependencies: FIA_UID.1 Timing of identification

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 records according to FMT_MTD.1/Audit clause (1) and FAU_STG.3 clause (1)*[454]

with

(1) time stamp of the evidence generation according to FPT_STM.1,
(2) and optionally the key usage counter of the signature key by means of digital signature generated according to *FCS_COP.1/CDS-ECDSA*[455] and keys holding the dedicated values of the security attributes Key identity that indicate key ownership of the TOE sample and Key usage type "Time stamp service".

FDP_DAU.2.2/TS The TSF shall provide *Administrator*[456] 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 1 ([PPM-TS-Au]**)**

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

[452] [PPM-Cl][assignment: *other specifically defined auditable events*]

[453] [assignment: other audit relevant information]

[454] [PPM-TS-Au] [assignment: *list of objects or information types*]

[455] **[selection: *FCS_COP.1/CDSECDSA, FCS_COP.1/CDS-RSA*]**

[456] [assignment: *list of subjects*]

signature key of exported audit records shall be defined according to FMT_MOF.1.1/TSA clause (5). 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 [TR-03151].

7.2.14 Access control on time stamp service

FDP_ITC.2/TS Import of user data with security attributes – User data for time stamping

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/TS	The TSF shall enforce the *Cryptographic Operation SFP*[457] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2/TS	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/TS	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/TS	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/TS	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: (1) *user data imported for time stamp generation to FDP_DAU.2/TS shall be imported with security attributes Key identity of the signature key and Key usage type TimeStamp, and the identification of the requested cryptographic operation*[458]*.*

Application note 2 ([PPM-TS-Au]**)**

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

FDP_ETC.2/TS Export of user data with security attributes - User data with time stamp

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

[457] [PPM-TS-Au][assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[458] [PPM-TS-Au][assignment: *additional importation control rules*]

FDP_ETC.2.1/TS The TSF shall enforce the *Cryptographic Operation SFP*[459] when exporting user data, controlled under the SFP(s), outside of the TOE.

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

FDP_ETC.2.3/TS 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/TS The TSF shall enforce the following rules when user data is exported from the TOE:

(1) *user data exported as time stamped data according to FDP_DAU.2/TS shall be exported with digital signature and Key identity of the used signature-creation key*[460]*.*

Application note 3 ([PPM-TS-Au]**)**

In case of internally generated data (e.g. audit records) the exported signed data shall be attributed with the *Key identity* of the used signature-creation key. Note that the TOE may implement more than one signature-creation key for signing internally generated data.

FDP_ACF.1/TS 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/TS The TSF shall enforce the *Cryptographic Operation SFP*[461] to objects based on the following:

(1) *subjects: subjects with security attribute Role Application Component, none other*[462]*;*
(2) *objects: user data*[463]*.*

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

(1) *Application Component, none other*[464] *is allowed to perform cryptographic operation according to FDP_DAU.2/TS on user data with cryptographic keys with Key usage type TimeStamp.*

[459] [PPM-TS-Au][assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[460] [PPM-TS-Au][assignment: *additional exportation control rules*]

[461] [PPM-TS-Au][assignment: *access control SFP*]

[462] *[assignment: other roles]*

[463] [PPM-TS-Au][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*]

[464] *[assignment: other roles]*

(2) *No other rules*[465,466].

FDP_ACF.1.3/TS The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *no further rules*[467].

FDP_ACF.1.4/TS 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 attributes;*
(2) *No further rules.*[468,469]

7.2.15 Security Management – Time stamp and audit

FMT_SMF.1/TSA Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

(1) *management of security functions behaviour FMT_MOF.1/TSA*[470].

FMT_SMR.1/TSA Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1/TSA The TSF shall maintain the roles **additional to those required by FMT_SMR.1 in the Base-PP**: *Auditor, Timekeeper*[471,472].

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

Application note 4 ([PPM-TS-Au]**)**

The ST selects the following more detailed Administrator roles as supported by the TOE:

– *Auditor* role in FMT_SMR.1/TSA separated from Administrator roles selected in the SFR FMT_SMR.1 according to the Base-PP and,

---

[465] [PPM-TS-Au][assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

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

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

[468] [PPM-TS-Au][assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

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

[470] [PPM-TS-Au][assignment: *list of management functions to be provided by the TSF*]

[471] [PPM-TS-Au][assignment: *authorised identified roles*]

[472] *[selection: Auditor, Timekeeper, no other roles]*

– *Timekeeper* role in FMT_SMR.1/TSA separated from Administrator roles selected in the SFR FMT_SMR.1 according to the Base-PP.

The assignment of security management of audit and other functions are performed in a way which does not result in a conflict of duties with the roles defined in FMT_SMR.1.

FMT_MOF.1/TSA 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/TSA	The TSF shall restrict the ability to

(1) *modify the behaviour of*[473] the functions *adjustment of the internal clock according to FPT_STM.1 clause (1)*[474] to *Timekeeper*[475,476]

(2) *modify the behaviour of*[477] the functions *adjustment of the internal clock according to FPT_STM.1 clause (2)*[478] to *Timekeeper*[479,480],

(3) *determine the behaviour of and modify the behaviour of*[481] the functions *select the auditable events according to FAU_GEN.1*[482] *to Auditor*[483,484],

(4) *determine the behaviour of and modify the behaviour of*[485] *the functions automatic export of audit trails according to FAU_STG.3.1 clause (1)*[486] to *Administrator*[487,488]

(5) *determine the behaviour of and modify the behaviour of*[489] the functions *FDP_DAU.2/TS by selection of signature key used to sign exported audit trails*[490] to *Administrator*[491,492].

---

[473] [PPM-TS-Au] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

[474] [PPM-TS-Au] [assignment: *list of functions*]

[475] [PPM-TS-Au] [assignment: *the authorised identified roles*]

[476] *[selection: Administrator, Timekeeper]*

[477] [PPM-TS-Au] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

[478] [PPM-TS-Au] [assignment: *list of functions*]

[479] [PPM-TS-Au] [assignment: *the authorised identified roles*]

[480] ***[selection: Administrator, Timekeeper]***

[481] [PPM-TS-Au] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

[482] [PPM-TS-Au] [assignment: *list of functions*]

[483] [PPM-TS-Au] [assignment: *the authorised identified roles*]

[484] ***[selection: Administrator, Auditor]***

[485] [PPM-TS-Au] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

[486] [PPM-TS-Au] [assignment: *list of functions*]

[487] [PPM-TS-Au] [assignment: *the authorised identified roles*]

[488] ***[selection: Administrator, Auditor]***

[489] [PPM-TS-Au] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

[490] [PPM-TS-Au] [assignment: *list of functions*]

[491] [PPM-TS-Au] [assignment: *the authorised identified roles*]

[492] ***[selection: Administrator, Auditor]***

Application note 5 ([PPM-TS-Au]**)**

The SFR defines additional management of security functions behaviour for new SFR with respect to the Base-PP. The refinements of FMT_MOF.1.1/TSA in bullets (2) to (5) are made in order to avoid further iterations of the component. The management of security functions for audit should only be used in exceptional cases.

7.3 Security Assurance Requirements

The security assurance requirement level is **EAL2** augmented with ALC_CMS.3 (Implementation representation CM coverage) and ALC_LCD.1 (Developer-Defined Lifecycle Model) and with specific refinements on ALC_CMS.3, ADV_ARC.1 and ATE_IND.2. The assurance components are identified in the table below (with augmentations in bold).

Assurance Class	Assurance Components
Security Target (ASE)	ST introduction (ASE_INT.1)
	Conformance claims (ASE_CCL.1)
	Security problem definition (ASE_SPD.1)
	Security objectives (ASE_OBJ.2)
	Extended components definition (ASE_ECD.1)
	Derived security requirements (ASE_REQ.2)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Security architecture description (ADV_ARC.1)
	Complete functional specification (ADV_FSP.2)
	Basic modular design (ADV_TDS.1)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life cycle support (ALC)	Production support, acceptance procedures and automation (ALC_CMC.2)
	Implementation representation CM coverage (ALC_CMS.3)
	Developer-Defined Lifecycle Model (ALC_LCD.1)
	Delivery procedures (ALC_DEL.1)
Tests (ATE)	Functional testing (ATE_FUN.1)
	Analysis of coverage (ATE_COV.1)
	Independent testing – sample (ATE_IND.2)
Vulnerability assessment	Vulnerability analysis (AVA_VAN.2)

Table 7: Security Assurance Requirements

7.3.1 Assurance Refinements

Refinement on ALC_CMS.3.1C:

The implementation representation listed shall comprise the implementation representation of the TOE defining the TSF to a level of detail such that the compliance of the TOE and TSF to the requirements imposed by the platform guidances on which the TOE is designed to run on, can be verified by that evidence.

Refinement on ADV_ARC.1.3D:

The security guidance documentation of each platform (hardware platform and operating system) on which the TOE is designed to run shall be provided in addition.

Refinement on ADV_ARC.1.1C to 1.5C:

The security architecture description shall include an assessment how each single security requirement imposed by the platform documentation (guidance documentation and if available evaluation or certification results) has been followed in the TOE design and implementation concept.

Examples for such security requirements could include but are not limited to:

– Dedicated library calls: Dedicated calls protecting against attacks may be provided by the platform for cryptographic operation. For example, dedicated calls implement operations that are hardened against timing side channel attacks, while others execute faster, but are not hardened. The platform guidance may require such library calls to be used.

– Key usage limitations: Key usage above a certain limit may reveal side channel information which can then be exploited. The implementation must ensure that the key usage limit is adhered to.

– Dedicated calls to ensure a correct program flow are provided (i.e. for boolean verification calls) to ensure protection against attacks that disturb the execution flow. Such library calls must be made use of in critical operations.

– Dedicated library calls are provided for the secure generation of cryptographic random numbers. Other random number generation functionality is present, but is not suitable to generate cryptographic random numbers. It must be ensured that correct random number generation library calls are used.

Refinement on ADV_ARC.1.1E:

The evaluators task includes to check consistency of the requirements considered in the architectural description against those outlined in the platform documentation.

Refinement on ATE_IND.2.1D:

Providing the TOE for testing shall include in addition the implementation representation of the TOE as defined by ALC_CMS.3.

Refinement of ATE_IND.2.2C:

The resources provided shall include additionally appropriate tools or access to the TOE development environment in order to enable the evaluator to perform source code review most efficiently.

Refinement of ATE_IND.2.3E:

The evaluators test activities shall include a verification of the TOE implementation representation provided in order to confirm code compliance of the TOE implementation representation to the security guidance of the hardware platform and operating system and libraries which the TOE/TSF is intended to be run on. Therefore, the evaluator shall assess and verify that all platform guidance requirements are met and indicate possible vulnerabilities to the AVA evaluation activity for the TOE for further consideration.

8 Rationales

8.1 Security Objectives Rationale

8.1.1 Security Objectives Rationale

The table below shows the mapping of Threats, Organisational Security Policies and Assumptions to Security Objectives for the TOE and for the TOE Environment.

	T.DataCompr	T.DataMani	T.Masqu	T.ServAcc	T.PhysAttack	T.FaUpD	OSP.SecCryM	OSP.SecService	OSP.KeyMan	OSP.TC	OSP.Update	OSP.SecCryM	OSP.Cluster	OSP.Audit	OSP.TimeService	A.SecComm	A.ClusterAppl
O.AccCtrl				X													
O.AuthentTOE							X	X									
O.DataAuth		X					X	X									
O.Enc	X						X	X									
O.I&A			X	X			X	X									
O.RBGS							X	X									
O.SecMan			X				X		X	X							
O.SecUpCP						X					X						
O.TChann	X	X	X	X			X	X									
O.TST					X												
O.Cluster												X	X				
O.Audit														X			
O.TimeService															X		
OE.AppComp	X	X		X						X							
OE.CommInf	X	X		X				X	X	X							
OE.SecComm	X	X		X												X	
OE.SecManag			X					X	X								
OE.SUCP						X					X						
OE.SecPlatform					X												
OE.ClusterCtrl													X				
OE.TSFdataTran													X				X
OE.Audit														X			

	T.DataCompr	T.DataMani	T.Masqu	T.ServAcc	T.PhysAttack	T.FaUpD	OSP.SecCryM	OSP.SecService	OSP.KeyMan	OSP.TC	OSP.Update	OSP.SecCryM	OSP.Cluster	OSP.Audit	OSP.TimeService	A.SecComm	A.ClusterAppl
OE.TimeSource															X		

Table 8: Security objective rationale

8.1.2 Security Objectives Sufficiency

The following paragraphs describe the rationale for the sufficiency of the Security Objectives relative to the Threats, OSPs and Assumptions.

8.1.2.1 Threats

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 a security service for the users to protect the confidentiality of user data,
- O.TChann requires the TOE to support establishing a trusted channel between the TSF and the application component, between the TSF and other users, and between the application component and other users. The trusted channel ensures authentication of all communication end points, and protected communication for the confidentiality and integrity of the communication and to prevent misuse of sessions of authorized users.
- OE.AppComp requires the application component to support the TOE for communication with users and trust centres.
- OE.CommInf requires the operational environment to provide a communication infrastructure; especially w.r.t. trust centre services.
- OE.SecComm requires the operational environment to protect the confidentiality and integrity of communication over local communication channels by physical security measures, and requires 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, the operational environment shall protect the communication, cf. A.SecComm and OE.SecComm. Note that OE.SecComm requires measures that the operational environment must be subject to a security audit that verifies that the communication between the TOE and the application is indeed protected.

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 a security service for the users to protect the integrity and authenticity of user data.
- O.TChann requires the TOE to support trusted channels for the authentication of all communication end points, for the protected communication with the application component, and for other users. This ensures the confidentiality and integrity of the

communication between the TOE and the other parties and prevents misuse of sessions of authorized users.

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

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

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

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

- O.I&A requires the TSF to uniquely identify users and to authenticate users before providing access to any controlled resources.
- O.AccCtrl requires the TSF to control access of security services, operations on user data, and management of TSF and TSF data.
- O. TChann requires mutual authentication of the external entity and the TOE, and the authentication of communicated data between them to prevent misuse of the communication with external entities. The operational environment is required by OE.SecComm to ensure that a secure channel is available if a trusted channel cannot be established.
- The operational environment OE.CommInf requires the provision of a public key infrastructure for entity authentication. OE.AppComp requires the application to support the communication with trust centres.

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

- OE.SecPlatform ensures that the TOE runs on a secure hardware platform and operating system that provides protection against physical attacks.
- As means to ensure robustness against perturbation O.TST requires the TSF to perform self-tests and to enter a secure state if the 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 UCPs are signed as required by OE.SUCP.

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

8.1.2.2 Organisational Security Policies

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” which require secure entity authentication of users and the TOE,
- O.Enc “Confidentiality of user data by means of encryption and decryption” and O.DataAuth ”Data authentication by cryptographic mechanisms” require secure cryptographic mechanisms for protection of the confidentiality and integrity of user data,
- O.TChann “Trusted channel” require secure cryptographic mechanisms for entity authentication of users and the TOE, and the protection of confidentiality and integrity of communication data.
- O.RBGS “Random bit generation service” requires the TOE to provide a cryptographically secure random bit generation service for the users.
- O.SecMan “Security management” requires secure management of TSF data and cryptographic keys by means of secure cryptographic mechanisms and 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”, which require the TSF to provide cryptographic security services for the user. The OSP.SecService is supported by OE.CommInf “Communication infrastructure” and OE.SecManag “Security management” which provide the necessary measures 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 centre services according to OE.CommInf “Communication infrastructure” and OE.SecManag “Security management”.

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

- O.SecMan “Security management” uses certificates for secure management of users, TSF, TSF data and cryptographic keys.
- OE.CommInf “Communication infrastructure” requires trust centres to generate secure certificates for trustworthy certificate holders 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 the communication with trust centres.

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

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

- O.Cluster “Cluster” requiring secure transfer in encrypted and integrity protected form of the security attributes of the known users and the cryptographic keys with their security attributes between Master-CSPLight and Slave-CSPLights.

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 CSPLights with distribution of Authentication Data Records and cryptographic keys between Master-CSPLight and Slave-CSPLights 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.ClusterCtrl requiring administrator to build a cluster only of trustworthy samples of the TOE as needed for scalability of performance and availability of security services.
- OE.TSFdataTrans requires the administrator and the application using the security services of the TOE transfer security attributes of the known users and cryptographic keys with their security attributes between Master-CSPLight and Slave-CSPLights as necessary for scalability of performance and availability of security services.

The organizational security policy OSP.Audit “Audit for key management and cryptographic operations” is directly implemented by

- the security objective for the TOE O.Audit requiring security auditing and
- the security objective for the operational environment OE.Audit requiring the regular audit review and the availability of exported audit records.

The organizational security policy OSP.TimeService “Time Service and Time stamp service” is directly implemented by

- the security objective for the TOE O.TimeService “Time services ” requiring the TOE to provide an internal time service and time stamp service for the user, and
- the security objective for the operational environment OE.TimeSource “External time source” requiring the operational environment to provide reliable external time stamps for adjustment of TOE internal time source.

8.1.2.3 Assumptions

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 require the operational environment to protect local communication physically or via trusted channel, and remote entities to support trusted channels using cryptographic mechanisms.

The assumption A.ClusterAppl is directly ensured by OE.TSFdataTrans.

8.2 Security Requirements Rationale

8.2.1 Security functional requirements rationale

Table 9 traces each SFR back to the security objectives for the TOE.

	O.I&A	O.AuthentTOE	O.Enc	O.DataAuth	O.RBGS	O. TChann	O.AccCtrl	O.SecMan	O.TST	O.SecUpCP	O.Audit	O.Cluster	O.TimeService
FAU_GEN.1											X		
FAU_GEN.1/CL											X		
FAU_STG.1											X		
FAU_STG.3											X		
FCS_CKM.1/AES			X	X				X					
FCS_CKM.1/AES_RSA			X	X				X					
FCS_CKM.1/ECC		X	X	X				X					
FCS_CKM.1/ECKA-EG			X	X				X					
FCS_CKM.1/PACE		X				X		X					
FCS_CKM.1/RSA		X	X	X				X					
FCS_CKM.1/TCAP		X				X		X					
FCS_CKM.4			X	X				X					
FCS_CKM.5/AES			X	X				X					
FCS_CKM.5/AES_RSA			X	X				X					
FCS_CKM.5/ECC			X	X				X					
FCS_CKM.5/ECDHE			X	X				X					
FCS_CKM.5/ECKA-EG			X	X				X					
FCS_CKM.5/CLDH												X	
FCS_COP.1/CDS-ECDSA		X		X									

	O.I&A	O.AuthentTOE	O.Enc	O.DataAuth	O.RBGS	O. TChann	O.AccCtrl	O.SecMan	O.TST	O.SecUpCP	O.Audit	O.Cluster	O.TimeService
FCS_COP.1/CDS-RSA		X		X									
FCS_COP.1/DecUCP										X			
FCS_COP.1/ED			X					X					
FCS_COP.1/Hash				X				X					
FCS_COP.1/HDM			X	X									
FCS_COP.1/HEM			X	X									
FCS_COP.1/HMAC		X		X									
FCS_COP.1/KU								X					
FCS_COP.1/KW								X					
FCS_COP.1/MAC				X									
FCS_COP.1/TCE						X							
FCS_COP.1/TCM						X							
FCS_COP.1/VDS-ECDSA				X									
FCS_COP.1/VDS-RSA				X									
FCS_COP.1/VDSUCP										X			
FCS_RNG.1					X			X					
FDP_ACC.1/KM							X	X					
FDP_ACC.1/Oper							X						
FDP_ACC.1/UCP										X			
FDP_ACC.1/CL												X	
FDP_ACF.1/Oper							X						
FDP_ACF.1/UCP										X			

	O.I&A	O.AuthentTOE	O.Enc	O.DataAuth	O.RBGS	O. TChann	O.AccCtrl	O.SecMan	O.TST	O.SecUpCP	O.Audit	O.Cluster	O.TimeService
FDP_ACF.1/TS													X
FDP_DAU.2/Att		X											
FDP_DAU.2/Sig				X									
FDP_DAU.2/TS											X		X
FDP_ETC.1				X									
FDP_ETC.2			X	X									
FDP_ETC.2/TS													X
FDP_ITC.2/UCP										X			
FDP_ITC.2/UD			X	X									
FDP_ITC.2/TS													X
FDP_RIP.1/UCP										X			
FIA_AFL.1/PINPUK	X												
FIA_AFL.1/PASSWORD	X												
FIA_API.1/CA	X	X				X							
FIA_API.1/PACE	X	X				X							
FIA_ATD.1	X						X	X					
FIA_UAU.1	X												
FIA_UAU.5	X					X							
FIA_UAU.6	X												
FIA_UID.1	X												
FIA_USB.1	X												
FMT_MOF.1	X					X							

	O.I&A	O.AuthentTOE	O.Enc	O.DataAuth	O.RBGS	O. TChann	O.AccCtrl	O.SecMan	O.TST	O.SecUpCP	O.Audit	O.Cluster	O.TimeService
FMT_MSA.1/KM			X	X		X	X	X					
FMT_MSA.2							X	X					
FMT_MSA.3/KM							X	X		X			
FMT_MTD.1/Audit											X		
FMT_MTD.1/KM								X					
FMT_MTD.1/RAD	X												
FMT_MTD.1/RK	X		X	X				X					
FMT_MTD.1/CL												X	
FMT_MTD.3	X												
FMT_MOF.1/TSA													X
FMT_SAE.1	X												
FMT_SMF.1								X					
FMT_SMF.1/TSA											X		X
FMT_SMR.1	X							X					
FMT_SMR.1/TSA											X		X
FPT_ESA.1/CK								X					
FPT_ESA.1/CL												X	
FPT_FLS.1									X				
FPT_ISA.1/Cert	X			X				X		X			
FPT_ISA.1/CK								X					
FPT_ISA.1/CL												X	
FPT_STM.1											X		X

	O.I&A	O.AuthentTOE	O.Enc	O.DataAuth	O.RBGS	O. TChann	O.AccCtrl	O.SecMan	O.TST	O.SecUpCP	O.Audit	O.Cluster	O.TimeService
FPT_TCT.1/CK								X		X			
FPT_TCT.1/CL												X	
FPT_TDC.1/CK			X	X				X					
FPT_TDC.1/CL												X	
FPT_TDC.1/Cert	X		X	X				X					
FPT_TDC.1/UCP										X			
FPT_TIT.1/Audit											X		
FPT_TIT.1/Cert	X			X				X		X			
FPT_TIT.1/CK								X					
FPT_TIT.1/CL												X	
FPT_TST.1									X				
FTP_ITC.1						X							

Table 9: Security functional requirement rationale

The following part of the chapter demonstrates that the SFRs meet all security objectives for the TOE.

The security objective for the TOE O.I&A “Identification and authentication of users” is met by the following SFR:

- The SFR FIA_ATD.1 lists the security attributes Identity, Authentication reference data and Role belonging to individual users and the SFR FMT_SMR.1 defines the security roles maintained by TSF.
- The SFR FIA_USB.1 requires the TSF to associate the user security attributes Identity and Role with subjects acting on the behalf of that user.
- The SFR FIA_UID.1 defines the TSF-mediated actions allowed on behalf of Unidentified User.
- The SFR FIA_UAU.1 defines the TSF-mediated actions allowed on behalf of Unauthenticated User.

- The SFR FIA_UAU.5 requires the TSF lists the authentication mechanisms and the rules for their application.
- The SFR FIA_API.1/CA and FIA_API.1/PACE require the TSF to authenticate external entities using Chip Authentication and PACE to communication endpoints of trusted channels.
- The SFR FIA_UAU.6 requires the TSF to request re-authentication of users under the listed conditions.
- The SFR FMT_MOF.1 requires the TSF to enable and disable of human user authentication.
- The SFR FMT_MTD.1/RAD and the SFR FMT_MTD.1/RK defines the management function of and the access limitation to authentication mechanisms and their TSF data
- 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 SFRs FIA_AFL.1/PINPUK and FIA_AFL.1/PASSWORD require the TSF to detect and react on failed authentication attempts.
- The SFR FPT_ISA.1/Cert and FPT_TIT.1/Cert require the TSF to import certificates integrity protected and with their security attributes including those for entity authentication.
- The SFR FPT_TDC.1/Cert requires the TSF to interpret the certificates correctly.

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

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

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

- The SFR FCS_CKM.1/ECC and FCS_CKM.1/RSA require (long term) key generation for the encryption and decryption security service of the TSF.
- The SFR FCS_CKM.1/AES, FCS_CKM.1/AES_RSA, FCS_CKM.5/ECDHE, and FCS_CKM.1/ECKA-EG, require key generation and FCS_CKM.5/AES, FCS_CKM.5/AES_RSA, FCS_CKM.5/ECKA-EG and FCS_CKM.5/ECC require key derivation for encryption and decryption security service of the TSF. Note the keys must be generated or agreed with the appropriate key type for encryption respectively for decryption or in case of symmetric cryptographic mechanisms for both according to FMT_MSA.1/KM.

- The FCS_COP.1/ED requires encryption and decryption as cryptographic operations for the encryption and decryption security service of the TSF.
- The FCS_COP.1/HDM requires hybrid decryption and the SFR FCS_COP.1/HEM requires hybrid encryption and decryption as cryptographic operations for the encryption and decryption security service of the TSF.
- The SFR FDP_ETC.2 require the TSF to export encrypted user data with reference to the key and data integrity checksums for decryption and FDP_ITC.2/UD require import of encrypted user data with reference to decryption key and data integrity checksums for decryption.
- The SFR FCS_CKM.4 requires the TSF to implement secure key destruction.
- The SFR FMT_MTD.1/RK requires the TSF management of root keys for key hierarchy known to the TSF if used for encryption.
- The SFR FPT_TDC.1/Cert requires the TSF to interpret consistently the security attributes of certificates (including those used for encryption and decryption).
- The SFR FPT_TDC.1/CK requires the TSF to interpret consistently the security attributes of keys (including those used for encryption and decryption).

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

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

- The SFR FPT_TDC.1/CK requires the TSF to interpret consistently the security attributes keys (including those used for data authentication).

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

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

- The SFR FTP_ITC.1 requires different types of trusted channel depending on the capability of the other endpoint. The cases are defined in Table 5. The remote entity and the TOE may use mutual authentication and key agreement by means of PACE according to FCS_CKM.1/PACE, shall provide integrity protection according to FCS_COP.1/TCM and may support confidentiality of the communication data according to FCS_COP.1/TCE. The cases 3 requires support of trusted channel with mutual authentication by FIA_API.1/CA, FIA_UAU.5, key agreement TCAP according to FCS_CKM.1/TCAP, encryption and MAC data authentication.
- The TOE authenticate themselves according to FIA_API.1/PACE in case of PACE. It authenticates themselves according to FIA_API.1/CA in case of TCAP as Proximity Integrated Circuit Card (PICC).
- The SFR FMT_MOF.1 limits the configuration of the trusted channel according to FTP_ITC.1.3 to an administrator.
- The SFR FMT_MSA.1/KM describe the requirements for management of key security attributes for these mechanisms.

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

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

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

- The SFR FIA_ATD.1 defines the security attributes of individual users including Role which is used to enforce the Key Management SFP.
- The SFR FDP_ACC.1/KM defines subjects, objects and operations of the Key Management SFP.
- The SFR FMT_SMF.1 lists the security management functions provided by the TSF.
- The SFR FMT_SMR.1 lists the security role supported by the TOE especially the administrator and – if supported - Crypto-Officer responsible for key management.
- The SFR FCS_CKM.1/AES, FCS_CKM.1/ECC, FCS_CKM.1/ECKA-EG, FCS_CKM.1/PACE, FCS_CKM.1/RSA, FCS_CKM.1/AES_RSA, FCS_CKM.1/TCAP require the TSF to implement key generation function according to the assigned standards.
- The SFR FCS_CKM.5/ECDHE require the TSF to implement key agreement function according to the assigned standards.

- The SFR FCS_CKM.5/AES and FCS_CKM.5/ECKA-EG require the TSF to implement key derivation function according to the assigned standards.
- The SFR FCS_CKM.1/AES_RSA and FCS_CKM.5/AES_RSA require the TSF to implement AES session key generation function with RSA key encryption respective RSA key decryption and AES key derivation according to the assigned standards.
- The SFR FCS_RNG.1 requires the TSF to implement a random number generator for key generation, key agreement functions and cryptographic operations.
- The SFR FCS_COP.1/ED requires the TSF to provide encryption and decryption according to AES which may be used for key management.
- The SFR FCS_COP.1/Hash requires the TSF to implement cryptographic primitive hash function for key derivation, cf. FCS_CKM.5.
- The SFR FPT_ISA.1/CK requires import and FPT_ESA.1/CK the export of cryptographic keys with security attributes and protection of confidentiality according to SFR FPT_TCT.1/CK and integrity protection according to FPT_TIT.1/CK.
- The SFR FPT_ISA.1/Cert requires import of certificates with security attributes and integrity protection according to FPT_TIT.1/Cert.
- The SFR FPT_TDC.1/Cert requires consistent interpretation of certificate's content. The SFR FPT_TDC.1/ CK requires consistent interpretation of security attributes imported with the key.
- The SFR FCS_COP.1/KW and FCS_COP.1/KU require the TSF key wrapping and unwrapping for key management.
- The SFR FCS_CKM.4 requires the TSF to implement secure key destruction.
- The SFR FMT_MSA.1/KM and FMT_MSA3/KM limit the setting of default values and specification of alternative initial values for security attributes of cryptographic keys to administrators. The SFR FMT_MSA.1/KM prevents modification or deletion of security attributes of keys.
- FMT_MSA.2 enforce secure values for security attributes.
- The SFR FMT_MTD.1/KM and FMT_MTD.1/RK restricts the management of cryptographic keys especially the import of root public keys to specifically authorized users.

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

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

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

- The UCP signature verification key may be updated according to FPT_ISA.1/Cert with integrity protection according to FPT_TIT.1/Cert.
- The UCP decryption key may be updated with confidentiality protection according to FPT_TCT.1/CK with FCS_COP.1/KU.

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

- The SFR FDP_ACC.1/CL defines subjects, objects and operations of the Clustering SFP.
- 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 an authorised identified role.
- The SFRs FPT_ESA.1/CL and FPT_ISA.1/CL require that export and import of TSF data is performed 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 between Master-CSPLight and Slave-CSPLight.
- The SFR FCS_CKM.5/CLDH requires the TSF to agree on cryptographic keys. Note, the Base-PP [PP-CSPLight] defines the SFRs FCS_COP.1/ED and FCS_COP.1/MAC for encryption and MAC of the transferred TSF data.
- The SFR FPT_TDC.1/CL requires the TSF interpret consistently the TSF exchanged between TOE samples of the cluster.

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

- The SFR FPT_STM.1 requires the TSF to provide time stamps for the real time service.
- The SFR FDP_DAU.2/TS requires the TSF to provide cryptographically protected time stamps for time stamp service supported by FCS_COP.1/CDS-ECDSA resp. FCS_COP.1/CDS-RSA for signature creation.
- The SFR FDP_ACF.1/TS defines access control on time stamp service to enforce the Cryptographic Operation SFP.
- The SFR FDP_ITC.2/TS for user data import with security attributes indicating the signature key for time stamps.
- The SFR FDP_ETC.2/TS requires the TSF to export user data with time stamps.
- The SFR FMT_SMF.1/TSA defines the management functions and FMT_SMR.1/TSA the roles for the time service and the time stamp service additional to those.
- The SFR FMT_MOF.1/TSA defines the management of the time service and the time service TSF.

The security objective for the TOE O.Audit “Audit” 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 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 export, clear and selection of events

causing audit data as management TSF data is an auditable event, cf. FAU_GEN.1, clause (11).
- The SFR FPT_TIT.1/Audit requires the TSF to protect audit records when transmitted and time when imported.
- SFR FAU_GEN.1/CL to generate the audit records of auditable events for clustering.

8.2.2 SFR Dependencies

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

The dependencies between SFRs are addressed as shown in the table below. Where a dependency is not met in the manner defined in [CC2] then a rationale is provided for why the dependency is unnecessary or else met in some other way.

Note, the column SFR components showing the concrete SFR satisfying the dependencies are typical use cases. It does not exclude that the SFR in the first column may solve dependencies of other SFR as well. E. g. the SFR FCS_CKM.1 defines requirements for ECC key generation, and a generated ECC key pair may not only 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.

No.	SFR	Dependency	Dependency satisfied by
	FAU	**Audit data generation**	
1.	FAU_GEN.1/CL	FPT_STM.1 Reliable time stamps	FPT_STM.1
2.	FAU_GEN.1	FPT_STM.1Reliable time stamps	FPT_STM.1
3.	FAU_STG.1	FAU_GEN.1Audit data generation	FAU_GEN.1
4.	FAU_STG.3	FAU_STG.1 Protected audittrailstorage	FAU_STG.1
	FCS	**Cryptographic Support**	
5.	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
6.	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
7.	FCS_CKM.1/ECC	FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4	FCS_COP.1/CDS-ECDSA, FCS_COP.1/VDS-ECDSA, FCS_CKM.4

No.	SFR	Dependency	Dependency satisfied by
		Cryptographic key destruction	
8.	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
9.	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
10.	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
11.	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
12.	FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1/ECC, FCS_CKM.1/ RSA, FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA, FCS_CKM.1/TCAP, FCS_CKM.1/PACE
13.	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
14.	FCS_CKM.5/AES_RSA	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/HDM with FCS_CKM.5/AES_RSA, FCS_CKM.4
15.	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-ECDSA, FCS_COP.1/VDS-ECDSA, FCS_CKM.4
16.	FCS_CKM.5/ECDHE	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/HEM with FCS_CKM.5/ECDHE, FCS_CKM.4
17.	FCS_CKM.5/ECKA-EG	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/HDM with FCS_CKM.5/ECKA-EG, FCS_CKM.4

No.	SFR	Dependency	Dependency satisfied by
18.	FCS_COP.1/CDS-ECDSA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/ECC, FCS_CKM.4
19.	FCS_COP.1/CDS-RSA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/RSA, FCS_CKM.4
20.	FCS_COP.1/DecUCP	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Import of UCP decryption key as TSF data with confidentiality protection FPT_TCT.1/CK and FCS_COP.1/KU, FCS_CKM.4
21.	FCS_COP.1/ED	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/AES, FCS_CKM.4
22.	FCS_COP.1/Hash	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Hash functions do not use keys
23.	FCS_COP.1/HDM	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.5/ECKA-EG, FCS_CKM.5/AES_RSA, FCS_CKM.5/ECDHE (note deterministic FCS_CKM.5 play the role of randomized FCS_CKM.1) FCS_CKM.4

No.	SFR	Dependency	Dependency satisfied by
24.	FCS_COP.1/HEM	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA, FCS_CKM.5/ECDHE, FCS_CKM.1/AES_RSA FCS_CKM.4
25.	FCS_COP.1/HMAC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_RNG.1 generates random strings as HMAC keys FCS_CKM.4
26.	FCS_COP.1/KU	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/AES FCS_CKM.4
27.	FCS_COP.1/KW	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/AES FCS_CKM.4
28.	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
29.	FCS_COP.1/TCE	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/TCAP, FCS_CKM.1/PACE, FCS_CKM.4
30.	FCS_COP.1/TCM	[FDP_ITC.1 Import of user data without	FCS_CKM.1/TCAP,

No.	SFR	Dependency	Dependency satisfied by
		security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/PACE, FCS_CKM.4
31.	FCS_COP.1/VDS-ECDSA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FPT_ISA.1/Cert (note keys are TSF data), FCS_CKM.4
32.	FCS_COP.1/VDS-RSA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FPT_ISA.1/Cert (note keys are TSF data), FCS_CKM.4
33.	FCS_COP.1/VDSUCP	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Import of signature verification key of UCP Issuer as TSF data FPT_ISA.1/Cert, FPT_TIT.1/Cert, FCS_CKM.4
34.	FCS_RNG.1	No dependencies	
35.	FCS_CKM.5/CLDH	[FCS_CKM.2Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4Cryptographic key destruction	FCS_COP.1/ED, FCS_COP.1/MAC and FCS_CKM.4
	FIA	**Identification and authentication**	
36.	FIA_AFL.1/PINPUK	FIA_UAU.1 Timing of authentication	FIA_UAU.1
37.	FIA_AFL.1/PASSWORD	FIA_UAU.1 Timing of authentication	FIA_UAU.1
38.	FIA_API.1/CA	No dependencies	
39.	FIA_API.1/PACE	No dependencies	
40.	FIA_ATD.1	No dependencies	

No.	SFR	Dependency	Dependency satisfied by
41.	FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.1
42.	FIA_UAU.5	No dependencies	
43.	FIA_UAU.6	No dependencies	
44.	FIA_UID.1	No dependencies	
45.	FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
	FDP	**User data protection**	
46.	FDP_ACC.1/KM	FDP_ACF.1 Security attribute based access control	Dependency on FDP_ACF.1 is not fulfilled. Access control to key management functions are specified by FMT_MTD.1/KM because cryptographic keys are TSF data.
47.	FDP_ACC.1/Oper	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/Oper
48.	FDP_ACC.1/UCP	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/UCP
49.	FDP_ACF.1/Oper	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/Oper, FMT_MSA.3/KM
50.	FDP_ACF.1/UCP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/UCP, FMT_MSA.3 is not included, because the security attributes of UCP are imported according to FDP_ITC.2/UCP without default values.
51.	FDP_DAU.2/Att	FIA_UID.1 Timing of identification	FIA_UID.1
52.	FDP_DAU.2/Sig	FIA_UID.1 Timing of identification	FIA_UID.1
53.	FDP_ETC.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/Oper
54.	FDP_ETC.2	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/Oper
55.	FDP_ITC.2/UCP	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/UCP trusted communication is

No.	SFR	Dependency	Dependency satisfied by
		[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	provided by FCS_COP.1/VDSUCP and FCS_COP.1/DecUCP, FPT_TDC.1/UCP
56.	FDP_ITC.2/UD	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/Oper trusted communication is provided by FCS_COP.1/HDM and FCS_COP.1/VDS-*, FPT_TDC.1/CK because import of user data is intended for cryptographic operation with key
57.	FDP_RIP.1/UCP	No dependencies	
58.	FDP_ACC.1/CL	FDP_ACF.1 Security attribute based access control	Dependency on FDP_ACF.1 is not fulfilled. Access control to key management functions are specified by FMT_MTD.1/CL because cryptographic keys are TSF data.
59.	FDP_ACF.1/TS	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/Oper, FMT_MSA.3
60.	FDP_DAU.2/TS	FIA_UID.1Timingof identification	FIA_UID.1
61.	FDP_ETC.2/TS	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/Oper
62.	FDP_ITC.2/TS	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1Inter-TSFtrusted channel or FTP_TRP.1Trusted path] FPT_TDC.1Inter-TSFbasicTSFdata consistency	FDP_ACC.1/Oper, trusted communication is provided byFCS_COP.1/HDM and FCS_COP.1/VDS-*, FTP_ITC.1, FPT_TDC.1/CK because import of user data is intended for cryptographic operation with key with appropriate security attribute “TimeStamp”

No.	SFR	Dependency	Dependency satisfied by
	FPT	**Protection of the TSF**	
63.	FPT_ESA.1/CK	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/KM, FMT_MTD.1/KM FMT_MSA.1/KM FPT_TDC.1/CK
64.	FPT_FLS.1	No dependencies	
65.	FPT_ISA.1/Cert	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/KM, FMT_MTD.1/RK, FMT_MSA.1/KM FPT_TDC.1/Cert
66.	FPT_ISA.1/CK	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/KM, FMT_MTD.1/RK, FMT_MTD.1/KM FMT_MSA.1/KM FPT_TDC.1/Cert
67.	FPT_TCT.1/CK	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]	FDP_ACC.1/KM, FMT_MTD.1/RK, FMT_MTD.1/KM
68.	FPT_TDC.1/Cert	No dependencies	
69.	FPT_TDC.1/CK	No dependencies	
70.	FPT_TDC.1/UCP	No dependencies	

No.	SFR	Dependency	Dependency satisfied by
71.	FPT_TIT.1/Cert	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]	FDP_ACC.1/KM, FMT_MTD.1/RK
72.	FPT_TIT.1/CK	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]	FDP_ACC.1/KM, FMT_MTD.1/KM
73.	FPT_TST.1	No dependencies	
74.	FPT_ESA.1/CL	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/CL FMT_MTD.1/CL, FMT_MTD.1/RAD and FMT_MTD.1/KM, FMT_MSA.1/KM applies for exported and imported keys, FPT_TDC.1/CL
75.	FPT_ISA.1/CL	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data] [FMT_MSA.1 Management of security attributes, orFMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data	FDP_ACC.1/CL FMT_MTD.1/CL, FMT_MTD.1/RAD and FMT_MTD.1/KM, FMT_MSA.1/KM applies for exported and imported keys, FPT_TDC.1/CL
76.	FPT_TCT.1/CL	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1Management of TSF data or FMT_MTD.3 Secure TSF data]	FDP_ACC.1/CL FMT_MTD.1/CL
77.	FPT_TDC.1/CL	No dependencies	
78.	FPT_TIT.1/CL	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]	FDP_ACC.1/CL, FMT_MTD.1/CL
79.	FPT_STM.1	No dependencies	

No.	SFR	Dependency	Dependency satisfied by
80.	FPT_TIT.1/Audit	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]	FDP_ACC.1/UCP FDP_ACC.1/KM and FDP_ACC.1/Oper if selected, FMT_MTD.1/Audit
	FMT	**Security management**	
81.	FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
82.	FMT_MSA.1/KM	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1/KM, FDP_ACC.1/Oper, FMT_SMF.1, FMT_SMR.1
83.	FMT_MSA.2	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FDP_ACC.1/KM, FDP_ACC.1/Oper, FMT_MSA.1/KM, FMT_SMR.1
84.	FMT_MSA.3/KM	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/KM, FMT_SMR.1
85.	FMT_MTD.1/KM	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
86.	FMT_MTD.1/RAD	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
87.	FMT_MTD.1/RK	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
88.	FMT_MTD.3	FMT_MTD.1 Management of TSF data	FMT_MTD.1/RAD
89.	FMT_SAE.1	FMT_SMR.1 Security roles, FPT_STM.1 Reliable time stamps	FMT_SMR.1, dependency on FPT_STM.1 is not fulfilled, cf. to the application note to FMT_SAE1
90.	FMT_SMF.1	No dependencies	
91.	FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.1
92.	FMT_MTD.1/CL	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1

No.	SFR	Dependency	Dependency satisfied by
93.	FMT_MOF.1/TSA	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1/TSA, FMT_SMR.1, FMT_SMF.1/TSA
94.	FMT_MTD.1/Audit	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1/TSA, FMT_SMR.1, FMT_SMF.1/TSA
95.	FMT_SMF.1/TSA	No dependencies	
96.	FMT_SMR.1/TSA	FIA_UID.1 Timing of identification	FIA_UID.1
	FTP	**Trusted channels**	
97.	FTP_ITC.1	No dependencies	

Table 10: Dependency rationale

9 TOE Summary Specification

This chapter describes how the TOE will realise the SFRs which are defined in chapter 7.2. For that purpose, the TOE Security Functionality (TSF) will be described by means of a set of security functions (SF.XXX) implemented by the TOE. This detailed description and analysis of the TSF demonstrates how the defined security functions of the TOE work together and support each other. Furthermore, it shows that no inconsistencies exist. Each SFR is implemented by at least one security function. For all SFRs an explanation is given, why and how the defined security functions of the TOE meet the respective SFRs. The given mapping of the SFRs and the security functions of the TOE at the end of this chapter should be considered as an overview and a guidance.

9.1 SF.USER_AUTH: User Authentication

The use of any of the security-relevant services of the TOE is not possible without user authentication. Only if a defined authentication status has been obtained then the TOE services can be realised; here the necessary user authentication status depends on the individual service. Command authentication can only be done by subjects (so-called *users*) which have to be registered at the TOE before.

At registration, together with the user's name (Identity), his permission (Role), authentication mechanism, the reference authentication data (RAD: public key or hash value of a password, depending on the authentication mechanism) and further attributes will be stored in the user database of the TOE. The command for change of a user's RAD has to be authenticated by the user himself. The user's permission decides which of the security-relevant services may be performed by this user (i. e. which user role the user may assume). The step immediately preceding the user authentication is the identification of a user. Therefore, the authentication procedure for the user fulfils directly the SFRs FIA_UID.1 (Timing of identification) and FIA_UAU.1 (Timing of authentication).

The TOE supports the following roles for the different users, thus implementing FMT_SMR.1 (Security roles):

- **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**: a successfully authenticated user in this role is allowed to access the TOE in order to perform management functions, including device management, user management and key management. It is taken by a human user or a subject acting on behalf of a human user after successful authentication as an Administrator.
- **Auditor**: a successfully authenticated user in this role is allowed to configure the audit functionality, review audit data and export and clear audit trails.
- **Timekeeper**: a successfully authenticated user in this role is allowed to adjust the internal time and configure the secure NTP service.
- **Key Owner**: a successfully authenticated user in this role is allowed to perform cryptographic operation with his 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 being authenticated as a human user (e. g. exporting

and importing of wrapped keys). This role may be assigned to an entity communicating through a trusted channel (which requires assured identification of its end points), as done e. g. by the SMAERS.

- **Cluster-CSP**: another TOE sample in the same 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.

At registration, for every user a dedicated authentication mechanism has to be chosen. The authentication mechanisms and the rules for their application are implemented in accordance with SFR FIA_UAU.5 with the support of SF.CRYPTO. A human user may authenticate himself to the TOE, and the TOE authenticates itself to an external entity in charge of the authenticated authorized user. After three unsuccessful user authentication attempts the TSF enforce the reset of user authentication data (PIN) via a PUK. On the other hand, in case of a user password authentication attempt fails, the next possible login time will be exponentially increased by a factor 1.4 in order both to avoid a complete blocking of the administration of the CryptoServer CSPLight and at the same time prevent brute force password guessing attacks. Thus SF.USER_AUTH supports FIA_AFL.1/PINPUK and FIA_AFL.1/PASSWORD (Authentication failure handling).

Further security services provided and related security functional requirements:

- The security attributes Identity, Authentication reference data and Role belonging to individual users are listed in accordance with SFR FIA_ATD.1 and the security roles maintained are defined in accordance with SFR FMT_SMR.1 and FMT_SMR.1/TSA.
- The user security attributes Identity and Role are associated with subjects acting on behalf of that user in accordance with SFR FIA_USB.1
- Re-authentication of users under the conditions listed in SFR FIA_UAU.6.
- Enable and disable of human user authentication in accordance with SFR FMT_MOF.1 and FMT_MOF.1/TSA. The management function of and the access limitation to authentication mechanisms and their TSF data are defined in accordance with FMT_MTD.1/RAD and FMT_MTD.1/RK.
- The secure values for password mechanisms are enforced in accordance with FMT_MTD.3.
- The validity of user authentication is limited, and the security attribute Role is reset to values defined by an administrator in accordance with FMT_MTD.1/RAD and FMT_SAE.1.
- Certificates are imported, while their integrity is protected, with their security attributes including those for entity authentication in accordance with FPT_ISA.1/Cert and FPT_TIT.1/Cert. The certificates are interpreted correctly in accordance with FPT_TDC.1/Cert.

9.2 SF.TRUSTED_CHANNEL: Trusted Channel

SF.TRUSTED_CHANNEL supports to establish a cryptographically protected trusted channel between the TOE and external entities. For exchanging sensitive data, a Secure Messaging session (trusted channel) has to be set up between the TOE and the external application component such as SMAERS. The application component (in client role) uses the security services of the TOE (in server role). TOE provides PACE protocol in ICC role for the trusted channel to protect the integrity of the messages exchanged in accordance with FTP_ITC.1. SF.TRUSTED_CHANNEL implements also terminal and chip authentication protocols for integrity and confidentiality protection of the communication with the external entities.

SF.TRUSTED_CHANNEL includes mutual authentication of the communicating entities, encryption and message authentication proof for the sent data, decryption and message authentication verification for received data, with the support of SF.ATTESTATION, SF.KEY_MAN and SF.CRYPTO, fulfilling the following SFRs:

- FIA_API.1/PACE Authentication Proof of Identity – PACE authentication to Application component
- FIA_API.1/CA Authentication Proof of Identity – Chip authentication to user
- FTP_ITC.1 Inter-TSF trusted channel
- FCS_CKM.1/PACE Cryptographic key generation – Key agreement for trusted channel PACE
- FCS_CKM.1/TCAP Cryptographic key generation – Key agreement by Terminal and Chip authentication protocols
- FCS_COP.1/TCE Cryptographic operation - Encryption for trusted channel
- FCS_COP.1/TCM Cryptographic operation - MAC for trusted channel
- FIA_UAU.5 Multiple authentication mechanisms
- FIA_UAU.6 Re-authenticating
- FMT_MOF.1 Management of security functions behaviour

9.3 SF.ATTESTATION: Authentication and Attestation of the TOE

TOE samples shall be delivered with attestation keys to attest these samples as genuine certified products. The attestation keys are generated in the TOE. Attestation of the TOE's identity to external entities is part of establishing trusted channels like PACE, terminal authentication or chip authentication. Therefore the TOE's security function SF.ATTESTATION supports SF.TRUSTED_CHANNEL while it is, on the other hand, supported by SF.CRYPTO, SF.KEY_MAN and SF.TIMESTAMP in order to provide its services.

The TOE mainly provides data authentication and non-repudiation services for user data (in the case when TOE serves SMAERS the user data is mainly the transaction log and audit log messages to be used for cash inspection). For this purpose SF.ATTESTATION generates, as well as verifies, digital signatures, including time stamps over the user data, e.g. log messages, and provides entity authentication and attestation services.

Security services provided and related SFRs fulfilled:

- Attestation service in accordance with FDP_DAU.2/Att, that can be used as a guarantee of the validity of attestation data to external entities. The attestation data provided by the SF.ATTESTATION represent the TOE sample as a genuine sample of the certified product. The cryptographic keys used for attestation are generated in accordance with FCS_CKM.1/ECC and/or computed by key agreement mechanism, in accordance with FCS_CKM.1/PACE and FCS_CKM.1/TCAP, for authentication of the TOE to external entities and attestation of the end points. As part of authentication of the TOE to external entities, TSF generates HMAC in accordance with the SFR FCS_COP.1/HMAC.
- Signature service providing also Data Authentication with Identity of Guarantor in accordance with FDP_DAU.2/Sig. Data To Be Signed (DTBS) by the TOE is imported from the application component over the PACE channel in accordance with FDP_ITC.2/UD and the signed data is exported to SMA over the same PACE channel, together with the Key identity of the used signature-creation key, in accordance with FDP_ETC.2.

- Signature service with time stamp and optional key usage counter providing Data Authentication with Identity of Guarantor in accordance with FDP_DAU.2/TS. This service is provided for signing and timestamping the audit log and transaction log messages. User data for time stamping is imported in accordance with FDP_ITC.2/TS, and the time stamped user data is exported in accordance with FDP_ETC.2/TS

9.4 SF.CRYPTO: Cryptographic Support

The TOE's security function SF.CRYPTO provides cryptographic support for the other TSFs using cryptographic mechanisms, and it enables cryptographic services like signature generation and verification for the user of the TOE. SF.CRYPTO is supported by SF.KEY_MAN and provides key derivation services for internal purposes. The services provided by SF.CRYPTO include

- encryption and decryption of user data,
- generation of random bits for internal purposes, e. g. for key generation, but also provided as a separate security service of the TOE,
- confidentiality and integrity protection of stored user data and TSF data,
- digital signature generation and verification.

SF.CRYPTO supports the following cryptographic services and operations:

- Hybrid data encryption/decryption and MAC calculation/verification as a self-contained security service of the TOE in accordance with the SFRs FCS_COP.1/HEM and FCS_COP.1/HDM
- Export of user data without security attributes in accordance with FDP_ETC.1 as part of a decryption service
- AES algorithm in CBC mode used for encryption or decryption in accordance with the SFRs FCS_COP.1/ED and FCS_COP.1/TCE
- AES algorithm used for CMAC generation and verification in accordance with the SFR FCS_COP.1/MAC and FCS_COP.1/TCM
- HMAC calculation with key size of 64 bytes in accordance with the SFR FCS_COP.1/HMAC
- ECDSA algorithm for signature generation or verification in accordance with the SFRs FCS_COP.1/CDS-ECDSA and FCS_COP.1/VDS-ECDSA
- The cryptographic algorithm *RSA* with padding mechanism EMSA-PSS with key sizes 2048 bits, 3072 bits, and 4096 bits modulus lengths used for RSA signature generation and verification in accordance with the SFRs FCS_COP.1/CDS-RSA and FCS_COP.1/VDS-RSA
- Hash algorithms SHA-256, SHA-384, SHA-512 in accordance with the SFR FCS_COP.1/Hash
- Key wrapping and unwrapping in accordance with the SFRs FCS_COP.1/KW and FCS_COP.1/KU
- Diffie-Hellmann key agreement in accordance with the SFR FCS_CKM.5/ECDHE
- Key Derivation, for internal purposes, in accordance with the SFRs FCS_CKM.5/ECKA-EG, FCS_CKM.5/AES_RSA, FCS_CKM.5/CLDH, FCS_CKM.5/AES and FCS_CKM.5/ECC,
- Random number generation by a hybrid RNG in accordance with the SFR FCS_RNG.1.

9.5 SF.ADMIN: Administration

The TOE provides functionality to administrate itself in a secure and controlled way, via its security function SF.ADMIN which provides access control on cryptographic TSF and cryptographic keys using also the internal cryptographic services provided by SF.CRYPTO. Security-relevant administration of the TOE cannot be done without user authentication. Only if a defined authentication status has been obtained then administration tasks can be executed. The administration security function SF.ADMIN is therefore also related to SF.USER_AUTH.

SF.ADMIN provides the following administrative services, in accordance with FMT_SMF.1 and FMT_SMR.1:

- Modifications of key attributes by an authorised user in Administrator role or Key Owner role, in accordance with FDP_ACF.1/Oper and FDP_ACF.1/TS fulfilling also the rules for access control to subjects, objects and operations in accordance with FDP_ACC.1/Oper,
- Management of the security functions behaviour related to time service and the time stamp service in accordance with FMT_SMF.1/TSA, FMT_SMR.1/TSA and FMT_MOF.1/TSA.

A subject in Administrator role is allowed to execute the administrative services including the user administration for which typical functions are available. Basically, these functions deal with administration of the user database (creation, deletion, changing). The commands for creation or deletion of a user have to be authenticated by a user in Administrator role. The command for changing the user's authentication token (password or public key) has to be authenticated by the respective user himself.

9.6 SF.KEY_MAN: Key Management

SF.KEY_MAN covers the security functionality related to 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. Key management is supported by SF.CRYPTO, and only if a defined authentication status has been obtained then key management tasks can be executed in accordance with the access control rules described in FDP_ACC.1/KM. The key management security function SF.KEY_MAN is therefore supported by SF.USER_AUTH and SF.CRYPTO.

Key management services provided and related group of SFRs fulfilled are the following:

- Key generation service:
  - FCS_CKM.1/RSA Cryptographic key generation – RSA key pair
  - FCS_CKM.1/ECC Cryptographic key generation – Elliptic curve key pair ECC
  - FCS_CKM.1/PACE Cryptographic key generation – Key agreement for trusted channel PACE
  - FCS_CKM.1/TCAP Cryptographic key generation – Key agreement by Terminal and Chip authentication protocols
  - FCS_CKM.1/ECKA-EG Cryptographic key generation – ECKA-EG key generation with ECC encryption
  - FCS_CKM.1/AES_RSA Cryptographic key generation – Key generation and RSA encryption
  - FCS_CKM.1/AES Cryptographic key generation – AES key
- Deletion of cryptographic keys:
  - FCS_CKM.4 Cryptographic key destruction
- Management of the security attributes (set, modify, delete) of cryptographic keys:
  - FMT_MSA.2 Secure security attributes

    - FMT_MSA.1/KM Management of security attributes – Key security attributes
    - FMT_MSA.3/KM Static attribute initialization – Key management
    - FMT_SMF.1 Specification of Management Functions
- Import and export of cryptographic keys and certificates:
    - FPT_TCT.1/CK TSF data confidentiality transfer protection – Cryptographic keys
    - FPT_TIT.1/CK TSF data integrity transfer protection – Cryptographic keys
    - FPT_ISA.1/CK Import of TSF data with security attributes – Cryptographic keys
    - FPT_TDC.1/CK Inter-TSF basic TSF data consistency – Key import
    - FPT_ISA.1/Cert Import of TSF data with security attributes – Certificates
    - FPT_ISA.1/CL Import of TSF data with security attributes – Cluster
    - FMT_MTD.1/KM Management of TSF data – Key management
    - FMT_MTD.1/RK Management of TSF data – Root key
    - FPT_TIT.1/Cert TSF data integrity transfer protection – Certificates
    - FPT_TDC.1/Cert Inter-TSF basic TSF data consistency – Certificate
    - FPT_ESA.1/CK Export of TSF data with security attributes – Cryptographic keys
    - FPT_ESA.1/CL Export of TSF data with security attributes – Cluster
    - FPT_TDC.1/CL Inter-TSF basic TSF data consistency – Clustering

9.7 SF.SWUPDATE: Software Update

The TOE security function SF.SWUPDATE supports downloading, integrity and authenticity verification and decryption of Update Code Packages (UCP) for the CryptoServer CSPLight. This service has to be authenticated by a user with the Administrator role, thereby fulfilling also the access control related SFRs FDP_ACC.1/UCP and FDP_ACF.1/UCP, therefore supported by SF.USER_AUTH.

SF.SWUPDATE downloads a UCP in accordance with the SFR FDP_ITC.2/UCP together with its security attributes *Issuer* and *Version Number,* which are identified successfully by the TOE before accepting the UCP as a valid update code package, in accordance with the SFR FPT_TDC.1/UCP. The *Version Number* must be higher than the current TOE software and the UCP must contain the *Issuer*'s electronic signature, calculated over the executable code, and only after its successful verification of authenticity, the UCP is stored to proceed with the software update procedures. The signature has to be calculated with a dedicated UCP Signature Key owned by the manufacturer. The public part of this UCP Signature Key is stored inside the TOE and will be used for signature verification, with the support of SF.CRYPTO, in accordance with FCS_COP.1/VDSUCP.

If the signature cannot be verified, the UCP is discarded without being installed on the TOE, in accordance with FDP_RIP.1/UCP, and the TSF will return an error code instead. Since the manufacturer uses this specific UCP Signature Key only for TOE software of CryptoServer CSPLight, it is assured that only software that is designed and released for CryptoServer CSPLight can be loaded onto the TOE. It is not possible to exchange the UCP Signature Key inside the TOE.

After successful UCP Signature verification, and after the UCP is successfully decrypted according to AES block cipher in CBC mode with PKCS#5 padding and cryptographic key

sizes 256 bits in accordance with FCS_COP.1/DecUCP, the UCP is accepted for TOE software update.

If the set of loaded software modules are incomplete or in any way not compliant, as detected during e.g., the first self-tests of the updated TOE, with the software that is released for this project, the TOE will return an error code and remove (de-install) the latest UCP installation and recovers back to the previously functioning software version.

9.8 SF.CLUSTER: Clustering of the TOE

The TOE provides security functionality, SF.CLUSTER, to establish a cluster of TOE samples for scalability of performance and availability of security services. The Administrator role is authorized to set up a CryptoServer CSPLight-cluster, in accordance with FDP_ACC.1/CL, which is composed of two TOE samples. For the initialization of a cluster the Administrator selects one TOE sample as Master-CryptoServer CSPLight and the other TOE sample as Slave-CryptoServer CSPLight. The Master-CryptoServer CSPLight provides cryptographic services to the SMAs through PACE secure channel. When the Master CryptoServer CSPLight becomes unavailable then the Slave CryptoServer CSPLight becomes a master and provides the cryptographic services to the SMAs. SF.CLUSTER is supported by SF.USER_AUTH and SF.KEY_MAN in order to provide its security services.

The TOE samples of the cluster agree on encryption and MAC keys using cluster secrets, in accordance with FCS_CKM.5/CLDH (using PACE as implementation), for encrypted, in accordance with FPT_TCT.1/CL, and integrity protected, in accordance with FPT_TIT.1/CL, exchange of Authentication Data Records and Cryptographic keys in order to ensure synchronization between master and slave in a secure manner. The TSF data exchanged between the master and the slave is interpreted in accordance with FPT_TDC.1/CL. The Master-CryptoServer CSPLight transfers TSF data Authentication Data Records of known users and cryptographic keys to Slave-CryptoServer CSPLight under control of the Administrator or the Application Component using the cluster in accordance with the SFRs FPT_ESA.1/CL, FPT_ISA.1/CL and FMT_MTD.1/CL. Audit records related to clustering are generated in accordance with FAU_GEN.1/CL.

9.9 SF.TIMESTAMP: Time Stamp Service

The TOE provides a time service as well as a time stamp service. The time service allows the user to query the internal time of the TSF. All time-related services (system time setting, system time querying, time stamping in context of data attestation, adding reliable timestamps to audit log entries) takes place using access to the TOE's internal system clock (real time clock) which can be set manually or with signed Network Time Protocol (NTP) in accordance with the SFR FPT_STM.1.

By adding a time stamp and a signature over the given data, the time stamp service provides evidence that user data were presented to the TSF and exported audit log messages were generated at a certain point in time and in a verifiable sequence. The validity of these user data and audit records can be verified later on with the respective verification service. SF.TIMESTAMP is supported by SF.CRYPTO and only if a Timekeeper user authentication has been obtained then time management tasks can be executed. SF.TIMESTAMP is therefore closely related to SF.USER_AUTH and SF.CRYPTO.

Security functional requirements concerned:

- FMT_SAE.1 Time-limited authorisation,
- FPT_STM.1 Reliable time stamps,
- FDP_ETC.2/TS Export of user data with security attributes - User data with time stamp,
- FDP_ACF.1/TS Security attribute based access control – Cryptographic operations,
- FMT_SMF.1/TSA Specification of Management Functions,
- FMT_SMR.1/TSA Security roles,
- FMT_MOF.1/TSA Management of security functions behaviour,
- FDP_DAU.2/TS Data Authentication with Identity of Guarantor – Signature with time stamp and optional key usage counter.

9.10 SF.AUDIT: Audit

The TOE provides secure auditing functionality, SF.AUDIT, which generates audit records on selected user activities and security events of the TOE in accordance with FAU_GEN.1. The audit records are generated in the TOE and exported to the SMA which then exports them as the audit logs to an interface device to be stored and finally made available for inspection by the authorities as complementary data to help interpret user data e.g.,Transaction Logs. Audit records are exported by the TOE in signed and time stamped form and hence SF.AUDIT is supported by SF.TIMESTAMP. SF.AUDIT requires Administrator or Auditor user authentication before providing its services, therefore, SF.AUDIT is supported by SF.USER_AUTH.

SF.AUDIT provides manual export, clearing after the manual export of the audit records in accordance with FMT_MTD.1/Audit (Management of TSF data).

SF.AUDIT monitors the events including:

- Self-test error,
- Stored data integrity failure,
- Failure of user authentication attempts,
- Results of services of SF.ADMIN, SF.KEY_MAN, SF.SWUPDATE, SF.TIMESTAMP and SF.CLUSTER and provides the corresponding audit records in accordance with the SFRs FAU_GEN.1 (Audit data generation), FAU_GEN.1/CL (Audit data generation iterated for clustering).

Setting of the number of audit records causing automatic export and clearing of exported audit records as well as the storage capacity is handled in accordance with the SFRs FAU_STG.1 (Protected audit trail storage), FAU_STG.3 (Action in Case of Possible Audit Data Loss) and FMT_MOF.1/TSA.

Coverage of SFRs by Security Functions

The following table shows that all TOE Security Functional Requirements (SFRs) are realised by the TSF (TOE Security Functionality) described in terms of security functions (SF.XXX).

SFR	SF.USER_AUTH	SF.TRUSTED_CHANNEL	SF.ATTESTATION	SF.CRYPTO	SF.ADMIN	SF.KEY_MAN	SF.SWUPDATE	SF.CLUSTER	SF.TIMESTAMP	SF.AUDIT
FDP_ACC.1/KM Subset access control – Cryptographic operation						X				
FMT_MSA.1/KM Management of security attributes – Key security attributes						X				
FMT_MSA.3/KM Static attribute initialization – Key management						X				
FMT_MTD.1/KM Management of TSF data – Key management						X				
FCS_COP.1/Hash Cryptographic operation – Hash				X						
FMT_MTD.1/RK Management of TSF data – Root key	X					X				
FPT_TIT.1/Cert TSF data integrity transfer protection – Certificates	X					X				
FPT_ISA.1/Cert Import of TSF data with security attributes - Certificates	X					X				
FPT_TDC.1/Cert Inter-TSF basic TSF data consistency - Certificate	X					X				
FCS_RNG.1 Random number generation				X						
FCS_CKM.1/AES Cryptographic key generation – AES key						X				
FCS_CKM.5/AES Cryptographic key derivation – AES key derivation				X						
FCS_CKM.1/ECC Cryptographic key generation – Elliptic curve key pair ECC			X			X				
FCS_CKM.5/ECC Cryptographic key derivation – ECC key pair derivation				X						
FCS_CKM.1/RSA Cryptographic key generation – RSA key pair						X				
FCS_CKM.5/ECDHE Cryptographic key derivation – Elliptic Curve Diffie-Hellman ephemeral key agreement				X						

SFR	SF.USER_AUTH	SF.TRUSTED_CHANNEL	SF.ATTESTATION	SF.CRYPTO	SF.ADMIN	SF.KEY_MAN	SF.SWUPDATE	SF.CLUSTER	SF.TIMESTAMP	SF.AUDIT
FCS_CKM.1/ECKA-EG Cryptographic key generation – ECKA-EG key generation with ECC encryption						X				
FCS_CKM.5/ECKA-EG Cryptographic key derivation – ECKA-EG key derivation				X						
FCS_CKM.1/AES_RSA Cryptographic key generation – Key generation and RSA encryption						X				
FCS_CKM.5/AES_RSA Cryptographic key derivation – RSA key derivation and decryption				X						
FCS_CKM.4 Cryptographic key destruction						X				
FCS_COP.1/KW Cryptographic operation – Key wrap				X						
FCS_COP.1/KU Cryptographic operation – Key unwrap				X						
FPT_TCT.1/CK TSF data confidentiality transfer protection – Cryptographic keys						X				
FPT_TIT.1/CK TSF data integrity transfer protection – Cryptographic keys						X				
FPT_ISA.1/CK Import of TSF data with security attributes – Cryptographic keys						X				
FPT_TDC.1/CK Inter-TSF basic TSF data consistency – Key import						X				
FPT_ESA.1/CK Export of TSF data with security attributes – Cryptographic keys						X				
FCS_COP.1/ED Cryptographic operation – Data encryption and decryption				X						
FCS_COP.1/HEM Cryptographic operation – Hybrid data encryption and MAC calculation				X						
FCS_COP.1/HDM Cryptographic operation – Hybrid data decryption and MAC verification				X						

SFR	SF.USER_AUTH	SF.TRUSTED_CHANNEL	SF.ATTESTATION	SF.CRYPTO	SF.ADMIN	SF.KEY_MAN	SF.SWUPDATE	SF.CLUSTER	SF.TIMESTAMP	SF.AUDIT
FCS_COP.1/MAC Cryptographic operation – MAC using AES				X						
FCS_COP.1/HMAC Cryptographic operation – HMAC	X		X	X						
FCS_COP.1/CDS-ECDSA Cryptographic operation – Creation of digital signatures ECDSA				X						
FCS_COP.1/VDS-ECDSA Cryptographic operation – Verification of digital signatures ECDSA				X						
FCS_COP.1/CDS-RSA Cryptographic operation – Creation of digital signatures RSA				X						
FCS_COP.1/VDS-RSA Cryptographic operation – Verification of digital signatures RSA				X						
FDP_DAU.2/Sig Data Authentication with Identity of Guarantor – Signature			X							
FIA_API.1/PACE Authentication Proof of Identity – PACE authentication to Application component		X								
FIA_API.1/CA Authentication Proof of Identity – Chip authentication to user		X								
FDP_DAU.2/Att Data Authentication with Identity of Guarantor - Attestation			X							
FTP_ITC.1 Inter-TSF trusted channel		X								
FCS_CKM.1/PACE Cryptographic key generation – Key agreement for trusted channel PACE		X	X			X				
FCS_CKM.1/TCAP Cryptographic key generation – Key agreement by Terminal and Chip authentication protocols		X	X			X				
FCS_COP.1/TCE Cryptographic operation - Encryption for trusted channel		X		X						

SFR	SF.USER_AUTH	SF.TRUSTED_CHANNEL	SF.ATTESTATION	SF.CRYPTO	SF.ADMIN	SF.KEY_MAN	SF.SWUPDATE	SF.CLUSTER	SF.TIMESTAMP	SF.AUDIT
FCS_COP.1/TCM Cryptographic operation - MAC for trusted channel		X		X						
FIA_ATD.1 User attribute definition – Identity based authentication	X									
FMT_MTD.1/RAD Management of TSF data – Authentication reference data and Authentication Data Records	X									
FMT_MTD.3 Secure TSF data	X									
FIA_AFL.1/PINPUK Authentication failure handling	X									
FIA_AFL.1/PASSWORD Authentication failure handling	X									
FIA_USB.1 User-subject binding	X									
FMT_SAE.1 Time-limited authorisation	X								X	
FIA_UID.1 Timing of identification	X									
FIA_UAU.1 Timing of authentication	X									
FIA_UAU.5 Multiple authentication mechanisms	X	X								
FIA_UAU.6 Re-authenticating	X	X								
FDP_ITC.2/UD Import of user data with security attributes – User data			X							
FDP_ETC.2 Export of user data with security attributes			X							
FDP_ETC.1 Export of user data without security attributes				X						
FDP_ACC.1/Oper Subset access control – Cryptographic operation					X					
FDP_ACF.1/Oper Security attribute based access control – Cryptographic operations					X					
FMT_SMF.1 Specification of Management Functions					X	X				

SFR	SF.USER_AUTH	SF.TRUSTED_CHANNEL	SF.ATTESTATION	SF.CRYPTO	SF.ADMIN	SF.KEY_MAN	SF.SWUPDATE	SF.CLUSTER	SF.TIMESTAMP	SF.AUDIT
FMT_SMR.1 Security roles	X				X					
FMT_MSA.2 Secure security attributes						X				
FMT_MOF.1 Management of security functions behaviour	X	X								
FPT_FLS.1 Failure with preservation of secure state										X
FPT_TST.1 TSF testing										X
FDP_ITC.2/UCP Import of user data with security attributes – Update Code Package							X			
FPT_TDC.1/UCP Inter-TSF basic TSF data consistency							X			
FCS_COP.1/VDSUCP Cryptographic operation – Verification of digital signature of the Issuer							X			
FCS_COP.1/DecUCP Cryptographic operation – Decryption of authentic Update Code Package							X			
FDP_ACC.1/UCP Subset access control – Update code Package							X			
FDP_ACF.1/UCP Security attribute based access control – Import Update Code Package							X			
FDP_RIP.1/UCP Subset residual information protection							X			
FDP_ACC.1/CL Subset access control – Clustering								X		
FMT_MTD.1/CL Management of TSF data – Authentication Data Records and cryptographic keys								X		
FCS_CKM.5/CLDH Cryptographic key derivation – Cluster keys				X				X		
FPT_TCT.1/CL TSF data confidentiality transfer protection – Cluster								X		

SFR	SF.USER_AUTH	SF.TRUSTED_CHANNEL	SF.ATTESTATION	SF.CRYPTO	SF.ADMIN	SF.KEY_MAN	SF.SWUPDATE	SF.CLUSTER	SF.TIMESTAMP	SF.AUDIT
FPT_TIT.1/CL TSF data integrity transfer protection – Cluster								X		
FPT_ISA.1/CL Import of TSF data with security attributes – Cluster						X		X		
FPT_ESA.1/CL Export of TSF data with security attributes – Cluster						X		X		
FPT_TDC.1/CL Inter-TSF basic TSF data consistency – Clustering						X		X		
FAU_GEN.1 Audit data generation										X
FMT_MTD.1/Audit Management of TSF data										X
FAU_STG.1 Protected audit trail storage										X
FAU_STG.3 Action in Case of Possible Audit Data Loss										X
FPT_STM.1 Reliable time stamps									X	
FPT_TIT.1/Audit TSF data integrity transfer protection – Audit functionality										X
FAU_GEN.1/CL Audit data generation								X		X
FDP_DAU.2/TS Data Authentication with Identity of Guarantor – Signature with time stamp and optional key usage counter			X						X	
FDP_ITC.2/TS Import of user data with security attributes – User data for time stamping			X							
FDP_ETC.2/TS Export of user data with security attributes - User data with time stamp			X						X	
FDP_ACF.1/TS Security attribute based access control – Cryptographic operations					X				X	
FMT_SMF.1/TSA Specification of Management Functions					X				X	
FMT_SMR.1/TSA Security roles	X				X				X	

SFR	SF.USER_AUTH	SF.TRUSTED_CHANNEL	SF.ATTESTATION	SF.CRYPTO	SF.ADMIN	SF.KEY_MAN	SF.SWUPDATE	SF.CLUSTER	SF.TIMESTAMP	SF.AUDIT
FMT_MOF.1/TSA Management of security functions behavior	X				X				X	X

Table 11: Mapping SFRs to Security Functions

10 Annex

This Annex contains the following sections:

Glossary and Acronyms

References

10.1 Glossary and Acronyms

The following glossary includes all used terms of this Security Target regarding to the Common Criteria and IT technology terms in alphabetical order.

Term	**Description**
authentication reference data	data used by the TOE to verify the authentication attempt of a user
authentication verification data	data used by the user to authenticate themselves to the TOE
authenticity	the property that ensures that the identity of a subject or resource is the one claimed (cf. ISO/IEC 7498-2:1989)
cluster	a system of TOE samples initialized by an administrator and communication through trusted channels in order to manage known users and to share the cryptographic keys
cryptographic key	a variable parameter which is used in a cryptographic algorithm or protocol
data integrity	the property that data has not been altered or destroyed in an unauthorized manner (cf. ISO/IEC 7498-2:1989)
firmware	executable code that is stored in hardware and cannot be dynamically written or modified during execution while operating on a non-modifiable or limited execution platform, cf. ISO/IEC 19790
hardware	physical equipment or comprises the physical components used to process programs and data or to protect physically the processing components, cf. ISO/IEC 19790
Issuer of update code package	Trusted authority issuing an update code package (UCP) and holding the signature private key for signing the UCP and corresponding to the public key implemented in the TOE for verification of the UCP. The issuer is typically the TOE manufacturer. The issuer of an UCP is identified by the security attribute Issuer of the UCP.
Platform guidance	All documentation provided by the hardware manufacturer, or software platform manufacturer, that provides information on how to securely implement functionality.

Term	Description
private key	confidential key used for asymmetric cryptographic mechanisms like decryption of cipher text, signature-creation or authentication proof, where it is difficult for the adversary to derive the confidential private key from the known public key
public key	public known used for asymmetric cryptographic mechanisms like encryption of cipher text, signature-verification or authentication verification, where it is difficult for the adversary to derive the confidential private key from the known public key
secret key	key of symmetric cryptographic mechanisms, using two identical keys with the same secret value or two different values, where one may be easy calculated from the other one, for complementary operations like encryption / decryption, signature-creation / signature-verification, or authentication proof / authentication verification.
secure channel	a trusted channel which is physically protected and logical separated communication channel between the TOE and the user, or is protected by means of cryptographic mechanisms
software	executable code that is stored on erasable media which can be dynamically written and modified during execution while operating on a modifiable execution platform, cf. ISO/IEC 19790
trusted channel	a means by which a TSF and another trusted IT product can communicate with necessary confidence (cf. CC part 1[CC1], paragraph 97)
update code package	code if implemented changing the TOE implementation at the end of the TOE life time

Table 12: Glossary

The following table includes all used acronyms of this Security Target regarding to the Common Criteria and IT technology terms in alphabetical order.

Acronym	Term
A.xxx	Assumption
CC	Common Criteria
ECC	Elliptic curve cryptography
HMAC	Keyed-Hash Message Authentication Code

Acronym	Term
KDF	Key derivation function
MAC	Message Authentication Code
n. a.	Not applicable
O.xxx	Security objective for the TOE
OE.xxx	Security objective for the TOE environment
OSP.xxx	Organisational security policy
PACE	Password Authenticated Connection Establishment
PKI	Public Key Infrastructure
PP	Protection Profile
SAR	Security assurance requirements
SFR	Security functional requirement
T.xxx	Threat
TOE	Target of Evaluation
TSF	TOE security functionality
UCP	update code package
CSP	Cryptographic Service Provider
CSPLight	Cryptographic Service Provider Light
ERS	Electronic Record-keeping System
CTSS	Certified Technical Security System
SMA	Security Module Application
SMAERS	Security Module Application for Electronic Record-keeping Systems

Table 13: Acronyms

10.2 References

[AIS 20/31]	Application Notes and Interpretation of the Scheme (AIS): AIS 20/AIS 31: A proposal for: Functionality classes for random number generators, Version 2.0 / Wolfgang Killmann (T-Systems GEI GmbH, Bonn), Werner Schindler (Bundesamt für Sicherheit in der Informationstechnik/BSI, Bonn), 18. September 2011
[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, CCMB-2017-04-004, Version 3.1, Revision 5, April 2017
[PP-CSPLight]	BSI-CC-PP-0111-2019: Common Criteria Protection Profile Cryptographic Service Provider Light, v1.0 / Bundesamt für Sicherheit in der Informationstechnik (BSI)
[PPC-CSPLight-TS-Au-Cl]	BSI-CC-PP-0113-2020: Common Criteria Protection Profile Configuration Cryptographic Service Provider Light - Time Stamp Service and Audit – Clustering (PPC-CSPLight-TS-Au-Cl), v1.0 / Bundesamt für Sicherheit in der Informationstechnik (BSI)
[PPM-Cl]	BSI-CC-PP-0113-2020, Protection Profile-Module CSPLight Clustering (PPM-Cl) (chapter 3 to chapter 9 of [PPC-CSPLight-TS-Au-Cl]) / Bundesamt für Sicherheit in der Informationstechnik (BSI)
[PPM-TS-Au]	BSI-CC-PP-0112-2020, Protection Profile-Module CSPLight Time Stamp Service and Audit (PPM-TS-Au) (from chapter 3 onwards), v1.0 / Bundesamt für Sicherheit in der Informationstechnik (BSI)
[PP-SMAERS]	Common Criteria Protection Profile Security Module Application for Electronic Record-keeping Systems (SMAERS), v1.0 / Bundesamt für Sicherheit in der Informationstechnik (BSI)
[FCG]	Fiscal Code of Germany in the version promulgated on 1 October 2002 (Federal Law Gazette [Bundesgesetzblatt] I p. 3866; 2003 I p. 61), last amended by Article 6 of the Law of 18. July 2017 (Federal Law Gazette I p. 2745)
[KSV]	Verordnung zur Bestimmung der technischen Anforderungen an elektronische Aufzeichnungs- und Sicherungssysteme im Geschäftsverkehr (Kassensicherungsverordnung – KassenSichV), Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 66, ausgegeben zu Bonn am 6. October 2017
[ANSI-X9.63]	ANSI-X9.63, Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2011

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

[FIPS 140-2] FIPS PUB 140-2, Security Requirements for Cryptographic Modules / National Institute of Standards and Technology (NIST), USA, May 2001

[FIPS PUB 180-4] FIPS PUB 180-4, Secure Hash Standard (SHS) / National Institute of Standards and Technology (NIST), USA, March 2012

[FIPS PUB 186-4] FIPS PUB 186-4, Digital Signature Standard / National Institute of Standards and Technology (NIST), USA, July 2013

[FIPS PUB 197] FIPS PUB 197, Advances Encryption Standard (AES) / National Institute of Standards and Technology (N11IST), USA, 26th November 2001

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

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

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

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

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

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

[NIST-SP800-38A] NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques / National Institute of Standards and Technology (NIST), USA, December 2001

[NIST-SP800-38B] NIST Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication / National Institute of Standards and Technology (NIST), USA, May 2005

[NIST-SP800-38C] NIST Special Publication 800-38C: Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality / National Institute of Standards and Technology (NIST), USA, May 2004

[NIST-SP800-38D] NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and

	GMAC / National Institute of Standards and Technology (NIST), USA, November 2007
[NIST-SP800-38F]	NIST Special Publication 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping / National Institute of Standards and Technology (NIST), USA, 2012
[NIST-SP800-56C]	NIST Special Publication 800-56C: Recommendation for Key Derivation through Extraction-then-Expansion / National Institute of Standards and Technology (NIST), USA, November 2011
[PKCS#1]	PKCS #1 v2.2: RSA Cryptographic Standard, https://www.emc.com/emc-plus/rsa-labs/pkcs/files/h11300-wp-pkcs-1v2-2-rsa-cryptography-standard.pdf, 27.10.2012
[RFC2104]	HMAC: Keyed-Hashing for Message Authentication, Internet Engineering Task Force (IETF), February 1997
[RFC5639]	RFC5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, http://www.ietf.org/rfc/rfc5639.txt, 2010
[RFC5903]	RFC5903, Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2
[RFC6954]	RFC6954, Using the Elliptic Curve Cryptography (ECC) Brainpool Curves for the Internet Key Exchange Protocol Version 2 (IKEv2)
[SOGIS IT-TDs]	SOG-IS, Recognition Agreement Management Committee Policies and Procedures, SOGIS IT-Technical Domains, February 2011
[TPMLib,Part 1]	Trusted Platform Module Library, Part 1: Architecture, Family “2.0”, Level 00, Revision 01.38, September 29, 2016
[TR-03110]	BSI, Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2 - Protocols for electronic IDentification, Authentication and trust Services (eIDAS), Version 2.21, 2016 / Bundesamt für Sicherheit in der Informationstechnik (BSI)
[TR-03111]	BSI, Elliptic Curve Cryptography, BSI Technical Guideline TR-03111, Version 2.1, 1.6.2018 / Bundesamt für Sicherheit in der Informationstechnik (BSI)
[TR-03151]	BSI, Technical GuidelineTR-03151Secure Element API (SEAPI), v1.0, 5. Juni 2018 / Bundesamt für Sicherheit in der Informationstechnik (BSI)
[TR-03153]	BSI, TR-03153 - Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme“, v1.01, 20. Dezember 2018 / Bundesamt für Sicherheit in der Informationstechnik (BSI)