D-TRUST Ein Unternehmen der Bundesdruckerei

D-TRUST Web-Dienst TSE-CSP Security Target

Version 1.4.5 2024-01-26

IMPRESSUM

D-TRUST GmbH
Kommandantenstraße 15
10969 Berlin
Tel.: +49 (0) 30 25 98 - 0

Table of Contents

1. Introduction

The Fiscal Code of Germany [FCG] section146a requires that for an electronic record-keeping system (ERS), the accounts and the records must be protected by a certified technical security system. The Federal Office for Information Security defines requirements for the components of the certified technical security system, i.e. for the security module using Common Criteria Protection Profiles, and for the storage medium and the unified digital interface by Federal Office's technical guidelines (cf. [KSV] section 5). The security module consists of a controller, executing the security module application (referenced as Client Remote Entity) and the cryptographic service provider (CSP).

This Security Target defines security requirements that apply to the cryptographic service provider (CSP). The requirements are defined in the Protection Profile "Cryptographic Service Provider Light" [PP-CSP-LIGHT]. A representative implementation for the Client Remote Entity of an ERS is the "Security Module Application for Electronic Record-keeping Systems" [PP-SMAERS]. Therefor the implementation of the "Cryptographic Service Provider Light" takes requirements of the [PP-SMAERS] and [TR-03151] into account.

1.1 ST Reference

- ST Reference: D-TRUST Web-Dienst TSE-CSP Security Target
- Sponsor: D-TRUST GmbH, Kommandantenstr. 15, 10969 Berlin
- Developer: Bundesdruckerei GmbH, Kommandantenstr. 18, 10969 Berlin
- ST Version: 1.4.5
- ST Date: 2024-01-26
- CC Version: 3.1 Revision 5
- Assurance Level: EAL 2 augmented with ALC_CMS.3, ALC_LCD.1
- Certification ID: [BSI-DSZ-CC-1139-V4]

1.2 TOE Reference

- TOE Name: D-TRUST Web-Dienst TSE-CSP
- TOE Version: 1.4.1
- TOE Filename: csplight-1.4.1-1856182-jar-with-dependencies.jar
- TOE SHA-256 Hash value: f1f27366c592f4279073d5e26135379709323668bf611ef90fd80d41d2f28645

2. TOE Overview

2.1 TOE Type

The TOE is a software application that provides, as server application, the functionality of the CSP according to [PP-CSP-LIGHT]. The TOE does not provide any kind of interface for direct user interaction. Instead, the TOE provides its services in form of RESTful service interfaces based on the HTTP/HTTPS protocol to be consumed by other applications.

As shown in Figure 1 the "Client Remote Interface" is based on HTTP only, since it carries the PACE-trusted channel data (RESTful with TC-Data over HTTP) and the "Administration Interface" is HTTPS based (RESTful over HTTPS).

The TOE has been developed in Java and requires a Java Virtual Machine (JVM), a particular operating system and a dedicated hardware system to run on.

2.2 Integration of the TOE in the Environment

The TOE is implemented and first deployed at the D-Trust TSS application, but is not restricted to. In the TSS deployment the TOE is the "D-TRUST Web-Dienst TSE-CSP" which is part of the D-Trust TSS. D-Trust develops a webservice as a remote variant of a "Technical Security System", (TSS, "Technische Sicherheitseinrichtung") in client/server architecture.

The following picture shows the TOE as part of the Remote CSP Service:

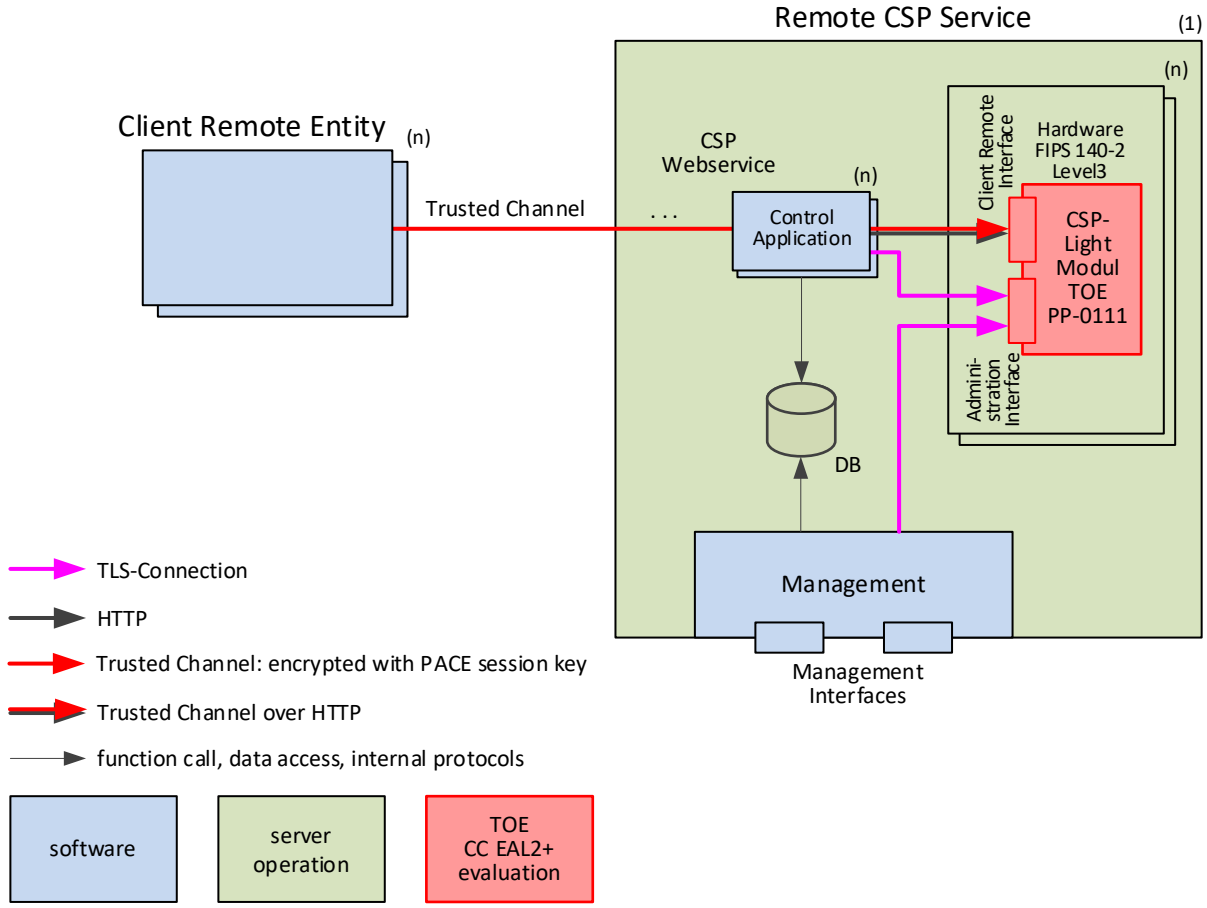


Figure 1. Architecture of the webservice

The webservice as shown in Figure 1 comprises several specific applications that work together to form a TSS and to address the challenges of the remote operation of a TSS. These applications are:

The Client Remote Entity (CRE) is operated in the local environment of the client user. In case of the TSS setup it exposes the functionality of the Secure-Element API (SE-API) and is intended to be installed on an ERS or in its operational environment under the physical control of the taxpayer (see figure 2 c [PP-SMAERS]) and represents the primary interface to the end user (being the ERS).

The **Remote CSP Service** is operated by D-Trust in their computing center (Trustcenter). It is used by multiple CREs and offers cryptographic services to them. It specifically comprises the following components:

1. The **CSP Webservice** is responsible for the authentication of the incoming request of a CRE and for processing the request. It comprises the Access Control module that is responsible for the verification of the access token that is transmitted along with the HTTP request and the Control Application that checks for existence and status of a CRE Account based on the transmitted key reference.
2. The TOE (**CSP Light Module)** as described in this Security Target stores the user data (i.e. userID and PACE password) (CRE Account) and provides the functionality to manage the CRE Account. It offers cryptographic services (e.g. creating signatures for the ERS) to CREs with an existing CRE Account. This module is the communication endpoint of the trusted channel for the communication with the CRE.
3. The **Management** module allows the Trustcenter to perform the required administrative operations (e.g. commissioning of CSP Light Modules, generation and destruction of signing keys located on the CSP Light Modules, issuing and revocation of certificates of signing keys) and to manage the life cycle of the CRE Account from the perspective of a CRE user (start operation, removal of CRE account, etc.).

2.3 Usage and Major Security Features

The TOE provides the following major security features:

1. warranty of a trusted channel communication in the ICC role with the CRE based on the PACE protocol,
2. creation and secure destruction of the signature key of a CRE for the CRE user (e.g. a taxpayer in case of a TSS),
3. secure management and assignment of the signature key of a CRE and the associated signature usage counter,
4. receipt of the data to be signed from the CRE (e.g. transaction data of an ERS), the allocation of the associated signature key and signature usage counter,
5. creation of the signature, including the signature usage counter increased by 1 and returning the signature, the signature counter, the signing time, the serial number of the signature key used to identify the CRE,
6. provision of the internal system time for the signature time with the possibility to set the system time by the administrator.

2.4 TOE Lifecycle

The TOE is part of the *Remote CSP Service* operated by D-Trust in its Trustcenter (computing center). By design, the D-Trust Web-Dienst TSE is multi-client capable. This means multiple key owners (having Client Remote Entities (CRE) installed locally) may use it in order to sign their process data. Therefore, the *Remote CSP Service* provides services for multiple "logical" CRE.

The TOE (a CSP Light Module) is operated at the *Remote CSP Service* to host signing keys for CRE Accounts. The *Remote CSP Service* operates multiple CSP Light Modules (TOEs) in order to provide load distribution and fail-safety. A TOE sample follows a defined lifecycle, specified as follows:

a) **Initialization**

For a CSP Light Module (the TOE) to be put into operation within the CSP cluster at the *Remote CSP Service*, it must be initialized by invoking the intializeCsp function at the CSP Light Module API. This function is to be triggered by the administrators using the four-eyes principle. It passes a unique ID (CspId) within the CSP cluster and two initialization "passwords" to the CSP Light Module. Each administrator contributes one secret password string of the two. Based on the concatenation of these strings the CSP internal system master keys (CspEncrKey, CspSignKey) are derived by means of cryptographic key derivation, see entry 6 in Table 1: Cryptographic primitives. After this, the passwords are no longer used by this CSP nor stored. The purpose of the passwords is the derivation of identical system master keys on different CSP modules.

During initialization of the CSP Light Module the administrator defines the behaviour of the trusted channel. The administrator also defines the cryptographic services offered to the Client Remote Entity to reduce threads based on unused functionality at the Client Remote Entity interface.

b) **Operations**

After initialization, a TOE instance may hold any number of CRE instances. Each CRE instance is represented by its CRE Account data. For each CRE Account the TOE is responsible for, the TOE holds its cryptographic data including PACE password, signing key and key usage counter (signature counter) either in the Master-CSP role or in the Slave-CSP role. The Master-CSP is the main acting CSP used for signature creation and only the Master-CSP maintains the respective key usage counter (signature counter). The Slave-CSP holds the data of a CRE instance for backup reason in case the Master-CSP fails. After incrementing the respective key usage counter (signature counter) this value is synchronized from the Master-CSP to the Slave-CSP. The Master- and Slave-CSP role, resp. may be transferred from one TOE instance to another TOE instance for a particular CRE Account, either triggered by the operations administration or caused by a break down of a TOE module (Fail-Over scenario). The Control Application module maintains the assignment of CSP instances together with their CSP roles for each CRE

Account in its database (TOE external) and is able to invoke the Master- and Slave-CSP every time a signature creation for a particular CRE Account is requested by the CRE. The Trusted Channel Data sent from the CRE is routed to the CSP in question and the Trusted Channel response data is returned to the CRE.

c) **Decommission**

For taking a TOE instance out of operation, every CRE Account (including the signature key) needs to be removed securely from the CSP. If no CRE Account is located at the particular CSP, the TOE is not invoked by the Access Control module any more. It may then be decommissioned by an administrative function invoked by the Administrator user at the Management Interface at the Remote CSP Service (in case of TSS deployment). Afterwards it may be physically removed from the CSP cluster.

2.5 CRE Account Lifecycle

Each CRE is identified by a so-called CRE Account, which follows the following lifecycle:

a) **Registration of the CRE Account**

Before a CRE can be used at the Remote CSP Service, it must be registered. A registered CRE is maintained in the Control Application database. The Control Application determines one CSP Light Module as Master-CSP and a different CSP Light Module as Slave-CSP, which serves as a backup. A CRE is identified by the so-called "key reference". This is a unique identifier (thus stands for the security attribute *Key Identity*) associated to the cryptographic data of the CRE within the CSP (PACE password, signing key, serial number and key usage counter). The key reference is also required for the initialization of a CRE (at the local site). Thus, by means of the key reference an initialized CRE is unambiguously bound to a CRE Account by referring to the CRE signing key held at its associated Master-CSP and Slave-CSP.

For setup of the CRE at the CSP the createUser API function is used. It provides the key reference and the PACE-Password for the trusted channel. This function needs to be invoked at the Master-CSP and the Slave-CSP the particular CRE is associated to. After this, the generateKey API function is to be invoked at the Master-CSP by the CRE user. This generates a signing key for this CRE. Then the key data needs to be transferred cryptographically secured to the Slave-CSP by means of the transferClusteredKey and syncClusteredKeyAPI functions.

b) **Signing Key Application**

Once a trusted channel request is received at the Remote CSP Service, the Control Application selects the Master-CSP associated to the requested key reference and forwards the request to it. In case of a signing request the signData API function is invoked through the trusted channel on the respective Master-CSP. This creates the signature and returns it to the Control Application encrypted in the trusted channel. Before returning the response the Application Control synchronizes the signature counter with the Slave-CSP. To do so it uses the transferSigCnt API function which returns the increased value of the key usage counter cryptographically sealed. It then uses the syncSigCnt API function on the Slave-CSP to import the new key usage counter. Finally the trusted channel respond gets sent to the CRE.

c) **Removal of the CRE Account together with Signing Key**

For decommissioning a particular CRE, its signing key needs to be removed at the associated Master-CSP and Slave-CSP. The TOE will remove the related persistent data at operating system level after their content was completely overwritten with zeros.

2.6 Startup and State

The TOE is a server application running on a dedicated operating system and hardware platform. Each hardware platform runs exactly one CSP Light Module. After power on of the hardware sample the installed operating system boots and enters its operational state only after the verification of the integrity of the server image is passed successfully. The application software comprising the TOE application starts after the boot up of the operating system is successfully completed. At start up, the TOE application software starts the TOE Self Test in any case.

The TOE configuration and all application data (e.g. CRE Account data including CRE signing key together with its security attributes) are stored persistently at the hardware file system.

The state of Trusted Channels (e.g. session secrets) and any authentication of external entities is held in volatile memory (RAM) only. Because of this any Trusted Channel and any authentication needs to be established (authenticated) again after reboot of the system e.g. at power on or reset.

2.7 Self Testing

The TOE implements Self Testing. During the self test, the TOE checks his security functionality and verifies the integrity of his data. This self testing is performed at power on or reset of the TOE and can be triggered via its API.

2.8 Required non-TOE Software / Hardware / Firmware

The use of the TOE requires the provision of a special operating environment consisting of software, hardware and operational environment:

2.8.1 Software

The TOE software is implemented in the Java programming language and is executable with the Java runtime from OpenJDK 17.

The operating system is set to Red Hat Enterprise Linux 8[1] (with minor release 8.7 or later and Kernel 4.18.0-xx., x86_64 Architecture) with SELinux as a security extension. A hardening directive for this operating system will be created, based on the developer's hardening guide [REDHAT], which guarantees the safe operation of the TOE.

2.8.2 Hardware

The TOE needs to run on one of the following hardware platforms:

- PrimeKey SEE Platform ("Secure Execution Environment") of the company "PrimeKey Labs GmbH". The overall product version 1.2.2 includes the TAs (Trust Anchor) firmware version 1.0.2 (FIPS certified) and the hardware version 1.0.0 (FIPS certified). This product provides an interface ("SEE Loader", certified to FIPS 140-2 Level 3) through which the required TOE software is deployed.
- Enforcer R2 of the company "private machines". The R2 version includes the hardware version ENFORCER.R2.X12SDV.1.0.0 and the following software/firmware versions: Security Anchor Bootloader 1.0.0, Security Anchor Firmware 1.4.0, libdrbg: 1.0.2, libucl: 2.5.13, Compute Engine Firmware: 1.0.0, Compute Engine Application 1.0.0, Compute Engine PM FIPS Crypto Library: 1.0.0.

This hardware is selected, because it is certified by FIPS 140-2 Level 3 (or FIPS 140-3 Level 4 respectively)[2]. This certification demonstrates that the hardware is using successful measures to prevent physical attackers from gaining access to the data of hardware.

The platform also provides a hardware-based, random number generator that is used by the TOE as an entropy source for seeding the TOEs deterministic RNG.

Although there are several CSP Light Module samples within the Remote CSP Service for redundancy reasons, each instance of a CSP Light Module is operated on a separate hardware unit. Each CSP Light Module is thus physically separated from its non-TOE environment.

2.9 Operational Environment

The TOE is securely operated in the D-Trust Trustcenter environment which is certified according to ISO/IEC 27001. The Trustcenter operates in conformance to an Information Security Management System (ISMS) with security level 'high' according to the Assumptions (A.SecComm) in [PP-CSP-LIGHT] and the Appendix: "Operational Requirements for CSPLight" in [PP-SMAERS].

2.10 TOE Specifications

The TOE follows the following specifications:

- Technische Richtlinie TR-03153 ([BSI-TR-03153]): "Technische Sicherheitseinrichtung für Elektronische Aufzeichnungssysteme". This document describes the basic structure of a TSS and its functionality. The major components of the TSS are the secure element (SE), the SE-API and the secure storage.
- Technische Richtlinie TR-03151 ([BSI-TR-03151]): "Secure Element API (SE-API)". This document defines treating the transactions and retrieving the signed data from the secure element as well as the management functionality. In addition, it defines the data formats for the messages that are created by the TSS.
- Common Criteria Protection Profile BSI-CC-PP-0105 ([PP-SMAERS]): Schutzprofil für die Anwendungskomponente des Sicherheitsmoduls ("Security Module Application for Electronic Record-keeping Systems", SMAERS). This PP defines the security functional and security assurance requirements for the SMAERS that is using the TOE.

[1] As an alternative the equivalent AlmaLinux (https://almalinux.org/de/) can be used.

[2] Please note that – by the time of the creation of this document – the FIPS certification of the Enforcer R2 has not yet been finished

- Common Criteria Protection Profile BSI-CC-PP-0111 ([PP-CSP-LIGHT]): Schutzprofil für einen einfachen kryptographischen Dienstanbieter ("Cryptographic Service Provider Light", CSP-L). This Protection Profile contains the requirements for the TOE described in this ST.
- BSI-CC-PP-0112-2020 ([PPC-CSP-LIGHT-TS-AU]) "Common Criteria Protection Profile Configurations, Cryptographic Service Provider Light – Time Stamp Service and Audit (PPC-CSPLight-TS-Au), Protection Profile-Module CSPLight Time Stamp Service and Audit (PPM-TS-Au)"
- BSI-CC-PP-0113-2020 ([PPC-CSP-LIGHT-TS-AU-CL]) "Common Criteria Protection Profile Configuration, Cryptographic Service Provider Light – Time Stamp Service and Audit - Clustering (PPC-CSPLight-TS-Au-Cl), Protection Profile-Module CSPLight Clustering (PPM-Cl)"

3. TOE description

The TOE is the main part of the D-Trust TSS Remote CSP Service. It is comprised of a software module running on a java virtual machine (JVM) based on Red Hat Linux 8 (64-bit) on a Secure Execution Environment (see chapter 2.8.2).

3.1 Physical Boundaries of the TOE

The TOE is a software server application expected to run on a java virtual machine (JVM) together with an operating system that supports the execution of the JVM. The TOE as a software application does not have any physical boundaries. The complete TOE in terms of the Common Criteria includes:

1. the software application implementing the CSP functionality as a server, delivered in form of a set of jar-files (java archive) integrity protected by a digital signature,
2. an integration, configuration and operations manual formatted as a PDF document [CSP-AGD],
3. an interface definition for application developer formatted as a PDF document [CSP-FSP],
4. the initial passwords of the system users (Administrator, Timekeeper and Auditor-Manager).

As desired, the guidance documents and the TOE are delivered to the customer via a personal delivery, encrypted and signed email or a secure download portal. These deliverables are signed in order to allow a verification of their authenticity at any time. The initial passwords are only delivered via verbal, personal delivery and are not written down in a document.

3.2 Logical Boundaries of the TOE

The TOE exposes its services via application interfaces by means of RESTful interfaces based on the HTTP protocol. These interfaces are only to be consumed by other applications in the client role. The TOE does not provide any kind of interface for direct user interaction. The TOE is only invoked by other components and does not access other components actively. Thus, it is a pure server application.

Provided Interfaces

The application interfaces (the RESTful interfaces) are divided into two logical end points, based on its purpose. Each endpoint is exposed by a particular TCP/IP port. Thus, the TOE provides the following logical interfaces:

Client Remote Interface:

The Client Remote Interface includes all operations necessary for the interaction with the CRE: establishment of the Trusted Channel (PACE connection), signing of transaction data, retrieval of key information, and support for the CRE update code package operation. At protocol level the operations of this interface are invoked by the Control Application module directly by means of HTTP requests (RESTful) over TCP/IP. The Control Application module is an internal Remote CSP Service module receiving the client requests from the CRE.

After establishment of the Trusted Channel the Control Application module hands over the encrypted Trusted Channel data obtained from the CRE to the CSP and returns the encrypted Trusted Channel data returned from the CSP inside the HTTP response to the CRE. This means that at the logical level of the Trusted Channel the communication endpoints are determined by the CRE module on the client side and the TOE.

In addition to the Trusted Channel data, routing parameters are included in the request to the CSP. They are required for the CSP Light Module to determine the particular trusted channel, since it serves several trusted channel connections from different CRE instances. The plain text routing parameters are cryptographically bound to the Trusted Channel data, so that forgery is warded off.

The Administration Interface:

The Administration Interface includes all operations necessary for initialization of a CSP Light Module, account operations (register, update CRE Account including management of the users password), generation and destruction of the signing key of a CRE, retrieval of CSP related key information, update of the CSP internal system time used for the signing time (log time) at signature creation.

3.3 Clustering

The TOE supports the Clustering concept based on [PP-CSP-LIGHT-TS-AU-CL]. Therefore, operations for synchronising the security attribute *signature key usage counter* from Master- to Slave-CSP and the transfer of the CRE signing key with security attributes from Master-CSP to Slave-CSP, and to transfer the Master-CSP and Slave-CSP role between TOE samples are provided. These operations are provided by the Administration Interface.

3.4 Timestamp and Auditing

The TOE supports the Timestamp and Audit services as defined by [PPC-CSP-LIGHT-TS-AU]. Therefore, an operation for adjusting the internal system time of the TOE is provided at its interface. The internal system time of the TOE is used to augment the transaction and audit log messages with a reliable signing time. So, 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.

The audit functionality generates audit records on defined user activities (e.g. key generation, key destruction) and security events (e.g. time update, update code package) of the TOE. These audit records are actively retrieved by the CRE in form of audit log messages.

3.5 Cryptographic Primitives

The following table summarizes the cryptographic primitives that are exposed via the interfaces of the TOE.

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits, ECC curve	Standard of Application
1	Authenticity of exported user data, Authenticity of Evidence Attestation Data	SHA384withPLAIN-ECDSA	FIPS PUB 186-4 B.4 and D.1.2.4 [FIPS PUB 186-4]	384 bit Curve: 1.3.132.0.34 (secp384r1)	[PP-CSP-LIGHT]
2	Communication with Client using PACE with generic mapping	- PACE with AES/CBC/ PKCS5Padding - CMAC and ECDHE	TR-03110-2 [TR-03110]	256 bit Curve: 1.3.36.3.3.2.8.1.1.7 (brainpoolP256r1)	[PP-CSP-LIGHT]
3	Communication with Client using PACE with Terminal and Chip Authentication	AES, CBC CMAC	[FIPS197]	256 bit	[PP-CSP-LIGHT]
4	Authenticity of imported Update Code Packages	SHA256withPLAIN-ECDSA	RFC5639 [RFC5639]	256 bit Curve: 1.3.36.3.3.2.8.1.1.7 (brainpoolP256r1)	[PP-CSP-LIGHT]
5	Confidentiality of imported Update Code Packages	- SHA256withPLAIN-ECDSA - AES	RFC5639 [RFC5639] FIPS PUB 197 [FIPS197]	256 bit Curve: 1.3.36.3.3.2.8.1.1.7 (brainpoolP256r1) 256 bit	[PP-CSP-LIGHT]
6	CSP initialization - generation of system master keys	SHA256 operation to generate AES keys (for encryption and CMAC), derived from two base keys	NIST FIPS PUB 180-4 [FIPS PUB 180-4]	256 bit	[PP-CSP-LIGHT-TS-AU-CL]
7	Signing key generation (key owner CRE key)	ECDSA DRG.3	FIPS PUB 186-4 B.4 and D.1.2.4 [FIPS PUB 186-4], [AIS20]	384 bit Curve: 1.3.132.0.34 (secp384r1)	[PP-CSP-LIGHT]
8	Serialnumber calculation of Remote Client Entity Public Key	SHA256	NIST FIPS PUB 180-4 [FIPS PUB 180-4]	256 bit	[PP-CSP-LIGHT]
9	Authenticity of signing key and security attributes	AES CMAC (truncated to 8 Byte)	NIST-SP800-38B [NIST-SP800-38B]	256 bit	[PP-CSP-LIGHT-TS-AU-CL]

10	Confidentiality of signing key and security attributes	AES/CBC/PKCS5Padding	FIPS PUB 197 [FIPS197]	256 bit	[PP-CSP-LIGHT-TS-AU-CL]
11	RSA signing key generation	RSA	PKCS #1 v2.2 [PKCS#1]	3072 bit	[PP-CSP-LIGHT]
12	ECDHE key derivation	ECDHE key agreement and key derivation [TR-03110-3] [TR-03111]	TR-03110-3 section A.2.3 TR-03111 [TR-03111]	128, 256 bit 256 bit Curve: 1.3.36.3.3.2.8.1.1.7 (brainpoolP256r1)	[PP-CSP-LIGHT]
13	Verification of Authenticity of exported user data, Verification of Authenticity of Evidence Attestation Data	SHA384withPLAIN-ECDSA	FIPS PUB 186-4 B.4 and D.1.2.4 [FIPS PUB 186-4]	384 bit Curve: 1.3.132.0.34 (secp384r1)	[PP-CSP-LIGHT]
14	Creation and verification of RSA signature	RSA EMSA-PSS	ISO/IEC 14888-2 [ISO/IEC 14888-2], PKCS #1 v2.2 [PKCS#1]	3072 bit	[PP-CSP-LIGHT]
15	HMAC generation, HMAC verification	HMAC-SHA256	RFC2104 [RFC2104], ISO 9797-2 [ISO/IEC 9797-2]	256 bit	[PP-CSP-LIGHT]
16	Hybrid encryption and decryption of user data	brainpolP256r1 brainpolP256r1 CMAC AES, CBC	[RFC5639] [RFC6954] [NIST-SP800-38B] [FIPS197]	AES 256 bit	[PP-CSP-LIGHT]

Table 1: Cryptographic primitives

4. Conformance Claims

4.1 Common Criteria Conformance Claim

This Security Target claims conformance to:

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

as follows:

1. CC Part 2 extended,
2. CC Part 3 conformant (EAL 2 augmented with ALC_CMS.3, ALC_LCD.1).

4.2 Protection Profile Conformance Claim

This Security Target claims strict conformance to the Protection Profile Configuration "Cryptographic Service Provider Light – Time Stamp Service Audit and Clustering (PPC-CSPLight-TS-Au-Cl)".

This PP-Configuration consists of the Base-PP [PP-CSP-LIGHT] together with two PP-Modules BSI-CC-PP-0112-2020 [PPC-CSP-LIGHT-TS-AU] and BSI-CC-PP-0113-2020 [PPC-CSP-LIGHT-TS-AU-CL].

4.3 Conformance Rationale

The TOE as described in this Security Target is a product to provide cryptographic services for the protection of the confidentiality and the integrity of user data, and for entity authentication, which is defined as the TOE Type by [PP-CSP-LIGHT].

[PP-CSP-LIGHT] requires strict conformance, which is claimed by this Security Target.

Two PP-Modules [PPC-CSP-LIGHT-TS-AU] and [PPC-CSP-LIGHT-TS-AU-CL] are used in this Security Target, which are consistent for the PP-Configuration.

[PPC-CSP-LIGHT-TS-AU] and [PPC-CSP-LIGHT-TS-AU-CL] requires strict conformance which is claimed by this Security Target.

5. Security Problem Definition Base-PP

5.1 Introduction

Assets

The assets of the TOE are

1. user data, whose integrity and confidentiality shall be protected,
2. cryptographic services and keys which shall be protected against unauthorized use or misuse, and whose integrity shall be protected,
3. update code packages (UCP), whose integrity and confidentiality shall be protected,
4. additional TSF-data (e.g. security flags), whose integrity and/or confidentiality shall be protected,
5. other TOE resources, whose unauthorized use and misuse shall be prevented.

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

Users and subjects

The TOE knows external entities (users) as

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

The TOE communicates with

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

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.

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 CSP. TSF data objects are created, temporarily or permanently stored, imported, exported and destroyed as objects of the security management. They may contain e. g. cryptographic keys with their security attributes, certificates, or authentication data records with authentication reference data of a user. Cryptographic keys are objects of the key management.

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

1. User Identity (User-ID),
2. Authentication reference data,
3. Role.

Passwords as Authentication Reference Data have the security attributes

1. status: values initial password, operational password,
2. 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 at least the following roles that can be taken by a user or a subject:

Role	Description
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 successful authenticated user in this role is allowed to access the TOE in order to perform management functions. It is taken by a human user or a subject acting on behalf of a human user after successful authentication as an Administrator.
Key Owner	A successful authenticated user 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 physically separated secure channel or through a trusted channel (which requires assured identification of its end points).

The Administrator role may be split into more detailed roles:

1. Crypto-Officer: a role that is allowed to access the TOE in order to manage a cryptographic TSF.
2. User Administrator: a role that is allowed to access the TOE in order to manage users.
3. Update Agent: a role that is allowed to import and install update code packages.

The SFR uses the general term Administrator or a selection between Administrator role and these detailed roles in case they are supported by the TOE and separation of duties is appropriate.

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

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

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

Cryptographic keys have at least the security attributes

1. Key identity, i.e. an attribute that uniquely identifies the key,
2. Key Owner, i.e. the identity of the owner this key is assigned to,
3. Key type, i.e. whether the key is as secret key, a private key, or a public key,
4. 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.
5. 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,

   and may have the security attributes
6. 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.

7. key usage counter, i. e. the number of operations performed with this key – for example the current number of signatures created with a private signature key.

The UCP have at least the security attributes

1. issuer of the UCP,
2. version number of the UCP.

5.2 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.

5.3 Organizational 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 CSP before storing any update data in the TOE. The TOE restricts the storage of authentic Update Code Package to authorized users.

5.4 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.

6. Security Problem Definition Timestamp and Audit [PPC-CSP-LIGHT-TS-AU]

6.1 Introduction

Assets

The assets of the TOE are

1. user data and time stamps shall be integrity protected,
2. time services which time base shall be protected against manipulation.

The cryptographic keys are TSF data because they are used for cryptographic time stamp operations protecting user data and audit records, 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.

Subjects

The TOE knows subjects as defined in the Base-PP. They obtain their associated security attributes by the TSF defined in the Base-PP. The security attributes of subjects known to the TOE are defined in the Base-PP

1. User Identity (User-ID),
2. Authentication reference data,
3. Role.

Objects

User data objects of the time stamp service are imported, used in time stamp operation, exported and destroyed after use. TSF data objects time and time stamps are created, temporarily or permanently stored, imported, exported and destroyed as objects of the security management. Cryptographic keys used by the time stamp service are TSF data objects of the key management as described in the Base-PP.

Security attributes

The role Administrator defined in the Base-PP may be split in more detailed roles. One of these roles may be

1. **Auditor Manager: role that is allowed to configure the audit functionality and read system audit logs,**
2. **Audit Log Receiver: role that is allowed to read audit logs associated to their own keys,**
3. The Timekeeper is allowed to adjust the internal time.

Cryptographic keys used for the time stamp service and the export of audit records have at least the security Attributes

1. Key identity that uniquely identifies the key,
2. Key Owner, i. e. the identity of the entity this key is assigned to,
3. Key type, i. e. as secret key, private key, public key,
4. Key usage type, identifying the cryptographic mechanism or service the key can be used for, where the keys for time stamp service (cf. FDP_DAU.2/TS) have the key usage type "TimeStamp",

and may have the security attribute

1. Key usage counter, i. e. the number of operations performed with this key, where the key usage counter of the private key used for time stamp service counts the number of created signature
2. Key validity time period, i. e. the time period for operational use of the key; the key must not be used before or after this time slot.

6.2 Threats

The PP-Module does not define threats additional to those defined in the Base-PP.

6.3 Organisational security policies

The PP-Module defines the following organisational security policies additional to those defined in the Base-PP.

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.

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.

6.4 Assumptions

The PP-Module does not define assumptions additional to those defined in the Base-PP.

7. Security Problem Definition Clustering [PPC-CSP-LIGHT-TS-AU-CL]

7.1 Introduction

Assets

The TOE protects the TSF data, the security attributes of the known users and the cryptographic keys with their security attributes transferred between Master-CSPLight and Slave-CSPLights.

Users and subjects

The TOE knows external entities (users) as

1. human user communicating with the TOE for security management of the TOE,
2. application component using the cryptographic and other security services of the TOE and supporting the communication with remote entities (e. g. by providing certificates),
3. cluster-CSPLight being another TOE sample in a cluster with the TOE.

The TOE communicates with cluster-CSPLight in encrypted and integrity protected form. The communication with human users and application component is described in the Base-PP. The subjects as active entities in the TOE perform operations on objects. They obtain their associated security attributes from the authenticated users on behalf they are acting, or by default.

Objects

The TSF operates TSF data objects (i. e. passive entities, that contain or receive information, and upon which subjects perform operations). The TSF data objects contain the security attributes of the known users and the cryptographic keys with their security attributes transferred between Master-CSPLight and Slave-CSPLights.

Security attributes

The security attributes of user known to the TOE are stored as defined in the Base-PP in Authentication Data Records containing

1. User Identity (User-ID),
2. Authentication reference data,
3. Role with detailed access rights.

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

1. Administrator: successful authenticated user allowed to access the TOE in order to perform management functions. It is taken by a human user or a subject acting on behalf of a human user after successful authentication as Administrator.

The role Administrator defined in the Base-PP may be split in more detailed roles:

1. Crypto-Officer: role that is allowed to access the TOE in order to perform management of a cryptographic TSF.
2. User Administrator: role that is allowed to access the TOE in order to perform user management.

The SFR uses the general term Administrator or a selection between Administrator role and these detailed roles in case they are supported by the TOE and separation of duties is appropriate.

1. Application Component: subjects in this role are allowed to use assigned security services of the TOE without authenticated human user session (e. g. export and import of wrapped keys). This role may be assigned to an entity communicating through a physically separated secure channel or through a trusted channel (which requires assured identification of its end points).
2. Cluster-CSPLight: another TOE sample in a 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 cryptographic keys and their security attributes are defined in the Base-PP and the PP-Module PPM-CSPLight-TS-Au. The PP-Module PPM-CSPLight-CL uses the security attributes

1. Key identity that uniquely identifies the key,
2. Key Owner, i. e. the identity of the entity this key is assigned to,
3. Key type, i. e. as secret key, private key, public key,
4. Key usage type, identifying the cryptographic mechanism or service the key can be used for; the PP-Module use the clustering encryption key for cryptographic operation according to FCS_COP.1/ED and clustering MAC keys for cryptographic operation according to FCS_COP.1/MAC as defined in the Base-PP.

5. Key access control attributes, i. e. list of combinations of the identity of the user, the role for which the user is authenticated and the allowed key management function or cryptographic operation, including
    - Clustering: 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.

7.2 Threats

The security problem definition of the PP-module does not define any threats additional to the threats described in the Base-PP.

7.3 Organisational security policies

The PP-Module defines the following organisational security policies additional to those defined in the Base-PP.

OSP.Cluster Cluster of 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.

7.4 Assumptions

The PP-Module defines the following assumptions additional to those defined in the Base-PP.

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-CSPLights as necessary for scalability of performance and availability of security services

8. Security Objectives

8.1 Security Objectives for 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 provide 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.

Additional Security Objectives for the TOE by [PPC-CSP-LIGHT-TS-AU]:

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 provide an internal time service and time stamp service for the user.

Additional Security Objectives for the TOE by [PPC-CSP-LIGHT-TS-AU-CL]:

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-CSPLights in encrypted and integrity protected form.

8.2 Security Objectives for the Operational 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.

Additional Security Objectives for the Operational Environment by [PPC-CSP-LIGHT-TS-AU]:

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.

Additional Security Objectives for the Operational Environment by [PPC-CSP-LIGHT-TS-AU-CL]:

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-CSPLights as necessary for scalability of performance and availability of security services.

8.3 Security Objectives Rationale

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

	T.DataCompr	T.DataMani	T.Masqu	T.ServAcc	T.PhysAttack	T.FaUpD	OSP.SecCryM	OSP.SecService	OSP.KeyMan	OSP.TC	OSP.Update	A.SecComm
O.AccCtrl				x								
O.AuthentTOE							x	x				
O.DataAuth		x					x	x				
O.Enc	x						x	x				
O.I&A			x	x			x	x				
O.RBGS							x	x				
O.SecMan			x				x		x	x		
O.SecUpCP						x					x	
O.TChann	x	x	x	x			x	x				
O.TST					x							
OE.AppComp	x	x		x						x		
OE.CommInf	x	x		x				x	x	x		
OE.SecComm	x	x		x								x
OE.SecManag			x					x	x			
OE.SUCP						x					x	
OE.SecPlatform					x							

Table 2: Security Objectives Rationale

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

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

- O.Enc requires the TOE to provide encryption and decryption as 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.

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 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.

Security Objectives Rationale by [PPC-CSP-LIGHT-TS-AU]:

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

	OSP.Audit	OSP.TimeService
O.Audit	x	
O.TimeService		x
OE.Audit	x	
OE.TimeSource		x

Table 3: Security Objectives Rationale by [PPC-CSP-Light-TS-AU]

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

The organizational security policy OSP.Audit "Audit for key management and cryptographic operations" is directly implemented by

1. the security objective for the TOE O.Audit requiring security auditing and
2. 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

1. 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
2. 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.

Security Objectives Rationale by [PPC-CSP-LIGHT-TS-AU-CL]:

The following table traces the security objectives for the TOE back the OSPs enforced by that security objective, and the security objective for the operational environment back OSPs enforced by that security objective, and assumptions upheld by that security objective. Note the OSP.SecCryM "Secure cryptographic mechanisms" defined in the Base-PP.

	OSP.SecCryM	OSP.Cluster	A.ClusterAppl
O.Cluster	x	x	
OE.ClusterCtrl		x	
OE.TSFdataTrans		x	x

Table 4: Security Objectives Rationale by [PPC-CSP-Light-TS-AU-CL]

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

The organizational security policy OSP.SecCryM "Secure cryptographic mechanisms" defined in the Base-PP is implemented by means of secure cryptographic mechanisms required in

1. 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:

1. 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.
2. 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.
3. 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 assumption A.ClusterAppl is directly ensured by OE.TSFdataTrans.

9. Extended Components Definition

9.1 Generation of random numbers (FCS_RNG)

Family Behaviour

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

Component levelling:

FCS_RNG: Random number generation	1

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

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no auditable events foreseen.

FCS_RNG.1 Random number generation

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

9.2 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].

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

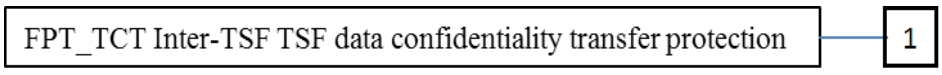
9.4 Inter-TSF TSF data confidentiality transfer protection (FPT_TCT)

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

Family Behaviour

This family requires confidentiality protection of exchanged TSF data.

Component levelling:



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

Management: FPT_TCT.1

There are no management activities foreseen.

Audit: FPT_TCT.1

There are no 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	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.

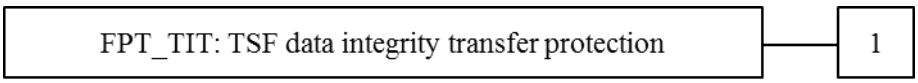
9.5 Inter-TSF TSF data integrity transfer protection (FPT_TIT)

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.

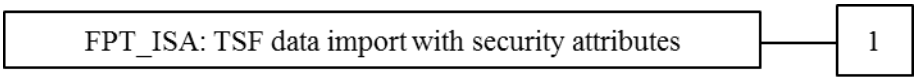
9.6 TSF data import with security attributes (FPT_ISA)

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_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] [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].

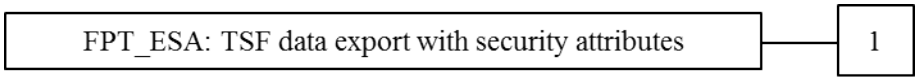
9.7 TSF data export with security attributes (FPT_ESA)

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].

10. Security Requirements

The CC allows several operations to be performed on functional requirements: *refinement*, *selection*, *assignment*, and *iteration*. Each of these operations is used in this ST.

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

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the ST authors are denoted as *italic* text and the original text of the component is given by a footnote.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as e.g. the length of a password. Assignments that have been made by the ST authors are denoted by showing as *italic* text and the original text of the component is given by a footnote.

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

A "ST Application Note" is used to interpret the given information of the security requirement above.

All references of tables in the PP application notes and footnotes applied to selections or assignments are references of the tables shown in the PP.

10.1 Security functional requirements

The TOE provides cryptographic security services for encryption and decryption of user data, entity authentication of external entities and to external entities, authentication prove and verification of user data, trusted channel 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 9.3 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. 10.1.4. The authentication may be mutual as required for trusted channels in chapter 10.1.5.

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 non-repudiation 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 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.

10.1.1 Key management

a) **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 on

(1) subjects: *Administrator*[3], Key Owner;

(2) objects: operational cryptographic keys;

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

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 to restrict the ability to

(1) set and change default values for 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 to *Administrator*[4],

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

(3) modify independent on key usage the security attributes Key usage counter of an existing key to none.

(4) modify the security attributes Key access control attribute of an existing key to *Administrator*[5],

(5) query the security attributes Key type, Key usage type, Key access control attributes, Key validity time period and Key usage counter of an identified key to *Administrator, Key Owner*[6]*.*

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

Consideration of PP Application Note 1: The application note does not require any action in this ST.

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 to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/KM The TSF shall allow the *Administrator*[7] to specify alternative initial values to override the default values when a cryptographic key is created.

---

[3] [selection: Administrator, Crypto-Officer]

[4] [selection: Administrator, Crypto-Officer]

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

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

[7] [selection: Administrator, Crypto-Officer]

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 the cryptographic keys to *Administrator, Key Owner*[8],

(2) import according to FPT_TCT.1/CK, FPT_TIT.1/CK and FPT_ISA.1/CK the cryptographic keys to *Administrator*[9],

(3) export according to FPT_TCT.1/CK, FPT_TIT.1/CK and FPT_ESA.1/CK the cryptographic keys to *Administrator*[10] 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 the cryptographic keys to *Administrator, Key Owner*[11].

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

Consideration of PP Application Note 2: The application note does not require any action in this ST.

ST application note 1: Transfer of any data between TOE samples in a cluster is not restricted by these rules. The respective rules are defined in MFT_MTD.1.1/CL.

b) **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 in accordance with a specified cryptographic algorithm SHA-256, SHA-384, SHA-512 and cryptographic key sizes none that meet the following: FIPS 180-4 [FIPS PUB 180-4].

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

Consideration of PP Application Note 3: The application note is considered in this ST.

c) **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, modify, clear and delete the root key pair to *Administrator*[12].

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

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

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

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

[12] [selection: Administrator, Crypto-Officer]

(2) import and delete a known as authentic public key of a certification authority in a PKI to *Administrator*[13].

PP Application note 4: The root key is defined here with respect to the key hierarchy known to the TOE. In case of clause (1), i. e. may be a key pair of an TOE internal key hierarchy. In clause (2) it may be a root public key of a PKI or a public key of another certification authority in a PKI known as 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.

Consideration of PP Application Note 4: The application note is considered in this ST.

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 to receive a certificate in a manner protected from modification and insertion errors.

FPT_TIT.1.2/Cert The TSF shall be able to determine on receipt of a certificate, whether modification and insertion has occurred.

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

Hierarchical to: No other components.

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

FPT_ISA.1.1/Cert The TSF shall enforce the Key management SFP when importing certificates, 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.

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 received.

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

FPT_ISA.1.5/Cert The TSF shall enforce the following rules when importing certificates 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.

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

Hierarchical to: No other components.

[13] [selection: Administrator, Crypto-Officer]

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 when shared between the TSF and another trusted IT product.

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

(1) the TOE reports about conflicts between the Key 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 when interpreting the certificate from a trust centre.

PP Application note 5: 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).

Consideration of PP Application Note 5: The application note is considered in this ST.

d) **Key generation, agreement and destruction**

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a *deterministic*[14] random number generator that implements:

(DRG.3.1) If initialized with a random seed using PTRNG (of the SEE hardware) as random source, the internal state of the RNG shall have 125 bit of entropy.

(DRG.3.2) The RNG provides forward secrecy.

(DRG.3.3.) The RNG provides backward secrecy even if the current internal state is known[15].

FCS_RNG.1.2 The TSF shall provide random numbers that meet

(DRG.3.4) The RNG initialized with a random seed using the PTRNG generates output for which 2^19 strings of bit length 128 are mutually different with probability ≥ 1 - 2^(-10).

(DRG.3.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A [BSI-TEST-SUITE].[16]

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

Consideration of PP Application Note 6: The application note is considered in this ST. As the TOE is a software application it has to rely on its environment to provide real random input as a seed for the random number generator. The TOE will retrieve 256 random bits for seeding its RNG from the physical RNG of its Secure Execution Environment.

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

[14] [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]

[15] [assignment: list of security capabilities]

[16] [a defined quality metric]

FCS_CKM.1.1/AES The TSF shall generate cryptographic AES keys in accordance with a specified cryptographic key generation algorithm AES and specified cryptographic key sizes 128 bits, *256 bits*[17] that meet the following: ISO 18033-3 [ISO/IEC 18033-3].

PP Application note 7: The cryptographic key(s) may be also used together with FCS_COP.1/ED, e. g. for internal purposes.

Consideration of PP Application Note 7: The cryptographic keys are not used 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 from *a string of two password, which has a length of 12 characters each with at least one uppercase and one lowercase letter, one digit and one special character*[18], in accordance with a specified cryptographic key derivation algorithms AES key generation using a bit string derived from input parameters with a KDF and specified cryptographic key sizes 128 bits, *256 bits*[19], that meet the following: NIST SP800-56C [NIST-SP800-56C].

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

Hierarchical to: No other components.

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

FCS_CKM.1.1/ECC The TSF shall generate cryptographic elliptic curve key pairs in accordance with a specified cryptographic key generation algorithm ECC key pair generation with *Curve P-384*[20] and specified cryptographic key sizes *384 bits*[21] that meet the following: *FIPS PUB 186-4 B.4 and D.1.2.4 [FIPS PUB 186-4]*[22].

ST application note 1: The elliptic curve key pair generation of FCS_CKM.1/ECC is used for the key generation of the CRE signing keys, see entry 7 of table 1 of this ST.

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

Consideration of PP Application Note 8: The elliptic key pairs are used for different key management use cases.

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

Hierarchical to: No other components.

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

FCS_CKM.5.1/ECC The TSF shall derive cryptographic elliptic curve key pairs from *Nonce of PACE protocol*[23] in accordance with a specified cryptographic key derivation algorithm ECC key pair generation with*brainpoolP256r1*[24] using bit string derived from input parameters with *EC-KP-Generator implemented by*

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

[18] [assignment: input parameters]

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

[20] [selection: elliptic curves in table 2]

[21] [selection: key size in table 2]

[22] [selection: standards in table 2]

[23] [assignment: input parameters]

[24] [selection: elliptic curves in table 2]

bouncyCastle JCE provider[25] and specified cryptographic key sizes *256 bits*[26] that meet the following: *RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111]*[27], [TR-03111].

PP Application note 9: The elliptic key pair derivation applies a key derivation function (KDF), e.g. from [TR-03111] (Section 4.3.3.) to the input parameter. It uses the output string of 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.

Consideration of PP Application Note 9: The elliptic curve key pair derivation of FCS_CKM.5/ECC is used during establishment of the trusted channel connection by the PACE protocol, see entry 2 in table 1 of this ST.

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 and specified cryptographic key sizes *3072 bits*[28] that meet the following: PKCS #1 v2.2 [PKCS#1].

PP Application note 10: The cryptographic key sizes assigned in FCS_CKM.1/RSA must be at least 2000 bits. Cryptographic key sizes of at least 3000 bits are recommended. The SFR FCS_CKM.1/RSA assigns given security attributes Key identity and Key owner.

Consideration of PP Application Note 10: Key sizes of 3072 bits are used.

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 for data encryption and MAC with AES-128, *AES-256*[29] from an agreed shared secret in accordance with a specified cryptographic key derivation algorithm Elliptic Curve Diffie-Hellman ephemeral key agreement *brainpoolP256r1*[30] and *brainpoolP256r1*[31] with a key derivation from the shared secret *according to [TR-03110-3] section "A.2.3 Key Derivation Function"*[32]and specified cryptographic key sizes 128 bits *256 bits*[33] that meet the following: TR-03111 [TR-03111].

PP Application note 11: The input parameters for key derivation is an agreed shared secret established by means of Elliptic Curve Diffie-Hellman. Table 2 lists elliptic curves and table 3 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]

---

[25] [assignment: KDF]

[26] [selection: key size in table 2]

[27] [selection: standards in table 2]

[28] [assignment: cryptographic key sizes]

[29] [selection: AES-256, none other]

[30] [selection: elliptic curves in table 2]

[31] [selection: DH group in table 3]

[32] [assignment: key derivation function]

[33] [selection:256 bits, none other]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/ECKA-EG The TSF shall generate ephemeral cryptographic elliptic curve key pairs for ECKGA-EG[TR-03111], sender role) in accordance with a specified cryptographic key generation algorithm ECC key pair generation with *brainpoolP256r1*[34] and specified cryptographic key sizes *256 bits*[35]that meet the following: *RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111]*[36].

ST application note 2: Since ECDHE was chosen in FCS_COP.1/HEM, this SFR is of no use for the TOE and won't be regarded any further.

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*[37] from a private and a public ECC key in accordance with a specified cryptographic key derivation algorithm ECKGA-EG[TR-03111] *brainpoolP256r1*[38] and X9.63 Key Derivation Function and specified cryptographic symmetric key sizes 128 bits*, 256 bits*[39] that meet the following: TR-03111[TR-03111], chapter 4.3.2.2.

PP Application note 12: FCS_CKM.5/ECKA-EG is used by both the sender (encryption) and the recipient (decryption) to compute a secret point S AB on an elliptic curve and derived a shared secret Z AB . 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 6.1.3).

Consideration of PP Application Note 12: Since ECDHE was chosen in FCS_COP.1/HEM, this SFR is of no use for the TOE and won't be regarded any further.

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*[40] in accordance with a specified cryptographic key generation algorithm X9.63 Key Derivation Function[ANSI-X9.63] and RSA EME-OAEP[PKCS#1] and specified cryptographic symmetric key sizes 128 bits*, 256 bits*[41] that meet the following: ISO/IEC18033-3 [ISO/IEC 18033-3], PKCS #1 v2.2 [PKCS#1].

PP Application note 13: The asymmetric cryptographic key sizes used in FCS_CKM.1/AES_RSA must be at least 2000 bits. Cryptographic key sizes of at least 3000 bits are recommended. FCS_CKM.1/AES_RSA and

[34] [selection: elliptic curves in table 2]

[35] [selection: key size in table 2]

[36] [selection: standards in table 2]

[37] [selection: AES-256, none other]

[38] [selection: elliptic curves in table 2]

[39] [selection:256 bits, none other]

[40] [selection: AES-256, none other]

[41] [selection:256 bits, none other]

FCS_CKM.5/AES_RSA do not provide self-contained security services for the user but they are only necessary steps for FCS_COP.1/HEM respective FCS_COP.1/HDM (refer to the next section 6.1.3).

Consideration of PP Application Note 13: Since ECDHE was chosen in FCS_COP.1/HEM, this SFR is of no use for the TOE and won't be regarded any further.

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*[42]from a decrypted RSA encrypted seed in accordance with a specified cryptographic key derivation algorithm RSA EME-OAEP[PKCS#1] and X9.63[ANSI-X9.63] Key Derivation Function and specified cryptographic symmetric key sizes 128 bits, *256 bits*[43] that meet the following: ISO/IEC 14888-2 [ISO/IEC 14888-2].

ST application note 3: Since ECDHE was chosen in FCS_COP.1/HEM, this SFR is of no use for the TOE and won't be regarded any further.

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 *zeroization*[44] that meets the following: *The key will be completely overwritten with zeros*[45].

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.

PP 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.

e) **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 in accordance with a specified cryptographic algorithm AES-Keywrap *KWP*[46] and cryptographic key sizes of the key encryption key 128 bits, *256 bits*[47] that meet the following: NIST SP800-38F [NIST-SP800-38F].

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

Consideration of PP Application Note 14: 256 bit Keywrap is chosen to accommodate for 256 bit keys.

---

[42] [selection: AES-256, none other]

[43] [selection:256 bits, none other]

[44] [assignment: cryptographic key destruction method]

[45] [assignment: list of standards]

[46] [selection: KW, KWP]

[47] [selection:256 bits, none other]

FCS_COP.1/KU Cryptographic operation – Key unwrap

Hierarchical to: No other components.

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

FCS_COP.1.1/KU The TSF shall perform key unwrap in accordance with a specified cryptographic algorithm AES-Keywrap *KWP*[48] and cryptographic key sizes of the key encryption key 128 bits, *256 bits*[49] that meet the following: NIST SP800-38F[NIST-SP800-38F].

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 by providing the ability to transmit and receive a cryptographic key 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 to transmit and receive cryptographic keys in a manner protected from modification and insertion errors according to FCS_COP.1/KW.

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

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

Hierarchical to: No other components.

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

FPT_ISA.1.1/CK The TSF shall enforce the Key Management SFP when importing cryptographic key, 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.

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 received.

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

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

---

[48] [selection: KW, KWP]

[49] [selection:256 bits, none other]

(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) *The cryptographic seal of the wrapped key (FPT_ESA.1/CK) is verified to prevent modification and insertion. If the verification fails the import is denied.*

The export time stamp associated with the key (FPT_ESA.1/CK) is verified against the actual system time of the CSP. If it differs for more than 30 seconds the import is denied[50].

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

Consideration of PP Application Note 15: The application note does not require any action in this ST.

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 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

when interpreting the imported key data object.

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 when exporting a cryptographic key, controlled under the SFP(s), outside of the TOE.

FPT_ESA.1.2/CK The TSF shall export the cryptographic key with the cryptographic key's 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.

FPT_ESA.1.4/CK The TSF shall enforce the following rules when a cryptographic key 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 *the TSF exports a time stamp of the export time together with the wrapped key. Furthermore a cryptographic seal over the wrapped key together with the export time stamp is appended to the cryptographic key. The security attribute csp role does not get exported and is set implicitly on import*[51].

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

[50] [assignment: additional importation control rules]

[51] [assignment: additional exportation control rules]

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.

Consideration of PP Application Note 16: The described threat is countered by FMT_MTD.1.1/KM clause 3 which prohibits export of keys with the security attribute "key usage counter".

10.1.2 Data encryption

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

Hierarchical to: No other components.

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

FCS_COP.1.1/ED The TSF shall perform data encryption and decryption in accordance with a specified cryptographic algorithm symmetric data encryption according to AES-128 and *AES-256*[52] in CBC and *no other*[53] mode and cryptographic key size 128 bits, *256 bit*[54] that meet the following: NIST-SP800-38A[NIST-SP800-38A], ISO 18033-3 [ISO/IEC 18033-3]~~, ISO 10116 [ISO/IEC 10116]~~.

PP Application note 17: Data encryption and decryption should be combined with data integrity mechanisms in Encrypt-then-MAC order, i. e. the MAC is calculated 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 6.1.3.

Consideration of PP Application Note 17: The application note is considered in this ST.

ST application note 4: The encryption and decryption are performed using PKCS5 [PKCS#5] Padding.

ST application note 5: The standard ISO 10116 is removed from this SFR because "no other" was chosen in selection 51. This mode is already described in ISO 18033-3 which means, ISO 10116 is not necessary.

10.1.3 Hybrid encryption with MAC for user data

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

Hierarchical to: No other components.

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

FCS_COP.1.1/HEM The TSF shall perform hybrid data encryption and MAC calculation in accordance with a specified cryptographic algorithm asymmetric key encryption according to *FCS_CKM.5/ECDHE*[55], symmetric data encryption according to AES-128, *AES-256*[56][FIPS197] in *CBC[NIST-SP800-38A]*[57] mode with *HMAC[RFC2104]*[58]

[52] [selection: AES-256, no other algorithm]

[53] [selection: CRT, OFB, CFB, no other]

[54] [selection: 256 bits, no other key size]

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

[56] [selection: AES-256, none other]

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

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

calculation and cryptographic symmetric key sizes 128 bits, *256 bits*[59] that meet the following: the referenced standards above according to the chosen selection.

PP Application note 18: 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.

Consideration of PP Application Note 18: The application note is considered in this ST.

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 in accordance with a specified cryptographic algorithm asymmetric key decryption according to *FCS_CKM.5/ECDHE*[60], verification of *HMAC[RFC2104]*[61] and symmetric data decryption according to AES with *AES-256*[62][FIPS197] in mode *CBC[NIST-SP800-38A]*[63] and cryptographic symmetric key sizes 128 bits, *256 bits*[64] that meet the following: the referenced standards above according to the chosen selection.

PP Application note 19: 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.

Consideration of PP Application Note 19: The application note is considered in this ST.

10.1.4 Data integrity mechanisms

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 in accordance with a specified cryptographic algorithm AES-128 and *AES-256*[65][FIPS197] CMAC[NIST-SP800-38B] and *no other*[66] and cryptographic key sizes 128 bits*, 256 bits*[67] that meet the following: the referenced standards above according to the chosen selection.

PP Application note 20: The MAC may be applied to plaintexts and cipher texts. The algorithm AES-128 CMAC is mandatory.

---

[59] [selection: 256 bits, no other key size]

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

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

[62] [selection: AES-128, AES-256]

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

[64] [selection: 256 bits, no other key size]

[65] [selection: AES-256, none other]

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

[67] [selection: 256 bits, no other key size]

Consideration of PP Application Note 20: The application note is considered in this ST.

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 in accordance with a specified cryptographic algorithm HMAC-SHA256 and *no other*[68] and cryptographic key sizes *256 bits*[69] that meet the following: RFC2104 [RFC2104], ISO 9797-2 [ISO/IEC 9797-2].

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

Consideration of PP Application Note 21: The application note is considered in this ST.

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 in accordance with a specified cryptographic algorithm ECDSA with *Curve P-384*[70] and cryptographic key sizes *384 bits*[71] that meet the following: *FIPS PUB 186-4 B.4 and D.1.2.4 [FIPS PUB 186-4]*[72].

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 in accordance with a specified cryptographic algorithm ECDSA with *Curve P-384*[73] and cryptographic key sizes *384 bits*[74] that meet the following: *FIPS PUB 186-4 B.4 and D.1.2.4 [FIPS PUB 186-4]*[75].

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]

---

[68] [selection: HMAC-SHA-1, HMAC- SHA384, no other]

[69] [assignment: cryptographic key sizes]

[70] [selection: elliptic curves in table 2]

[71] [selection: key size in table 2]

[72] [selection: standards in table 2]

[73] [selection: elliptic curves in table 2]

[74] [selection: key size in table 2]

[75] [selection: standards in table 2]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/CDS-RSA The TSF shall perform signature-creation in accordance with a specified cryptographic algorithm RSA and EMSA-PSS and cryptographic key sizes *3072 bits*[76] that meet the following: ISO/IEC 14888-2 [ISO/IEC 14888-2], PKCS #1, v2.2 [PKCS#1].

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

Hierarchical to: No other components.

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

FCS_COP.1.1/VDS-RSA The TSF shall perform signature-verification in accordance with a specified cryptographic algorithm RSA and EMSA-PSS and cryptographic key sizes *3072 bits*[77] that meet the following: ISO/IEC 14888-2 [ISO/IEC 14888-2], PKCS #1, v2.2 [PKCS#1].

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 imported according to FDP_ITC.2/UD by means of *FCS_COP.1/CDS-ECDSA*[78] 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 with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

PP Application note 22: 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.

Consideration of PP Application Note 22: The application note is considered in this ST.

10.1.5 Authentication and attestation of the TOE, trusted channel

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/CA The TSF shall provide Chip Authentication Version 2 according to [TR-03110] section 3.4 to prove the identity of the TOE 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

[76] [assignment: cryptographic key sizes]

[77] [assignment: cryptographic key sizes]

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

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 by means of *FCS_COP.1/CDS-ECDSA*[79] 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 with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

PP Application note 23: 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].

Consideration of PP Application Note 23: The attestation data includes:

- Client input data,
- Product identifier: D-TRUST CSP Web Dienst TSE CSP,
- Software version,
- CC-certification ID,
- CSP-ID,
- Timestamp in the format YYYY.MM.DD hh:mm:ss,
- 256 bits of random created by means of FCS_RNG.1,
- A digital signature over the rest of the attestation data.

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 separated from other communication channels*[80] and provides assured identification of its end points *FIA_API.1/PACE, FIA_UAU.5.1 (2), FIA_API.1/CA, FIA_UAU.5.1 (4) or (5), and (6)*[81] and protection of the channel data from modification or disclosure *modification, disclosure*[82] as required by *FCS_COP.1/TCM, FCS_COP.1/TCE*[83].

FTP_ITC.1.2 The TSF shall permit the remote trusted IT product 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).

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 agreement algorithm PACE with *brainpoolP256r1*[84] and Generic Mapping in ICC role and specified cryptographic key sizes *256 bit*[85] that meet the following: ICAO Doc9303, Part 11, section 4.4 [ICAO Doc9303].

[79] [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]]

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

[81] [selection: Authentication of the TOE and remote entity according to the case in table 4]

[82] [assignment: according to the case in table 4]

[83] [selection: cryptographic operation according to the case in table 4]

[84] [selection: elliptic curves in table 2]

[85] [selection: 128 bits, 192 bits, 256 bits]

PP Application note 24: 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.

Consideration of PP Application Note 24: The application note does not require any action in this ST.

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 agreement algorithms Terminal Authentication version 2 and Chip Authentication Version 2 and specified cryptographic key sizes *256 bits*[86]that meet the following: BSI TR-03110 [TR-03110], section 3.3 and 3.4.

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 in accordance with a specified cryptographic algorithm AES in *CBC[NIST-SP800-38A]*[87] mode and cryptographic key sizes *256 bits*[88]that meet the following: [FIPS197].

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 in accordance with a specified cryptographic algorithm AES *CMAC[NIST-SP800-38B]*[89]and cryptographic key sizes *256 bits*[90] that meet the following: [FIPS197].

10.1.6 User identification and authentication

FIA_ATD.1 User attribute definition – Identity based authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

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

(1) Identity,
(2) Authentication reference data,
(3) Role.

---

[86] [selection: 128 bits, 192 bits, 256 bits]

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

[88] [selection: 128 bits, 192 bits, 256 bits]

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

[90] [selection: 128 bits, 192 bits, 256 bits]

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

(1) create the initial Authentication reference data of all authorized users to *Administrator*[91],

(2) delete the Authentication reference data of an authorized user to *Administrator*[92],

(3) modify the Authentication reference data to the corresponding authorized user.

(4) create the permanently stored session key of a trusted channel as Authentication reference data to *Administrator*[93]

(5) define the time in range *of 10 minutes to 24 hours*[94] after which the user security attribute Role of the authentication data record is reset according to FMT_SAE.1 to *Administrator*[95],

(6) define the value *Unauthenticated user*[96] to which the security attribute Role of the authentication data record shall be reset according to FMT_SAE.1 to *Administrator*[97].

PP Application note 25: 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.

Consideration of PP Application Note 25: The application note is considered in this ST.

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 by enforcing a change of initial passwords to a different operational password on the first successful authentication of the user.

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *5*[98] unsuccessful authentication attempts occur related to *Administrator authentication*[99].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been surpassed[100], the TSF shall *delay the next authentication attempt for 1 minute*[101].

---

[91] [selection: Administrator, User Administrator]

[92] [selection: Administrator, User Administrator]

[93] [selection: Administrator, User Administrator]

[94] [assignment: time frame]

[95] [selection: Administrator, User Administrator]

[96] [selection: Unidentified user, Unauthenticated user]

[97] [selection: Administrator, User Administrator]

[98] [selection: [assignment: positive integer number], an [selection: Administrator, User Administrator] configurable positive integer within [assignment: range of acceptable values]]

[99] [assignment: list of authentication events]

[100] [selection: met, surpassed]

[101] [assignment: list of actions]

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

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

(1) Identity,

(2) Role.

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

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

(1) 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.

FMT_SAE.1 Time-limited authorisation

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FPT_STM.1 Reliable time stamps

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for a Role to *Administrator*[102].

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), after the expiration time for the indicated security attribute has passed.

PP Application note 26: 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. If the security target requires FPT_STM.1 (e.g. if the PP-module "Time Stamp and Audit" claimed), this time stamp shall be used to meet FMT_SAE.1.

Consideration of PP Application Note 26: The application note is considered in this ST.

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) *self attestation*[103]

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 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

[102] [selection: Administrator, User Administrator]

[103] [assignment: list of other TSF-mediated actions]

(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 role*[104] for authentication,

(4) *self attestation*[105]

on behalf of the user.

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.

PP Application note 27: Clause (2) and (3) in FIA_UAU.1.1 allows mutual identification for mutual authentication, e. g. by exchange of certificates.

Consideration of PP Application Note 27: The application note does not require any action in this ST.

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

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,

(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) *password authentication shall be used for authentication of the application control*[106].

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,

[104] [selection: a role, a set of role]

[105] [assignment: list of other TSF mediated actions]

[106] [assignment: additional rules]

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

(4) *the PACE channel is automatically terminated after 24 hours*[107].

10.1.7 Access control

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

Hierarchical to: No other components.

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

FDP_ITC.2.1/UD The TSF shall enforce the Cryptographic Operation SFP 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.

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.

PP Application note 28: Keys to be used for the cryptographic operation of the imported user data are identified by security attribute Key identity.

Consideration of PP Application Note 28: The application note does not require any action in this ST.

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 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,

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

(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.

PP Application note 29: 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.

Consideration of PP Application Note 29: The application note is considered in this ST.

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 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 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 on

(1) subjects: *Administrator*[108], Key Owner, *Application Component*[109];

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

(3) operations: cryptographic operation

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 to objects based on the following:

(1) subjects: subjects with security attribute Role *Administrator*[110], Key Owner, *Application Component*[111];

(2) objects:

(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.

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*[112] 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) *none*[113].

---

[108] [selection: Administrator, Crypto-Officer]

[109] [assignment: other roles]

[110] [selection: Administrator, Crypto-Officer]

[111] [assignment: other roles]

[112] [selection: Administrator, Crypto-Officer]

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

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 5 **of this ST**.

(2) *subjects in the role of Administrator are allowed to perform an attestation function as defined in FDP_DAU.2.1/Att using the corresponding private key of a user* [114].

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) *none*[115].

Access control rules for cryptographic operation:

Security attribute Role of the subject	**Security attribute of the cryptographic key**	**Cryptographic operation referenced by SFR allowed for the subject on user data with the cryptographic key**
Administrator[116]	Key type: symmetric Key usage type: Key wrap Key validity time period:	FCS_COP.1/KW
Administrator[117]	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	FCS_COP.1/HDM FCS_CKM.5/AES_RSA
(any authenticated user)	**Key type: public** **Key usage type: encryption** **Key validity time period: as in certificate**	**FCS_COP.1/HEM** **FCS_CKM.1/ECC**

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

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

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

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

Key Owner	**Key type: private** **Key usage type: encryption** **Key validity time period: as in certificate**	**FCS_COP.1/HDM** **FCS_CKM.5/ECDHE**
Key Owner	Key type: private Key usage type: DS-ECDSA Key validity time period:	FCS_COP.1/CDS-ECDSA
(any authenticated user)	Key type: public Key usage type: DS-ECDSA Key validity time period:	FCS_COP.1/VDS-ECDSA
Key Owner	Key type: private Key usage type: DS-RSA Key validity time period:	FCS_COP.1/CDS-RSA
(any authenticated user)	Key type: public Key usage type: DS-RSA Key validity time period:	FCS_COP.1/VDS-RSA

Table 5: Security attributes and access control

ST application note 6: The assignments 111, 112 and 113 are set to *none* to avoid writing trivial rules, since there are none other needed.

ST application note 7: Table 5 is extended because no acces control rules are defined for the case that FCS_CKM.5/ECDHE is chosen in FCS_COP.1/HEM and FCS_COP.1/HDM

10.1.8 Security Management

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

(1) management of security functions behaviour (FMT_MOF.1),

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

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

(4) *manual export of user data from Master-CSP and import to Slave-CSP by the Administrator*[118].

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*[119], *no other roles*[120].

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

PP Application note 30: The ST may select the general role Administrator or more detailed administrator roles as supported by the TOE.

Consideration of PP Application Note 30: The application note is considered in this ST.

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

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

[120] [selection: [assignment: other roles], no other roles]

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) *Key usage counter*[121].

The cryptographic keys shall have

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

ST application note 8: The security attribute "Key usage counter" is a number which shall not be decremented.

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 the functions password authentication according to FIA_UAU.5.1, clause (1) to *Administrator*[122].
(2) disable the functions password authentication according to FIA_UAU.5.1, clause (1) to *Administrator*[123],
(3) determine the behavior of the functions trusted channel according to FDP_ITC.1.2 by defining the remote trusted IT products permitted to initiate communication via the trusted channel to *Administrator*[124],
(4) determine the behavior of the functions trusted channel according to FDP_ITC.1.3 by defining the entities for which the TSF shall enforce communication via the trusted channel to *Administrator*[125].

Application note 31: The refinements of FMT_MOF.1.1 in bullets (2) to (4) are made in order to avoid iteration of the component. In case of 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).

Consideration of PP Application Note 31: The application note is considered in this ST.

ST application note 9: The clauses 1 and 2 permit the administrator to enable and disable password authentication for other users who don't belong to the role administrator. If password authentication is disabled for a user, that user cannot authenticate itself at the TSF which means the users account cannot access any functions offered by the TSFIs which require authentication.

[121] [assignment: additional security attributes]

[122] [selection: Administrator, User Administrator]

[123] [selection: Administrator, User Administrator]

[124] [selection: Administrator, User Administrator]

[125] [selection: Administrator, User Administrator]

10.1.9 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*[126].

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 to demonstrate the correct operation of *integral parts of the TOE:*

- *execute a basic test of its security functionality,*
- *verify the integrity of its TSF data and*
- *verify the integrity of its executables*[127].

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

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

ST application note 10: Additionally to power-on and initial startup the self test is a function offered by the TSFI which does not require any authentication (FIA_UID.1).

10.1.10 Import and verification of Update Code Package

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

Hierarchical to: No other components.

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

FDP_ITC.2.1/UCP The TSF shall enforce the Update SFP 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.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

---

[126] [assignment: list of types of additional failures]

[127] [assignment: parts of TSF]

FPT_TDC.1.1/UCP The TSF shall provide the capability to consistently interpret security attributes Issuer and Version Number 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 in accordance with a specified cryptographic algorithm *SHA256withPLAIN-ECDSA (brainpoolP256r1)*[128] and cryptographic key sizes *256 bit*[129] that meet the following: *[RFC5639]*[130].

Application note 32: 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

Consideration of PP Application Note 32: The application note does not require any action in this ST.

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 in accordance with a specified cryptographic algorithm *SHA256withPLAIN-ECDSA (brainpoolP256r1) plus AES256*[131] and cryptographic key sizes *256 bit*[132] that meet the following: *[RFC5639], [FIPS197]*[133].

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 on

(1) subjects: *Administrator*[134];

(2) objects: Update Code Package;

(3) operations: import, store.

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

Hierarchical to: No other components.

---

[128] [assignment: cryptographic algorithm]

[129] [assignment: cryptographic key sizes]

[130] [assignment: list of standards]

[131] [assignment: cryptographic algorithm]

[132] [assignment: cryptographic key sizes]

[133] [assignment: list of standards]

[134] [selection: Administrator, Update Agent]

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 to objects based on the following:

(1) subjects: *Administrator*[135];

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

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*[136] is allowed to import Update Code Package according to FDP_ITC.2/UCP.

(2) *Administrator*[137] 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.

FDP_ACF.1.3/UCP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[138].

FDP_ACF.1.4/UCP The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*[139].

FDP_RIP.1/UCP Subset residual information protection

Hierarchical to: No other components

Dependencies: No dependencies.

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

10.2 Additional Security functional requirements by [PPC-CSP-LIGHT-TS-AU]

10.2.1 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)

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*[140] 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 *Key Owner, Auditor Manager*[141] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

---

[135] [selection: Administrator, Update Agent]

[136] [selection: Administrator, Update Agent]

[137] [selection: Administrator, Update Agent]

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

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

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

[141] [assignment: list of subjects]

PP TS-Au Application note 1: The TSF according to FDP_DAU.2/TS is intended for time stamp service of the TOE for any provided user data and exported audit records. The user data source shall select the security attribute Key usage type "TimeStamp" of the signature key of the time stamp service. The signature key of exported audit records shall be defined according to FMT_MOF.1.1/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].

Consideration of PP TS-Au Application Note 1: The application note does not require any action in this ST.

10.2.2 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 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.

PP TS-Au Application note 2: Keys to be used for the cryptographic operation of the imported user data are identified by security attribute Key identity.

Consideration of PP TS-Au Application Note 2: The application note does not require any action in this ST.

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]

FDP_ETC.2.1/TS The TSF shall enforce the Cryptographic Operation SFP 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.

Application note 3: 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.

Consideration of PP TS-Au Application Note 3: The application note does not require any action in this ST.

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 to objects based on the following:

(1) subjects: subjects with security attribute Role Application Component, *no other roles*[142],

(2) objects: user data.

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, *no other roles*[143] is allowed to perform cryptographic operation according to FDP_DAU.2/TS on user data with cryptographic keys with Key usage type TimeStamp.

(2) *none*[144].

FDP_ACF.1.3/TS The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[145].

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) *none*[146].

10.2.3 Security Management

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.

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 Manager, Audit Log Receiver*** *and Timekeeper*[147].

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

PP TS-Au Application note 4: The ST may select the general role Administrator or more detailed Administrator roles as supported by the TOE. The ST may select

– Auditor role in FMT_SMR.1/TSA separated from Administrator roles selected in the SFR FMT_SMR.1 according to the Base-PP and, or

– Timekeeper role in FMT_SMR.1/TSA separated from Administrator roles selected in the SFR FMT_SMR.1 according to the Base-PP and, or

– no other roles in FMT_SMR.1/TSA and assign the management of audit TSF in FMT_MTD.1/Audit to a selected Administrator role in the SFR FMT_SMR.1 according to the Base-PP.

The assignment of security management of audit and other functions must not result in a conflict of duties

[142] [assignment: other roles]

[143] [assignment: other roles]

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

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

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

[147] [selection: Auditor, Timekeeper, no other roles]

Consideration of PP TS-Au Application Note 4: In this ST the role Auditor is split into two roles Auditor Manager and Audit Log Receiver. The Auditor Manager is responsible for configuration of the audit data and can read system audit logs. The Audit Log Receiver can only read audit logs associated to their own keys.

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 the functions adjustment of the internal clock according to FPT_STM.1 clause (1) to *Timekeeper*[148],

(2) modify the behaviour of the functions adjustment of the internal clock according to FPT_STM.1 clause (2) to *Timekeeper*[149],

(3) determine the behaviour of and modify the behaviour of the functions select the auditable events according to FAU_GEN.1 to ***Auditor Manager***[150],

(4) determine the behaviour of and modify the behaviour of the functions automatic export of audit trails according to FAU_STG.3.1 clause (1) to ***Auditor Manager***[151],

(5) determine the behaviour of and modify the behaviour of the functions FDP_DAU.2/TS by selection of signature key used to sign exported audit trails to *Administrator*[152].

PP TS-Au Application note 5: 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

Consideration of PP TS-Au Application Note 5: The application note does not require any action in this ST.

ST application note 11: Clause 2 is set to the Timekeeper but since the referenced clause is not selected in this ST the functionality does not exist. Clause 4 is set to Auditor Manager but since automatic export of audit records is not enabled in this ST according to the PP application note this functionality does not exist.

10.2.4 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 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),

[148] [selection: Administrator, Timekeeper]

[149] [selection: Administrator, Timekeeper]

[150] [selection: Administrator, Auditor]

[151] [selection: Administrator, Auditor]

[152] [selection: Administrator, Auditor]

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

(10) No other event[153],

(11) Generation of client key with security attribute key usage counter,

(12) Destruction of client key with security attribute key usage counter,

(13) Other signature application of client key with security attribute key usage counter[154]*.*

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*[155].

PP TS-Au Application note 6: 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 this PP-Module.

Consideration of PP TS-Au Application Note 6: The application note does not require any action in this ST.

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 **the audit records to Auditor Manager and Audit Log Receiver**[156],

(2) clear after manual export **the audit records to Auditor Manager and Audit Log Receiver**[157],

(3) select audited events in FAU_GEN.1 **the audit records to Auditor Manager**[158],

(4) define the number of audit records causing automatic export and clearing of exported audit records according to FAU_STG.3.1 clause (1) **the audit records to none**[159],

(5) define the percentage of storage capacity of audit records if actions are assigned in FAU_STG.3.1 clause (2) **the audit records to none**[160]**.**

~~the audit records to [selection: Auditor, Administrator]~~[161].

PP TS-Au Application note 7: 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

---

[153] [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]

[154] [assignment: additional specifically defined auditable events]

[155] [assignment: other audit relevant information]

[156] [refinement]

[157] [refinement]

[158] [refinement]

[159] [refinement]

[160] [refinement]

[161][refinement]

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).

Consideration of PP TS-Au Application Note 7: The application note is considered in this ST.

ST application note 12: The selection in the PP was replaced by 5 refinements since the role Auditor is split into two roles in this ST as described in FMT_SMR.1/TSA. The referenced functions in clauses 4 and 5 are not enabled in accordance to the PP.

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 unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.3 Action in Case of Possible Audit Data Loss

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall

(1) automatically export audit trails and clear automatically exported audit records if the audit trail exceeds an ***Auditor Manager***[162] defined number of audit records within *500000-500000*[163]

(2) *no actions*[164] if the audit trail exceeds an ***Auditor Manager***[165] settable percentage of storage capacity.

PP TS-Au Application note 8: The ST writer shall perform the open operations in FAU_STG.3.1 element. If the number of audit records in clause (1) is set to 1 then the TSF export each audit record automatically. If the number of audit records in clause (1) is set higher than maximum number of audit records in the audit trail then the TSF does not export audit records automatically. The assignment of clause (2) may be "no actions" if an appropriate number of audit records is assigned in clause (1).

Consideration of PP TS-Au Application Note 8: The maximum number of audit records is 499999 which means the TSF does not export audit records automatically.

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

(1) internal clock with accuracy of 1700 ms maximum deviation per day[166] *with the ability of adjustment of the clock by the Timekeeper*[167]*.*[168]

---

[162] [selection: Administrator, Auditor]

[163] [assignment: pre-defined range]

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

[165] [selection: Administrator, Auditor]

[166] [assignment: approximate deviation]

[167] [selection: Administrator, Timekeeper]

[168] [selection:

(1) internal clock with accuracy [assignment: approximate deviation] with the ability of adjustment of the clock by the [selection: Administrator, Timekeeper],

(2) internal clock with accuracy [assignment: approximate deviation] 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 [selection: Administrator, Timekeeper]

PP TS-Au Application note 9: 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.

Consideration of PP TS-Au Application Note 9: The application note is considered in this ST.

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, *Key Management SFP*[169] to transmit TSF data audit records in a manner protected from modification, deletion, insertion and replay errors.

FPT_TIT.1.2/Audit The TSF shall be able to determine on receipt of TSF data time, whether modification has occurred.

PP TS-Au Application note 10: 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.

Consideration of PP TS-Au Application Note 10: The application note is considered in this ST.

10.3 Additional Security functional requirements by [PPC-CSP-LIGHT-TS-AU-CL]

10.3.1 Clustering

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 on

(1) subjects: Administrator;

(2) objects: cluster keys, Authentication Data Records, cryptographic keys;

(3) operations: generation, export, import.

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 the cluster keys to Administrator,

[169] [selection: Key Management SFP, Cryptographic Operation SFP]

(2) export from the Master-CSP according to FPT_ESA.1/CL, FPT_TCT.1/CL and FPT_TIT.1/CL the Authentication Data Records to *Application Component, Administrator*[170],

(3) import into Slave-CSP according to FPT_ISA.1/CL, FPT_TCT.1/CL and FPT_TIT.1/CL the Authentication Data Records to *Application Component, Administrator*[171]

(4) export from the Master-CSP according to FPT_ESA.1/CL, FPT_TCT.1/CL and FPT_TIT.1/CL the cryptographic keys to *Application Component, Administrator*[172],

(5) import into Slave-CSP according to FPT_ISA.1/CL, FPT_TCT.1/CL and FPT_TIT.1/CL the cryptographic keys to *Application Component, Administrator*[173].

PP TS-Au-Cl Application note 1: 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.

Consideration of PP TS-Au-Cl Application Note 1: The application note does not require any action in this ST.

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 from an agreed shared secret in accordance with a specified cryptographic key derivation algorithm anonymous Diffie-Hellman Key Agreement for ECC key pair generation with *Curve P-384*[174] and specified cryptographic key sizes *384 bits*[175] that meet the following: *FIPS PUB 186-4 B.4 and D.1.2.4 [FIPS PUB 186-4]*[176].

PP TS-Au-Cl Application note 2: The cryptographic cluster keys shall be used for encryption according to FCS_COP.1/ED (cf. Base-PP) 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. The tables 2 and 3 are defined in the Base-PP [PP CSPLight].

Consideration of PP TS-Au-Cl Application Note 2: The application note is considered in this ST.

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 informationflow 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 by providing the ability to transmit and receive Authentication Data Records and cryptographic keys in a manner protected from unauthorised disclosure according to FCS_COP.1/ED.

PP TS-Au-Cl Application note 3: FCS_COP.1/ED is defined in the Base-PP.

Consideration of PP TS-Au-Cl Application Note 3: The application note does not require any action in this ST.

---

[170] [selection: Application Component, Administrator, User Administrator]

[171] [selection: Application Component, Administrator, User Administrator]

[172] [selection: Application Component, Administrator, Crypto-Officer]

[173] [selection: Application Component, Administrator, Crypto-Officer]

[174] [selection: elliptic curves in the table 2 [PP CSPLight]]

[175] [selection: key size in the table 2 [PP CSPLight]]

[176] [selection: standards in the tables 2 and 3 [[PP CSPLight], [TR-03111]]

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 informationflow 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 to transmit and receive Authentication Data Records and cryptographic keys in a manner protected from modification 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, whether modification has occurred according to FCS_COP.1/MAC.

PP TS-Au-Cl Application note 4: FCS_COP.1/MAC is defined in the Base-PP.

Consideration of PP TS-Au-Cl Application Note 4: The application note does not require any action in this ST.

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 informationflow 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 when importing Authentication Data Records and cryptographic keys, controlled under the SFP, from 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.

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 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 is as intended by the source of the Authentication Data Records and cryptographic keys.

FPT_ISA.1.5/CL The TSF in role Slave-CSPLight shall enforce the following rules when importing Authentication Data Records and cryptographic keys controlled under the SFP from 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.

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

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset informationflow 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 when exporting Authentication Data Records and cryptographic keys, controlled under the SFP(s), to Slave-CSPLight.

FPT_ESA.1.2/CL The TSF in role Master-CSPLight shall export the Authentication Data Records and cryptographic keys 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 to Slave-CSPLight, are unambiguously associated with the exported Authentication Data Records and cryptographic keys.

FPT_ESA.1.4/CL The TSF in role Master-CSPLight shall enforce the following rules when Authentication Data Records and cryptographic keys is exported 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.

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 when shared between the TSF and TOE sample in the cluster.

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,

when interpreting the Authentication Data Records and cryptographic keys from Master-CSPLight.

10.3.2 Security audit

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 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,

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

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*[177].

PP TS-Au-Cl Application note 5: 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.

PP TS-Au-Cl Application note 6: FMT_MTD.1/RAD is defined in the Base-PP.

Consideration of PP TS-Au-Cl Application Note 5 and 6: The application notes do not require any action in this ST.

[177] [assignment: other audit relevant information]

10.4 Security assurance requirements

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.

10.5 Security requirements rationale

This chapter is equivalent to the corresponding chapter in [PP-CSP-LIGHT], because no additional SFRs were introduced in this Security Target, which were not already present in the Protection Profile.

10.5.1 Dependency rationale

This chapter is equivalent to the corresponding chapters in [PP-CSP-LIGHT], [PPC-CSP-LIGHT-TS-AU] and [PPC-CSP-LIGHT-TS-AU-CL], because no additional SFRs were introduced in this Security Target, which were not already present in the Protection Profile.

10.5.2 Security functional requirements rationale

This chapter is equivalent to the corresponding chapters in [PP-CSP-LIGHT], [PPC-CSP-LIGHT-TS-AU] and [PPC-CSP-LIGHT-TS-AU-CL], because no additional SFRs were introduced in this Security Target, which were not already present in the Protection Profile.

10.5.3 Security assurance requirements rationale

This chapter is equivalent to the corresponding chapter in [PP-CSP-LIGHT].

11. TOE Summary Specification

11.1 Self Testing and Integrity Protection

The TOE implements Self Testing as required by [PP-CSP-LIGHT] and integrity protection as required by [PPC-CSP-LIGHT-TS-AU]. During the self test, the TOE

1. executes a basic test of its security functionality in the form of cryptographic test vectors,
2. verifies the integrity of its TSF data consisting of account data, key data, audit record data (e.g. FAU_STG.1, FAU_STG.3). TSF data is stored in ASN.1 structures within flat files in the environment. The verification of integrity includes:
    a. The verification of the integrity of each user account
    b. The verification of the integrity of each key of an ERS and each system key
    c. The verification of all audit logs that are only stored for the CSP-L
    d. The verification of all audit logs that have been created for a user key (as long as the audit log has not yet been retrieved by the user and deleted on the TOE)

    The verification of the integrity is based on a MAC.
3. and verifies the integrity of its executables.

The test of security functionality consists of tests regarding cryptographic functionality of the TOE. To do that known test vectors are used as follows:

1. To test SHA-256, SHA-384 and SHA-512 three test vectors each, taken from the files SHA256ShortMsg.rsp, SHA384ShortMsg.rsp and SHA512ShortMsg.rsp contained in the download from https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/shs/shabytetestvectors.zip, are used,
2. To test AES-CBC 3 test vectors each, taken from the files CBCVarTxt256.rsp, CBCVarKey256.rsp, CBCVarTxt128.rsp and CBCVarKey128.rsp contained in the download from https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/aes/KAT_AES.zip, are used,
3. To test AES-CMAC three test vectors each, taken from the files CMACGenAES128, CMACVerAES128, CMACGenAES256 and CMACVerAES256, contained in the download from https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/mac/cmactestvectors.zip, are used,
4. To test HMAC three test vectors taken from the file HMAC.rsp contained in the download from https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/mac/hmactestvectors.zip are used,
5. To test KeyWrap and KeyUnwrap three test vectors each, taken from the files KWP_AD_128.txt, KWP_AE_128.txt, KWP_AD_256.txt and KWP_AE_256.txt contained in the download from https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/mac/kwtestvectors.zip, are used,
6. To test ECDSA signature creation three test vectors, taken from the file SigGenComponent.txt contained in the download from https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/components/186-3ecdsasiggencomponenttestvectors.zip, are used,
7. To test RSA signature creation three test vectors, taken from the file SigGenPSS_186-3.txt containe din the download from https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/dss/186-3rsatestvectors.zip, are used,
8. To test the Random Number Generator three test vectors, taken from the file drbgtestvectors_no_reseed/Hash_DRBG.rsp contained in the download from https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/drbg/drbgtestvectors.zip, are used.

If the self test fails, the TOE will enter a secure state. This means that no function can be executed except the function to perform the self test again (FPT_FLS.1) and the configuration function of the Administration interface, which is restricted to the administrator user only. The self test will be executed at the start of the TOE software; this is performed at power on or reset of the TOE (FPT_TST.1.1). The only way to exit the secure state is a successful self test.

After multiple failed self test it is the administrator's responsibility to decide whether the TOE can be returned into a working state by changing configuration data or has to be put out of operation.

In addition, the TOE provides a function that allows to invoke this self test functionality via its API (FPT_TST.1.2, FPT_TST.1.3).

The TOE provides an API function to generate evidence attestation data (FDP_DAU.2.1/Att, FCS_COP.1/CDS-ECDSA). The attestation data is built up by Client input data, the product identifier ("D-TRUST CSP Web Dienst TSE CSP"), software version, CC-certification ID, CSP-ID, the current timestamp and 256 bits of random (FCS_RNG.1), signed by means of the attestation key of the TOE.

For verification of the TOE evidence attestation data, the TOE provides an API function (FDP_DAU.2.2/Att, FCS_COP.1/VDS-ECDSA).

11.2 User Identification and Authentication

A major part of the security management of the TOE is the user identification and authentication (FMT_SMF.1, FMT_SMF.1/TSA). For each user the TOE maintains the security attributes Identity, Authentication Reference Data and Role (FIA_ATD.1).

The authentication concept of the TOE is based on the following roles the TOE maintains (FMT_SMR.1, FMT_SMR.1/TSA):

Role	**Description**	**Used for and used by**
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. Only actions allowed for the Unidentified User are permitted (FIA_UID.1). [PP-CSP-LIGHT]	- Operations at the Client interface of the TOE to start and continue the establishment of the Trusted Channel by PACE protocol [TR-03111] triggered by the CRE in PCD role (FIA_UAU.5 (2)). - Start of the TOE self-test and attestation data generation at the administration interface
Unauthenticated User	This role is associated with an identified user but not (successfully) authenticated user. Only actions allowed for the Unauthenticated User are permitted (FIA_UAU.1). [PP-CSP-LIGHT]	- Operation to continue und finalize the establishment of the Trusted Channel by PACE protocol [TR-03111] triggered by the CRE in PCD role before the CRE has authenticated as Key Owner.
Administrator	Successful authenticated user in this role is allowed to access the TOE in order to perform management functions. It is taken by a human user or a subject acting on behalf of a human user after successful authentication as an Administrator. [PP-CSP-LIGHT]	- All operations at the administration interface of the TOE by the Administrator user via the Management.
Auditor Manager	Successful authenticated user in this role is allowed to configure audit log functionality generated by the TOE and receive the audit logs for the TOE. (FMT_SMR.1/TSA)	- Configuration of the audit log functionality. - Receiving and exporting audit logs generated for the Auditor Manager. - The Management module is used to configure and receive audit logs
Audit Log Receiver	Successful authenticated user in this role is allowed to receive the audit logs generated by the TOE. (FMT_SMR.1/TSA)	- Receiving audit logs generated for the CRE.
Timekeeper	Successful authenticated user in the role is allowed to adjust the internal time. [PP-CSP-LIGHT-TS-AU]	- Adjusting the internal time.

Key Owner	Successful authenticated user allowed to perform cryptographic operation with his own keys. This role is claimed by the CRE. [PP-CSP-LIGHT]	- Key management operations at the Administration interface (key creation, key removal) operating only on the client key the requestor is the owner of. - All operations at the Client interface of the TOE transmitting Trusted Channel data over an established PACE channel. The CRE is the requestor as client acting as key owner authenticated by PACE authentication procedure [TR-03111]. - The signature key usage counter synchronization, signing key export and import operations requested by the Control Application acting on behalf of the key owner during the signing operation.
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 physically separated secure channel. [PP-CSP-LIGHT]	- All operations at the Client interface of the TOE requested by the Control Application for forwarding encrypted Trusted Channel data from and to the CRE and for providing CSP control data (meta data) for addressing the CRE Account by the key reference.

Table 6: user role definition

The TOEs authentication concept knows the following users and their associated user role:

User	**User attributes FIA_ATD.1**		
	Identity	**Role**	**Authentication Reference Data**
Administrator	admin	Administrator, Key Owner, Timekeeper	Password
Zeit-Administrator	time	Timekeeper	Password
Auditor	audit	Auditor Manager	Password
Client	<userId>	Key Owner, Audit Log Receiver	Password (PACE-Password)
Application Component	application	Application Component	Password

Table 7: user attributes

Within the CSP, each single user is associated to one or more roles (FIA_USB.1, FIA_UAU.6 (1)). After authentication a user inherits the permissions of the roles he's associated to.

The Administrator user, acting as human user, logs into the TOE via the application component *Management module* (see Figure 1) by means of password authentication (FIA_UAU.5.1 (1)). After TOE initialization (see 2.4a), the TOE holds an initial password for the Administrator user, which has to be changed to a different operational password on the first successful authentication of the Administrator user (FMT_MTD.3).

After five unsuccessful authentication attempts of the Administrator user in sequence are surpassed, the TSF delays the next authentication attempt for 1 minute (FIA_AFL.1).

An authenticated user has to re-authenticate after start or restart of the TOE, happened at power on or hardware reset (FIA_UAU.6).

11.3 Access Control

The TOE enforces the access control policy as required by [PP-CSP-LIGHT]. The TOE will allow access to its functions only for authenticated and authorised users based on their role (FMT_SAE.1).

The key management including their security attributes is restricted to the Administrator user holding the Administrator role (FDP_ACC.1/KM, FMT_MSA.1/KM, FDP_ACC.1/Oper). The access to cryptographic operations is controlled by the security attribute of the cryptographic key and the user role (FDP_ACF.1/Oper).

The Auditor Manager role is able to configure the behaviour of auditable events (FMT_MOF.1.1/TSA) and to export and clear after export the audit record (FMT_MTD.1). The Audit Log Receiver role is only able to export and clear after export the audit records for the CRE (FMT_MTD.1).

The generation of the TOE system master keys during the TOE initialization (FMT_MTD.1/RK), the import and export of the key owners signing keys (FMT_MTD.1/KM, FPT_ESA.1/CK) and the import and deletion of root key certificates (FMT_MTD.1/RK) is restricted to the Administrator user. The import and export of the key owners signing keys during the CSP Failover procedure is also allowed for the Application Component.

The cluster management (e.g. adding, changing and removing of CSP Light Modules, relocation of CRE Accounts including the key owners signing keys) is restricted to the Administrator user and Application Component (FDP_ACC.1/CL, FMT_MTD.1/CL).

The user management is restricted to the Administrator user (FMT_MTD.1/RAD).

The audit functions are restricted to the the Auditor Manager user (FMT_MTD.1/Audit).

Functions regarding the internal clock are restricted to the Timekeeper User (FMT_MOF.1/TSA).

The UCP operation at the TOE API is restricted to the Administrator user holding the Administrator role (FDP_ACC.1/UCP, FDP_ACF.1/UCP).

The start of the self test (FPT_TST.1) is only accessible for authorised users (FPT_TST.1.2/ FPT_TST.1.3). According FIA_UID.1 this includes the Unidentified User.

11.4 Trusted Channel

For the communication of the CRE with the TOE the TOE only allows trusted channel functionality in ICC role (FIA_API.1.1/PACE). Caused by the client-server architecture the CRE belongs to the entities for which the TOE enforces communication by a Trusted Channel (FTP_ITC.1, FMT_MOF.1.1 (4)).

The Trusted Channel functionality includes

1. permitting the CRE to act as remote trusted IT product which initiates the trusted channel communication by means of the API operations establishTrustedChannel, continueTrustedChannel (FTP_ITC.1, FMT_MOF.1.1 (3)),
2. processing the PACE protocol by continueTrustedChannel API function with the CRE (FCS_CKM.5/ECC, FCS_CKM.1/PACE, FCS_CKM.1/AES),
3. mutual authentication of the communicating entities (FIA_API.1/PACE, FIA_API.1/CA), to assure identification of its end points according to FTP_ITC.1.1 (see PP Table 4: "Operation in SFR for trusted channel") based on the selection in FTP_ITC.1.1 in Table 4 [PP-CSP-LIGHT] by means of
   a. Generic Mapping (FIA_UAU.5.1 (2), FIA_UAU.5.2 (3))
   b. Chip Authentication Version 2 (FIA_API1.1/CA, FIA_UAU.5.1 (5), (6), FCS_CKM.1/TCAP)
   c. Terminal Authentication Version 2 (FIA_API.1/CA, FIA_UAU.5.1 (4), (6), FCS_CKM.1/TCAP)
4. encryption of the sent data (FCS_COP.1/TCE, FCS_CKM.1/PACE),
5. message authentication proof of the sent data (FCS_COP.1/TCM, FCS_CKM.1/PACE,FCS_CKM.5/ECC, FCS_COP.1/MAC),
6. decryption of received data (FCS_COP.1/TCE) and
7. message authentication verification of the received data (FCS_COP.1/TCM, FCS_CKM.5/ECC).

11.5 Log Message creation and verification

The TOE generates Transaction Log Message on request of the CRE by means of the signData API function for a particular CRE Account (holding the key owners signing key) referenced by the key reference as key identifier (FDP_ITC.2/UD (4), FDP_ITC.2/TS). In order to calculate the hash of the data to be signed (the processdata) the TOE supports two different modes:

1) The hash is completely calculated by the TOE based on the submitted processdata
2) Only the last round of the hash function is performed by the TOE (lastRoundOnCSPL). In this case, the TOE expects the internal state of a hash function and the last block instead of the whole processdata.

The data elements (processdata, transaction counter, a.o.) received from the CRE are augmented with the signing time stamp (see 11.6), *serialnumber* of the signing key and the new value of the key usage counter (signature counter). Then a transaction log message according to the ASN.1 structure defined in [TR-03151] chapter 10 is build. The signature value (over all other Log Message data elements) is created (FDP_DAU.2.1/Sig, FCS_COP.1/CDS-ECDSA) and the Log Message is returned (exported) to the requesting CRE (FDP_ETC.2, FDP_ETC.2/TS).

The TOE provides a Log Message verification service to calling applications the caller is able to verify the validity of a provided Log Message (Transaction, Audit) together with the Certificate of the respective CRE Account (FDP_DAU.2.2/Sig, FDP_DAU.2.2/TS, FCS_COP.1/VDS-ECDSA).

11.6 Timestamp and Audit

The TOE supports a time stamp service through cryptographic protected time stamps (FDP_DAU.2.1/TS) by means of signature creation (FCS_COP.1/CDS-ECDSA). By means of the time stamp service the exported Transaction Log Messages, System Log Messages and Audit Log Messages are time stamped and integrity protected (FPT_TIT.1/Audit, FDP_DAU.2/Sig). For the time stamp source, the hardware system internal clock with appropriate accuracy is used (FPT_STM.1). The TOE internal clock is periodically adjusted based on an external NTP-sourced real time service within the Trustcenter via the updateTime function at the TOE API. This operation is restricted to the Timekeeper user (FDP_ACF.1/TS, FMT_MOF.1/TSA).

The TOE generates audit records of auditable events (FAU_GEN.1, FAU_GEN.1/CL).

CRE Account specific audit records are requested by the CRE periodically and returned by the TOE as signed Audit Log Messages. These events are: clock adjustment (FAU_GEN.1.1 c)), start-up of the TOE (FAU_GEN.1.1 d(1)), import of UCP (FAU_GEN.1.1 d(2)), key owner signature key generation (FAU_GEN.1.1 d(11)) and import caused by CRE Account relocation or fail-over caused by CSP break down (FAU_GEN.1.1/CL c) (3)), key owner signature key export (FAU_GEN.1.1/CL c) (2)) and destruction in the TOE (FAU_GEN.1.1 d(12)). The signature of these kind of Audit Log Messages is created by means of the CRE Account specific signature key (key owner signing key).

System wide audit events (i.e. authentication failures (FAU_GEN.1.1 d(3)), start up and shutdown of the audit service (at system start-up and shutdown) (FAU_GEN.1.1 a)) are also returned by the TOE as signed Audit Log Messages (signed by the CRE Account specific signature key) and in addition are provided to the Auditor user (in Auditor Manager role) on request. The Audit Log Messages exported to the Auditor user are created by means of the TOE internal System-AuditLog Signaturekey.

11.7 Management of Certificates

The TOE provides functionality for Certificate Management:

1. import and deletion of a known as authentic certificate of the root CA (FMT_MTD.1/RK, FPT_TIT.1/Cert),
2. import and deletion of certificates issued by the trusted root CA (FPT_TIT.1/Cert, FPT_ISA.1/Cert, FPT_TDC.1/Cert).

11.8 Cryptographic Support

The implementation of the cryptographic functionality is based on the cryptographic library "bouncyCastle JCE provider" version 1.70. The library is part of the TOE and compiled into the CSP Light Module.

11.8.1 Operational Cryptographic Support

The TOE implements the cryptographic primitives required for its operation as CSP Light Module in the context of the TSS. This specifically includes:

1. CSP initialization with generation of the system master keys and cluster keys (FCS_COP.1/Hash, FCS_CKM.5/AES, FCS_CKM.5/CLDH), see 2.4a)
2. Cryptographic operations for the Trusted Channel according to 11.4
3. Signing key creation (key owner signing key) for the CRE Account (FCS_CKM.1/ECC) and key management therefore (FDP_ACC.1/KM, FMT_MSA.1/KM, FMT_MSA.3/KM) including key owner signing key deletion (FMT_MTD.1.1/KM (4)),
4. Signature creation (FCS_COP.1/CDS-ECDSA) of transaction and system log messages as requested by the CRE via the Trusted Channel,
5. Signature creation (FCS_COP.1/CDS-ECDSA) of audit log messages based on internally stored audit records created and exported (returned) on request by the CRE via the Trusted Channel,
6. Key usage counter synchronization according to 11.9.3 and signing key transfer within the cluster according to 11.9.4,
7. Signature verification and decryption of the CSP Update Code Package (11.10),
8. Provision of random numbers based on a hash based random number generator (FCS_RNG.1) for TOE internal usage.

The TOE will overwrite all cryptographic keys with zeros as soon as they are no longer needed (FCS_CKM.4).

11.8.2 Generic Cryptographic Support

Furthermore, the TOE needs to support the following generic cryptographic primitives and operations requested by the [PP-CSP-LIGHT]:

1. Generation of RSA keys (FCS_CKM.1/RSA),

2. Creation and verification of digital RSA signatures (FCS_COP.1/CDS-RSA, FCS_COP.1/VDS-RSA),
3. Hybrid encryption and decryption of user data (FCS_COP.1/HEM, FCS_COP.1/HDM, FCS_CKM.5/ECDHE, FDP_ETC.1).

11.9 TOE Redundancy und Fail-Over Concept

11.9.1 Load distribution and fail-safety

The signature key of a CRE Account (e.g. the key owners signature key) is securely stored within the CSP. If the CSP hardware (e.g. storage medium) fails, the key owner signature key would be lost forever. To encounter this, it is necessary to provide a redundancy concept for the signature key. By the concept implemented, each signature key is securely stored at a main CSP (Master-CSP according to [PPC-CSP-LIGHT-TS-AU-CL]) and at a backup CSP also (Slave-CSP according to [PPC-CSP-LIGHT-TS-AU-CL]). During normal operation, only the Master-CSP (the CSP responsible for the CRE Account with the signature key in question) performs the signature creation triggered by the signData function at the CSP API interface. Every time a trusted channel operation is performed at the Master-CSP, the latest signature key usage counter is synchronized to the Slave-CSP by means of a signature counter synchronisation operation (11.9.3).

11.9.2 Fail-Over

If the Master-CSP fails, the signature key and its security attributes are securely transferred (wrapped and sealed) from the Slave-CSP and imported (verified and unwrapped) to a newly assigned CSP taking over the Master-CSP role. For details of key export and import see below (11.9.4). To do this, after initialization a CSP-Light module performs an elliptic curve Diffie-Hellmann key agreement with every other active CSP-Light module. These keys are the cluster keys according to [PPC-CSP-LIGHT-TS-AU-CL] (FCS_CKM.5/CLDH).

11.9.3 Key Usage Counter Synchronization

After invocation of an API function within the Trusted Channel at the Master-CSP, a sealed data structure holding the key reference, the new value of the signature key usage counter and a time stamp representing the export time (current system time) is requested from the Master-CSP. The cryptographic seal added to this data structure is created by means of the system master signing key CspSignKey and transferred to the Slave-CSP (by the syncSigCnt API function). This is done before the created signature is returned by the response to the CRE.

At the invocation of the syncSigCnt API operation on the Slave-CSP, it first verifies the cryptographic seal of the data imported (by means of CspSignKey) to prevent modification and insertion. If the verification fails, the import is denied (FPT_ISA.1/CK). Then the wrapped data are unwrapped (decrypted by means of the CspEncrKey), (FCS_COP.1/KU). The key the imported key usage counter is imported for is identified uniquely by the key reference (FMT_MSA.2).

The value of the signature key usage counter is only imported (stored) at the importing CSP (Slave-CSP) if it is not lower than the signature key usage counter currently stored for the respective TS account (identified by the reference key). If at any point, the import is denied all imported data and all data derived from that are destroyed by means of zeroization (FCS_CKM.4) before the related resource is released.

11.9.4 Signing Key Transfer within the Cluster

The key transfer of the CRE Account signing keys (key owner signing keys) takes place at the Fail-Over-Procedure when the Master-CSP fails (see above) or at the relocation of a CRE Account from one CSP to another CSP triggered by the Administrator.

a) **Signing Key Cluster-Export**

By means of the transferClusteredKey API function the CSP returns the signature key together with the security attributes key identity (key reference), PACE password, serial number and signature key usage counter (FPT_ESA.1/CL) together with a time stamp representing the exporting time (current system time). All these elements are wrapped (encrypted by means of the Cluster encryption key of the target CSP) (FCS_COP.1/KW, FCS_COP.1/ED, FPT_TCT.1/CL). A cryptographic seal over the wrapped data (created by means of the Cluster signing key of the target CSP) is appended to the exported data (FPT_ESA.1/CK, FCS_COP.1/MAC).

b) **Signing Key Cluster-Import**

By means of the syncClusteredKey API function the CSP first verifies (by means of Cluster signing key of the respective source CSP) the cryptographic seal of the data imported to prevent modification and insertion (FPT_TDC.1/CK). If the verification fails, the import is denied (FPT_ISA.1/CK). Then the wrapped data are unwrapped (decrypted by means of the respective Cluster encryption key) (FCS_COP.1/KU, FPT_TIT.1/CK, FPT_TCT.1/CK, FPT_TIT.1/CL, FPT_TDC.1/CL). The key identity and the other security attributes are verified (FPT_ISA.1/CL). The key to import and its associated security attributes are identified uniquely by the key reference (FMT_MSA.2).

The exporting time stamp (see above) associated with the imported data is verified against the actual system time by the importing CSP. If it differs for more than 30 seconds the import is denied (FPT_ISA.1/CK). If at any point, the import is denied all imported data and all data derived from that are destroyed by means of zeroization (FCS_CKM.4) before the related resource is released.

11.9.5 Signing Key Deletion

The key owner is able to delete the CRE Account signing keys he owns via the administration interface as well as by means of the Client interface via Trusted Channel (FMT_MTD.1.1/KM (4)).

In the first case, the key is securely deleted by the TOE; however, the TOE assumes that the user will delete the key on the slave-CSP themselves (by calling the same function there).

In the latter case the signing key deletion performed via the Trusted Channel terminating at the Master-CSP also triggers the deletion of the same signing key hold at the Slave-CSP. This signing key deletion synchronization between Master and Slave-CSP is based on the key usage counter synchronization as described in 11.9.3.

11.10 TOE Secure Update

The TOE provides functionality for a secure update of the TOE. Therefore, the updateCodePackage function is provided by the TOE-API. It can only be invoked by the Administrator (FDP_ACC.1/UCP, FDP_ACF.1/UCP). It imports a signed and encrypted binary package (FDP_ITC.2/UCP) consisting of the following elements: package name, version number, signature, signature key reference (representing the issuer), encryption key reference, encrypted software binary (FPT_TDC.1/UCP, FDP_ACF.1/UCP).

Before applying the UCP, the importing CSP verifies the signature value as signature over the UCP. The signature key used for signature verification is stated by the signature key reference, the key used for decryption by the CSP is stated by the encryption key reference. If the verification of the Update Code Package fails (FCS_COP.1/VDSUCP), the TOE will overwrite the memory segment of the UCP with zeroes before releasing it (FDP_RIP.1/UCP, FCS_CKM.4).

Then the TOE verifies the security attribute issuer and version (FPT_TDC.1/UCP, FDP_ACF.1.1/UCP (2) (b)). The TOE will only proceed, if the provided update has a higher or equal version number compared to the currently installed TOE version. It should be noted that in case of an equal version number, the TOE will not actually apply the update as it can be assumed that the versions are identical.

By means of the decryption key the TOE decrypts the encrypted software binary (FCS_COP.1/DecUCP) and replaces the software package as stated by the package name element. After this, a restart of the TOE application software is performed automatically.

If at any point the import is denied, the import procedure is aborted and all imported data and data derived from that are destroyed by means of zeroization (FDP_RIP.1/UCP, FCS_CKM.4) before the related resource is released.

12. Annex

12.1 Reference Documentation

ID	Dokument
AIS20	Anwendungshinweise und Interpretationen zum Schema (AIS) AIS 20, Version 3, 15.05.2013, Zertifizierungsstelle des BSI im Rahmen des Zertifizierungsschemas. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_pdf.pdf?__blob=publicationFile&v=2
ANSI-X9.63	ANSI-X9.63, Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2011
BSI-TEST-SUITE	BSI Test suite, Implementation of test procedure A and test procedure B of AIS 31
BSI-TR-03151	Technical Guideline BSI TR-03151 – Secure Element API (SE API), Version 1.0.1, 20. December 2018
BSI-TR-03153	Technische Richtlinie BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, Ver. 1.0.1
CC1	Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017
CC2	Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, April 2017
CC3	Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, April 2017
CSP-AGD	D-TRUST-TSE-WEB – Dokumentation und Integratorhandbuch CSP-Light-Modul, Version 1.4.1
CSP-FSP	D-TRUST-TSE-WEB – Schnittstellen- und Funktionsspezifikation CSP-Light-Modul, Version 1.6.8
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)
FIPS PUB 180-4	NIST, Secure Hash, Standard (SHS), 2012
FIPS PUB 186-4	Digital Signature Standard (DSS), FIPS 186-4
FIPS197	Federal Information Processing Standards Publication 197 (FIPS PUB 197), Advanced Encryption Standard (AES), 2001
ICAO Doc9303	ICAO: Machine Readable Travel Documents, ICAO Doc9303, Part 11: Security Mechanisms for MRTDSs, seventh edition, 2015
ISO/IEC 9797-2	ISO/IEC 9797-2 Information Technology – Security techniques, Message Authentication Codes (MACs), Part 2: Mechanisms using a dedicated hash-function, 2011
ISO/IEC 10116	ISO/IEC 10116 Information Technology – Security techniques, Modes of operation for an n-bit block cipher, 2017
ISO/IEC 18033-3	ISO/IEC 18033-3 Information technology – Security techniques, Encryption algorithms – Part 3: Block ciphers, 2010
ISO/IEC 14888-2	ISO/IEC 14888-2 Information technology – Security techniques, Digital signatures with appendix – Part 2: Integer factorization based mechanisms, 2008
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. Oktober 2017
NIST-SP800-38A	NIST, SP800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques
NIST-SP800-38B	NIST, SP800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005
NIST-SP800-38F	NIST, SP800-38F Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, 2012
NIST-SP800-56C	NIST, Recommendation for Key Derivation through Extraction-then-Expansion, Special Publication SP800-56C, November 2011
PKCS#1	PKCS #1 v2.2: RSA Cryptographic Standard, https://www.emc.com/emc-plus/rsa-labs/pkcs/files/h11300-wp-pkcs-1v2-2-rsa-cryptography-standard.pdf, 27.10.2012

PKCS#5	PKCS #5: Password-Based Cryptography Specification Version 2.0, https://tools.ietf.org/html/rfc2898
PP-CSP-LIGHT	Common Criteria Protection Profile, Cryptographic Service Provider Light BSI-CC-PP-0111-2019, Version 1.0
PP-SMAERS	Common Criteria Protection Profile, Security Module Application for Electronic Record-keeping Systems (SMAERS), BSI-CC-PP-0105-V2-2020, Version 1.0
PPC-CSP-LIGHT-TS-AU	Common Criteria Profile Configurations, Cryptographic Service Provider Light – Time Stamp Service and Audit (PPC-CSPLight-TS-Au), Protection Profile-Module CSPLight Time Stamp Service and Audit (PPM-TS-Au), BSI-CC-PP-0112-2020, Version 1.0
PPC-CSP-LIGHT-TS-AU-CL	Common Criteria Protection Profile Configuration, Cryptographic Service Provider Light – Time Stamp Service and Audit – Clustering (PPC-CSPLight-TS-Au-Cl), Protection Profile-Module CSPLight Clustering (PPM-Cl), BSI-CC-PP-0113-2020, Version 1.0
REDHAT	Red Hat Enterprise Linux 8 Security Hardening, Securing Red Hat Enterprise Linux 8, 2020-03-10
RFC2104	RFC2104, HMAC: Keyed-Hashing for Message Authentication
RFC5639	Elliptic Curve Cryptography (ECC) Brainpool Standard, Curves and Curve Generation
TR-03110	BSI, Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2 - Protocols for electronic IDentification, Authentication and trust Services (eIDAS), Version 2.21, 2016
TR-03110-3	Technical Guideline TR-03110 - Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3: Common Specifications, Version 2.21, 21. December 2016
TR-03111	BSI, Elliptic Curve Cryptography, BSI Technical Guideline TR-03111, Version 2.1, 1.6.2018
TR-03151	Technical Guideline BSI TR-03151 Secure Element API (SE API), Version 1.0.1, 20. December 2018
TR-03153	Technische Richtlinie BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, Ver. 1.0.1

12.2 Terminology

Acronym	**Term**
API	Application-Programming-Interface
CRE	Client Remote Entity
CSP	Cryptographic Service Provider
ERS	Electronic Record-keeping System
HSM	Hardware Security Module
OAuth	Open Authentication
PACE	Password Authenticated Connection Establishment
SMA	Security Module Application
SMAERS	Security Module Application for Electronic Record-keeping Systems
TC	Trusted Channel
TOE	Target of Evaluation
TSE	Technische Sicherheitseinrichtung
TSS	Technical Security System