Federal Office
for Information Security

Common Criteria Protection Profile Security Module Application for Electronic Record-keeping Systems (SMAERS)

BSI-CC-PP-0105-V2-2020

Version 1.0

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

Internet: https://www.bsi.bund.de
© Federal Office for Information Security 2020

Table of Contents

Figures

Tables

1 PP introduction

In order to combat tax-fraud, electronic record-keeping systems in Germany must be equipped with a 'Certified Technical Security System' (CTSS; 'Zertifizierte Technische Sicherheitseinrichtung') that consists of a storage medium, a security module, and a unified digital interface. The security module is subject to common criteria security certifications. W.r.t. to security requirements for the security module – defined by Bundesamt für Sicherheit in der Informationstechnik – the module consists of two components:

1. an application component that handles the business logic and functionality required to serve an electronic record-keeping system. This component is dubbed the *security module application for electronic record-keeping systems* (SMAERS).
2. a generic and reusable cryptographic component that implements the core cryptographic functionality required. This component is dubbed *cryptographic service provider* (CSP).

This protection profile defines the security requirements of the SMAERS component. Depending on the overall architecture, different security requirements exist for a CSP. These are defined in two protection profiles and protection profile configurations. For details on allowed architectures and required protection profiles and configurations, cf. Chapter 1.2 below, in particular *Section Non-TOE Hardware/ Software/ Firmware available to the TOE*.

In the following, the abbreviation CSP is redundantly used for all allowed configurations mentioned.

1.1 PP Reference

Title:	Common Criteria Protection Profile Security Module Application for Electronic Record-keeping Systems (SMAERS)
Sponsor:	BSI
CC Version:	3.1 Revision 5
Assurance Level:	EAL2 augmented with ALC_LCD.1 and ALC_CMS.3
General Status:	Final
Version Number:	1.0
Registration:	BSI-CC-PP-0105-V2-2020
Keywords:	security module application, electronic record-keeping systems

1.2 TOE Overview

TOE Type

The Target of Evaluation (TOE) is a *security module application* implemented as software. It is either running on the platform of the CSP (referred to as *platform-architecture*), or running on a separate device communicating with the CSP via a trusted channel (referred to as *client-server architecture*), cf. [PP CSP][PP CSPLight].

The TOE has to securely store sensitive objects (user data and TSF data, see assets). In case of the platform-architecture, the CSP platform provides suitable mechanisms for this that may be used by the TOE.

In case of the client-server architecture, where the TOE can not directly rely on the CSP platform, a platform with secure storage must be used. The platform that executes the TOE has to provide mechanisms to preserve the integrity, confidentiality (when required), and to prevent rollback of stored sensitive objects, including the TOE software itself. The confirmation of suitability of the chosen platform shall be part of the evaluation.

The TOE relies on the CSP for all cryptographic operations except for the implementation for the trusted channel. In addition the TOE must rely on the platform in case of update code package verification.

TOE Definition

The TOE is a security module application as part of the security module of a certified technical security system (CTSS) for electronic record-keeping systems (ERS). Figure 1 describes the interaction between TOE and non-TOE components.

The CTSS consists of a security module, a storage medium, and a CTSS interface component providing the standardized digital interface (cf. [FCG], section 146a, paragraph 1, sentence 3) for the electronic record-keeping system and cash inspection (cf. [FCG], section 146b). The [KSV] section 2 requires the security module to provide

– the point in time when the transaction starts (cf. [KSV] section 2 sentence 2 number 1),

– the transaction number (cf. [KSV] section 2 sentence 2 number 2),

– the point in time when the transaction is completed or terminated (cf. [KSV] section 2 sentence 2 number 6), and

– the check value (cf. [KSV] section 2 sentence 2 number 7).

The security module provides the logging of transactions and other audit-relevant processes in the form of log messages (cf. [TR TSEA], Chapter 3.1). Log messages are created by the TOE using the CSP.

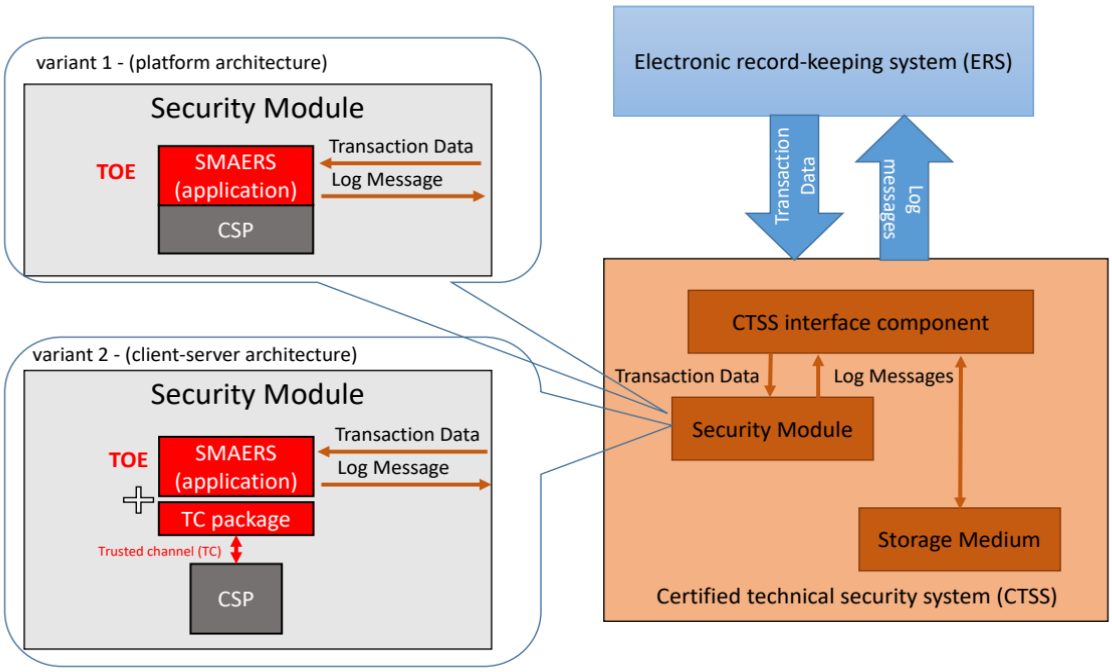


Figure 1: Description and interaction between the TOE and the relevant non-TOE components

Log messages consist of either certified data or audit data [TR SE], as well as protocol data and a signature. There are three types of *log messages*, i.e. *transaction logs, system logs* and *audit logs*, cf. [TR SE] and Appendix: Log Message Structure and Data Dependency.

Transaction logs are created to protect the transaction data of the electronic record-keeping system as certified data. They are generated whenever a transaction is started, finished (i.e. completed or terminated), and may be generated when transaction data are updated. The protocol data of *transaction logs* contain the

transaction number of the transaction and time stamps. All *transaction logs* with the same transaction number build together the required data of the fiscal transaction according to [KSV] Section 2, Sentence 2.

System logs are generated to log the execution of system operations as described in [TR SE] and TSF security events.

Audit logs are generated to document management or configuration operations of the CSP. The audit data of *audit logs* provide information for the interpretation of the *transaction logs,* e.g. providing information about setting or readjusting the time source that is used for time stamps.

The TOE

- imports transaction data from the CTSS interface component and includes it as certified data in a *transaction log*,
- generates part of the protocol data for the *transaction log* including
  - the transaction number generated by the TSF,
  - the serial number included by the TSF for verification of the digital signature (keyID),
- includes the timestamp, signature counter and digital signature created by the CSP over the certified data and the protocol data in the transaction log and system log,
- imports audit records from the CSP (cf. FAU_GEN.1) and exports them as *audit log*[1],
- generates a *system log* consisting of commands and TSF security events as certified data,
- exports all types of *log messages* to the CTSS interface component,
- provides identification and authentication of users, access control and security management of the TSF for authorized users by using cryptographic services of the CSP.

The signature counter enumerating the signatures created for *log messages* and the time stamps when the signature was created are generated by the CSP and are part of the protocol data.

The main part of the protection profile in hand assumes the TOE being implemented as software running on a component that is physically separated from the CSP in a client-server architecture, cf. [PP CSP][PP CSPL]). That means the security target shall claim the package *trusted channel* between the TOE and the CSP in Chapter 7. A trusted channel is necessary because the TOE and the CSP are implemented as separated components and must interact through a trusted channel in order to protect the integrity of the communication data, and to prevent misuse of the CSP w.r.t. signing and time stamping services provided for the TOE.

In case of the platform architecture, the TOE is running on a CSP where the CSP serves as a secure execution platform, cf. platform architecture [PP CSP]. Then, the package *trusted channel* is not required. Note that the TOE must not be operated in the platform architecture in combination with CSPLight.

The TOE must be compliant to BSI Technical Guideline TR-03153 [TR TSEA], and must use cryptographic services of the CSP compliant with BSI Technical Guideline TR-03116-5 [TR CryAS].

Method of Use

The TOE is part of the security module of the CTSS protecting accounts and records of one or more electronic record-keeping systems. If more than one electronic record-keeping system uses the TOE the *serial number of ERS (clientID)* sending input must be identifiable and known to the TOE for selecting the signature-creation key.

1 A CSP meeting BSI TR-03151 [TR SE] shall export audit records in a format suitable to directly create Audit logs, e.g. by allowing for (hashed) protocol data as additional input for the signed export of audit records.

The TOE generates time stamped and signed log messages using the CSP's cryptographic services in order to generate verifiable sequences of transaction data and log messages for cash register inspection, cf. [FCG], Section 146b.

The TOE provides security management features of the TSF for administrators. The security management features are used to configure the communication channels between the TOE with the CTSS interface component and the CSP. The TOE may support the security management functionality of the CSP by providing a communication interface to an administrator or other services, e.g. to a time server.

The TOE requires the platform to support receiving and verifying the integrity of update code packages (UCPs) for installation of a new certified TOE.

TOE Life Cycle

The TOE life cycle is part of the life cycle of the CTSS. The life cycle documentation shall describe the complete life cycle of the CTSS including details necessary for the understanding of the interaction with and configuration of the CSP including. While only the TOE life cycle is part of the common criteria certification the additional documentation has to be provided within the certification process and has to be approved by BSI in a separate process.

The additional documentation must address, but is not limited to the following documents:

- The provisioning of the CSP within the life cylce of the CTSS describing the initial personalization and subsequent renewal of keying material used in the context of the TOE, the assignment and separation of users and roles contained in the CSP, and the audit configuration of the CSP.
- The update procedures to allow for recovery from security incidents including the procedures for creating, distributing, and enforcing installation of update code packages for the TOE and the CSP,
- The PKI concept of the underlying public key infrastructure (PKI) and the audit reports of the involved trust centers to ensure the correct identification of the taxpayer, the binding of the CTSS and keying material to the taxpayer, and the verifiability of generated signatures by third parties.

If any steps within the CTSS life cycle are delegated to an external entity, e.g. an integrator, the additional life cycle documentation must explicitly define the entities and their obligations.

Additional documentation must be provided in the following cases:

- If the client-server model is used, the personalization and management of the password used to protect the trusted channel between the TOE and the CSP must be described.
- If a CSPLight is used instead of a CSP, it must be securely operated in an environment certified according to ISO/IEC 27001. The operator must implement and continuously maintain an information security management system (ISMS) with security level *high* according to Appendix: Operational Requirements for CSPLight.

Non-TOE Hardware/Software/Firmware available to the TOE

The TOE requires

- a CSP. The CSP must be certified according to one of the following protection profiles:
  - Common Criteria Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit [PPC-CSP-TS-Au]
  - Common Criteria Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service, Audit and Clustering [PPC-CSP-TS-Au-Cl]

  - Common Criteria Protection Profile Configuration Cryptographic Service Provider Light – Time Stamp Service, Audit and Clustering [PPC-CSPLight-TS-Au-Cl] running on hardware that meets Appendix: Operational Requirements for CSPLight.
- a CTSS interface component that provides the transaction data and receives log messages
- an underlying platform with a secure storage (see OE.SMAERSPlatform).

The security target has to reference a fully defined API description of the CSP.

The CSP shall meet [TR CryAS].

2 Conformance Claims

2.1 CC Conformance Claims

The PP claims conformance to CC version 3.1 revision 5.

Conformance of this PP with respect to CC Part 2 [CCP2] (security functional components) is CC part 2 extended.

Conformance of this PP with respect to CC Part 3 [CCP3] (security assurance components) is CC part 3 conformant.

2.2 Package Claim

This PP claims conformance to EAL2 augmented with ALC_LCD.1 and ALC_CMS.3.

2.3 PP Claim

This PP does not claim conformance to any other PP.

2.4 Conformance Rationale

The dependencies of security assurance components of the package EAL2 are solved within the package [CCP3]. The components ALC_LCD.1 and ALC_CMS.3 have no dependencies on other components.

2.5 Conformance Statement

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

3 Security Problem Definition

3.1 Introduction

Assets

The assets of the TOE are

– the transaction data provided by the CTSS interface component, where authenticity and integrity including completeness of the transaction data shall be protected, i.e. verification of the transaction log messages shall determine whether the transaction data was received from the CTSS interface component, and modifications and gaps shall be detectable,

– the transaction number (as part of the transaction data) that enumerates transactions. The transaction number must be continuously increasing without gaps.

– the audit records imported from the CSP and exported as audit logs to the CTSS interface component, the system logs and transaction logs

– the update code package (UCP) and the UCP version number

– the PACE password to setup the trusted channel to the CSP (only in case the package 'Trusted Channel' is claimed).

The CSP protects and enumerates its audit records against undetected modification and gaps.

Asset	Protection
transaction data	authenticity, integrity
transaction number	authenticity, integrity
audit logs/audit records, system logs and transaction logs	authenticity, integrity
update code package	authenticity
UCP version number	integrity

Table 1: Assets to be protected by the TOE

Users and Subjects

The users and subjects defined below are distinct from the role model in [TR SE]. Users and roles defined in the latter, including e.g. the taxpayer acting as (CTSS-)administrator, converge in the CTSS interface component.

The TOE knows users as external entities active communicating with the TOE as

– *electronic record-keeping system (ERS),*

– *CTSS interface component*,

– *CSP*,

– *(SMAERS-) administrator*.

The *ERS* is tested by the TOE as an external entity and communicates with the TOE through the *CTSS interface component*. The TOE also uses the *CTSS interface component* as a passive external entity for the storage of transaction logs, system logs, and audit logs. The TOE uses the CSP as external entity providing security services and audit records.

The (SMAERS-) administrator is assumed to be the TOE manufacturer or an integrator acting on behalf of the manufacturer and must not be the taxpayer.

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

Roles

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

– role *unidentified user*: This role is associated with any user not (successfully) identified by the TOE. This role is assumed for subjects after start-up of the TOE and deactivated *CTSS interface component.* The TOE allows users in this role to run self-test of the TOE.

– role *administrator*: A user in this role is allowed to perform management functions. The administrator subject is acting on behalf of a human user after successful authentication as administrator until logout.

– role *CTSS interface*: A subject in this role is allowed to import *Transaction Data* from *CTSS interface component*, to generate *transaction logs and system logs*, and to export *transaction logs and system logs* to the *CTSS interface component*. A subject in this role is started automatically after start-up of the TOE if the *CTSS interface role* is *activated* and the *CTSS interface component* and the *CSP* are successfully tested according to FPT_TEE.1. The ERS uses the CTSS role.

– *CSP role*: A subject in this role is allowed to import audit records from CSP and to export *Audit logs* to the *CTSS interface component*. In addition the CSP role is allowed to start the update process. A subject in *CSP role* is started automatically after start-up of the TOE if the *CSP* is successfully tested according to FPT_TEE.1.

Objects

The TSF operates on the following types of user data objects

– *transaction data* (TD),

– *audit records,*

– *data-to-be-signed* (DTBS),

– *protocolData with signature* containing the time stamp, the signature counter, and the digital signature; all generated by the CSP (cf. [TR SE] and [TR TSEA]),

– *log messages* (LM) as *transaction log, system log* or *audit log,*

– *update code package* (UCP)

– *commands (type of operation).*

The formats of *transaction data* and *log messages* meet [TR SE].

The CTSS interface component provides *transaction data* as data to be certified by means of *transaction logs (cf. below).*

Audit records are data imported from the CSP.

The *data-to-be-signed* compiled by the TSF and sent to the CSP for signing and time stamping consists of

– certified data i.e.

  • in case of *a transaction log*: the *transaction data* with the type of the certified data *transaction log*, object identifier (id-SE-API-transaction-log): bsi-de (0.4.0.127.0.7) applications (3) sE-API (7) sE-API-dataformats(1) 1 (cf. [TR SE], chapter 2.3.1)

  - in case of *a system log*: the security related events with the type of the certified data system *log,* object identifier (id-SE-API-system-log): bsi-de (0.4.0.127.0.7) applications (3) sE-API (7) sE-API-dataformats(1) 2 (cf. [TR SE], chapter 2.3.2)
  - in case of *an audit log*: the *audit record* with the type of the certified data *audit log,* object identifier (id-SE-API-audit-log): bsi-de (0.4.0.127.0.7) applications (3) sE-API (7) sE-API-dataformats(1) 3 (cf. [TR SE], chapter 2.3.3)
- protocol data generated by the TSF
  - the *transaction number*,
  - the *keyID* as a hash value of the signature-verification key,
  - the *type of the operation* as name of the API function whose execution is recorded by the *log message*, i.e. *StartTransaction*, *UpdateTransaction* or *FinishTransaction*,
  - the *optional protocol data* (may be empty).

The CSP adds to the *data-to-be-signed*

- the point in *time* when the *log message* was created,
- the *signature counter* that enumerates the signatures created with the signature-creation key.

Refer to [TR SE] for details of the log messages format.

The Update Code Package (UCP) is a complete software package that is managed by the secure platform and its operating system that executes the SMAERS application. The operating system of the secure platform performs an update of the SMAERS application, it is required that the verification of the UCP is performed by the operating system prior to installation. Depending on the update procedure of the operating system either the new TOE alone or the old TOE and the new TOE together perform an *upgrade* by exporting and importing TSF data into the new TOE.

Security Attributes

Users known to the TOE have the security attributes stored in an *authentication data record (ADR):*

- *user identity* (User-ID),
- *authentication reference data*,
- *role* with detailed access rights gained after successful authentication.

The *CTSS interface component* and CSP known to the TOE have at least the security attributes *identity*, cf. FIA_ATD.1.

Passwords as *authentication reference data* have the security attributes

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

The *transaction data* (TD) have the security attributes

- *clientID* to determine the signature-creation key to be used for signing the *Transaction log* and the *keyID* to be included in the protocol data of the *Transaction log,*
- *type of the operation* to determine the actual transaction as *StartTransaction, UpdateTransaction or FinishTransaction.*
- *transaction number* to assign the TD to an ongoing transaction and enumerating the transactions continuously increasing without gaps.

The TOE accepts *transaction data* only if the clientID is known and mapped to a signature key in the CSP *(keyID).*

The TOE manages for each known keyID the last assigned transaction number and the transaction numbers of the ongoing transactions. If the *type of the operation* of imported *transaction data* is *StartTransaction,* then a new transaction is started and the TOE generates a new *transaction number* by addition of 1 to the last assigned *transaction number*, includes this value in the protocol data of the *transaction log* returned to the CTSS interface component, and add this value to the list of ongoing transaction. If the *type of the operation* is *UpdateTransaction* or F*inishTransaction* and meets the *transaction number* of an ongoing transaction, the *transaction number* in the transaction data is imported and assigned to the protocol data of the *transaction log.* If the *type of the operation* is *FinishTransaction* or the transaction is terminated by the TOE, the *transaction number* is removed from the list of ongoing transactions cf. [TR SE].

A UCP has the security attributes

– *issuer*: identifier of the authorized issuer of the UCP signing the UCP,
– *signature*: digital signature of the UCP generated by the authorized issuer,
– version number.

Log messages

Log messages include at least the following security attributes and the signature used by the tax inspector of the cash register inspection

– *signature counter* enumerating the *log message* continuously increasing without gaps,
– *time stamp* as time when the *log message* was created,
– *keyID* to determine the certificate to be used for the verification of the digital signatures as a check value of the transaction data.

The following security attributes are conditional in log messages:

– Transaction logs contain the security attribute *transaction number* assigning the *log message* to the transaction of the electronic record-keeping system and the *type of operation*, i.e start, update or finish transaction.
– System logs contain the security attribute *event* assigning the *log message* to the security related event of the TSF.
– Audit logs contain the security attribute *audit record* assigning the log message to security related events of the CSP.

3.2 Threats

T.EvadTD Evading *Transaction Data*
The attacker prevents sending to the TOE legally required *transaction data* in order to avoid generation of valid *Transaction logs*.

T.ManipTD Manipulation of *Transaction Data*
The attacker manipulates *transaction data* sent by the electronic record-keeping system through the CTSS interface component to the TOE, or generates forged *transaction data* and sends them to the TOE in order to generate incorrect *transaction logs*.

T.ManipDTBS Manipulation of Data-To Be-Signed-And-Time-Stamped
The attacker generates forged or manipulates *Data-To-Be-Signed* sent for signing and time stamping to the

CSP. A forged *transaction log* may result in forged transaction data provided for cash inspection. A forged *audit log* or *system log* may result in faulty interpretation of the transaction data.

T.ManipLM Manipulation of a *Log Message*
The attacker manipulates without detection a *log message* exported to the CTSS interface component. This log message is then used for cash inspection.

T.ManipLMS Manipulation of a *Log Message Sequence*
The attacker manipulates without detection the *log message sequence* exported to the CTSS interface component. This log message sequence is then used for cash inspection.

T.ManipTN Manipulation of *Transaction Number*
The attacker manipulates the TOE's internal *transaction number* used in *log messages*.

T.FaUpD Faulty *Update Code Package*
An attacker deploys an unauthorized manipulated *update code package* or restores a previous TSF implementation enabling attacks against integrity of TSF implementation, or confidentiality and integrity of user data or TSF data after installation of the manipulated *update code package*.

Application note 1: The taxpayer is the subject that owns and operates the ERS and CTSS (either directly or indirectly). The taxpayer is assumed to use an ERS equipped with a CTSS, to prevent misuse of the ERS by unauthorized persons, and to correctly tally all transactions with the ERS as required by law (c.f. OSP.SecERS and OSP.ProtDev). The TOE does not protect against threats that result from temporarily or permanently not using an ERS as required by law. The taxpayer is however also considered as potential attacker, who may use a manipulated CTSS or manipulates logs after they were produced by the CTSS.

3.3 Organisational Security Policies

OSP.SecERS Secure use of the Electronic Record-Keeping System
The taxpayer shall use an electronic record-keeping system to generate accounts, records and receipts. The electronic record-keeping system shall record separately, correctly, completely, and in real time accounts and records of all transactions that are legally required; cf. [FCG], Section 146a (1), Sentence 1. The receipt shall include besides the transaction data the points in time when the transaction is started, completed or terminated, and the transaction number provided by the certified security device; cf. [KSV], Section 6, Sentence 1.

OSP.CertSecDev Certified Security Device
The electronic record-keeping system and the accounts and records generated by the electronic record-keeping system shall be protected by a certified security device; cf. [FCG], Section 146a (1), Sentence 2. The security module of the certified security device generates time stamps of the start, completion, and termination of a transaction, as well as a transaction number; cf. [KSV], Section 2, Sentence 3.

OSP.ProtDev Protection of Electronic Record-Keeping System and Certified Security Sevice
The taxpayer shall correctly operate the electronic record-keeping system (cf. [FCG], Section 379 (1), Sentence 1, Number 4), and correctly protect the electronic record-keeping system and the certified security device; cf. [FCG], Section 379 (1), Sentence 1, Numbers 5.

OSP.ValidTrans Validation of transactions
A sequence of transactions is valid if (1) all Log messages meet the requirements for content defined in [KSV] section 2, (2) their check values according to [KSV] section 2 sentence 2 number 7 are valid digital signatures, (3) the transaction numbers are consecutive increasing without gaps (cf. [KSV] section 2 sentence 4), and (4) the points in time when the transaction starts are monotonic increasing. The sequence of Log messages support detection of incomplete transactions and manipulations.

OSP.Update Authorized *Update Code Package*s
*Update Code Package*s are delivered to the TOE from the platform and are signed by the authorized issuer. The platform verifies the authenticity of the received *Update Code Package* before installation.

Application note 2: The update is performed by the platform provided by the operational environment, c.f. OE.CSPPlatform for the platform architecture or OE.SMAERSPlatform for the client-server architecture.

3.4 Assumptions

A.SMAERSPlatform Secure platform storage

The platform that executes the TOE provide mechanisms to preserve the confidentiality, integrity and to prevent rollback of stored sensitive objects, including the TOE software itself.

A.CSP Cryptographic Service Provider

A CSP is *either* remotely accessible via trusted channel to the TOE (client-server architecture) and certified as compliant to [PPC-CSP-TS-Au], [PPC-CSP-TS-Au-Cl], or [PPC-CSPLight-TS-Au-Cl] running on hardware that meets Appendix: Operational Requirements for CSPLight as well as the requirements in chapter 1.2 section “TOE Life Cycle”
Or, the operational environment provides a cryptographic service provider for the TOE that is certified as compliant to [PPC-CSP-TS-Au] or [PPC-CSP-TS-Au-Cl] (platform architecture).
The CSP exports audit records in form of audit logs meeting [TR SE]. Also, the CSP must provide a fully defined API description.

A.ProtComCSP Protection of Communication between TOE and CSP

The integrity of the communication data between TOE and CSP in the client-server architecture is protected via a trusted channel, and the security target must claim the package *Trusted Channel*, defined in Chapter 7. In case of the platform architecture of the CSP, the CSP provides a secure execution environment for the TOE and protects the integrity of communication data with the TOE directly using the security services of the CSP.

A.ProtComERS Protection of Communication between TOE and Electronic Record-Keeping System

The electronic record-keeping system provides transaction data whenever a transaction starts, transaction data are updated, or when the transaction is completed or terminated. The ERS and the TOE must be contained in the same physical operational environment that must protect the integrity of communication data between the TOE and the electronic record-keeping system see Figure 2.

A.VerifLMS Verification of Log Message Sequences

The operational environment verifies the digital signatures, the transaction numbers and the time stamps of *log messages* in sequence in order to detect forged or missing *log messages*. The certificate of the signature-verification data is securely distributed to the tax inspector. The tax inspector ensures that the transactions are created by a certified security module, e.g. in form of test transactions.

A.Admin Trustworthy Administrator

The administrator acts in a trustworthy way and must be independent of the taxpayer (cf. Application note 1).

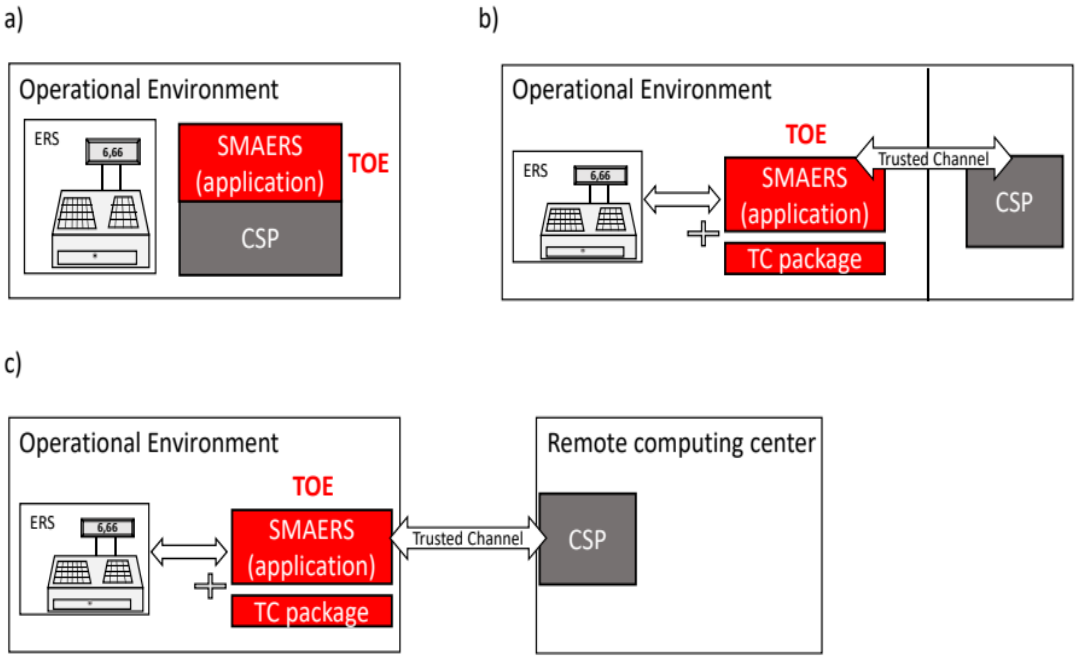


Figure 2: The TOE is always operated as a local component. a) platform architecture b) client-server architecture with local computing center c) client-server architecture with remote computing center

4 Security Objectives

4.1 Security Objectives for the TOE

O.GenLM Generation of *Log Messages*

The TSF shall generate *transaction logs* containing

– *transaction data*, *transaction number* created by the TSF, and

– time stamps and digital signatures created by the cryptographic service provider.

The TSF shall generate *system logs*.

O.ImpExp Import of *Transaction Data* from and Export of *Log Messages* to CTSS Interface Component

The TSF shall import *transaction data* from the electronic record-keeping system through the CTSS interface component, import *audit records* from the CSP and export *log messages* to the CTSS interface component.

O.IAA Authentication of Administrators

The TOE shall verify the claimed identity of the administrators by means of password.

O.SecMan Security Management

The TOE shall restrict the security management of TSF and TSF data to authenticated administrators The TSF prevents management of the t*ransaction number* generation.

O.TEE Test of External Entities

The TSF shall test the presence and identity of the electronic record-keeping system and cryptographic service provider connected to the TOE, and allow generation of *transaction logs* only if both pass the tests, and must enter a secure state if any test fails.

O.TST Self-Test and Secure State

The TSF shall perform self-tests. The TSF enters a secure state if the self-test fails, or the test of the presence and identity of the electronic record-keeping system fails, or the test of the presence and identity of cryptographic service provider fails. It shall also test for new succesfully installed update code packages and the correctness of the increased version number.

O.ImpExpUCP Secure Import and Export of User Data

The TSF shall securely export the user data and TSF data to the secure storage of the platform and import the user data and TSF data after the successful update process.

4.2 Security Objectives for the Operational Environment

OE.ERS Trustworthy Electronic Record-Keeping System

The taxpayer shall correctly use an electronic record-keeping system that provides separately, correctly, completely and in real time all *transaction data* that are legally required for the generation of *log messages* to the TOE (cf. Application Note 1). The electronic record-keeping system shall support testing its presence and identity as an external entity by the TOE. The electronic record-keeping system shall produce receipts including not only the transaction data, but also the points in time whenever a transaction is started, completed or terminated, as well as the transaction number provided by the certified security device.

OE.SMAERSPlatform Secure platform storage

The platform that executes the TOE has to ensure the integrity of the TOE itself and to provide secure storage which protects the integrity and confidentiality of stored security relevant objects as required (cf. Chapter 1.2 "TOE Type"). The platform verifies and installs the UCP.

OE.CSP Cryptographic Service Provider Component

A CSP must be *either* remotely accessible via a trusted channel to the TOE (client-server architecture) and certified as compliant to [PPC-CSP-TS-Au], [PPC-CSP-TS-Au-Cl], or [PPC-CSPLight-TS-Au-Cl] running on hardware that meets Appendix: Operational Requirements for CSPLight.

Or, the operational environment shall provide a cryptographic service provider for the TOE that is certified as compliant to [PPC-CSP-TS-Au] or [PPC-CSP-TS-Au-Cl], i.e. using the platform architecture.

The CSP shall export audit records in form of audit logs meeting [TR SE].

Application note 3: The Common Criteria Protection Profile Configurations [PPC-CSP-TS-Au], [PPC-CSP-TS-Au-Cl], and [PPC-CSPLight-TS-Au-Cl] require the cryptographic service provider to provide security services to digitally sign *transaction data*, to verify a signature of an *update code package*, and for time services. The CSP audit records shall be exported meeting [TR SE] in order to avoid a transformation of an audit record into a log message. The vendor of the TOE may provide the TOE together with a certified cryptographic service provider.

OE.CSPPlatform CSP as a Secure Platform of the TOE

In case of the platform architecture, the CSP provides a secure execution environment and security services for the TOE running on top.

Application note 4: In the typical case of a client-server architecture, the TOE and the CSP are physically separated components and the TOE cannot rely on the CSP as a secure execution platform. Instead, the security target shall claim the package trusted channel (Chapter 7) to protect the integrity of the communication between the TOE and the CSP.

OE.Transaction Verification of Transaction

The operational environment shall verify the validity of *log message sequences* by verification of the corresponding digital signatures, shall verify the *transaction number*s as being consecutive without gaps, and shall verify the points in time when the transaction starts as being consecutively increasing with increasing t*ransaction number*s, and consider the *log messages*. The taxpayer shall ensure that the cryptographic service provider holds digital signature creation data and a corresponding valid certificate. The certificate shall be securely distributed to the tax inspector.

OE.SecOEnv Secure Operational Environment

The operational environment shall protect the integrity of the communication between the electronic record-keeping system and the TOE. The administrator shall act in a trustworthy way and is assumed to be the manufacturer or integrator. The administrator must be independent of the taxpayer.

OE.SecCommCSP Secure communication between TOE and CSP

The security target shall claim the package trusted channel (Chapter 7) to protect the integrity of the communication between the TOE and the CSP in the client-server architecture. In case of the platform architecture, the operational environment shall protect the integrity of the communication between the TOE and the cryptographic service provider.

OE.SUCP Signed Update Code Packages

The manufacturer shall issue digitally signed *update code package*s together with its security attributes.

OE.SecUCP Secure download and authorized use of *Update Code Package*

The platform shall verify the authenticity of received *update code packages* and install only authentic *update code packages*.

4.3 Security Objective Rationale

The following table traces a security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective, and a 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.EvadTD	T.ManipTD	T.ManipDTBS	T.ManipLM	T.ManipLMS	T.ManipTN	T.FaUpD	OSP.SecERS	OSP.CertSecDev	OSP.ProtDev	OSP.ValidTrans	OSP.Update	A.CSP	A.SMAERSPlatform	A.ProtComCSP	A.ProtComERS	A.VerifLMS	A.Admin
O.GenLM	x			x	x						x							
O.IAA				x							x							
O.ImpExp					x						x							
O.SecMan						x					x							
O.TEE	x	x	x	x	x			x										
O.TST				x			x											
O.ImpExpUCP							x					x						
OE.CSP				x					x				x					
OE.SMAERSPlatform		x	x				x							x				
OE.CSPPlatform			x												x			
OE.ERS	x	x						x										
OE.SecUCP							x					x						
OE.SecCommCSP			x												x			
OE.SecOEnv	x			x	x			x		x						x		x
OE.SUCP							x					x						
OE.Transaction											x						x	

Table 2: Security Objective Rationale

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 threat *T.EvadTD Evading Transaction Data* is mitigated by:

– The security objective for the TOE O.GenLM requiring the TSF to create *transaction logs* containing *transaction data* and a *transaction number* generated by the TSF, and time stamps and digital signatures, therefore allowing to decide whether presented transaction data have a corresponding transaction data set in the transaction data set sequence.

– The security objective for the TOE O.TEE requiring the TSF to test the presence and identity of the electronic record-keeping system connected to the TOE.

– The security objective for the operational environment OE.ERS requiring the taxpayer to use an electronic record-keeping system that provides completely and in real time all *transaction data* that are legally required for generation of *log messages* to the TOE.

– The security objective for the operational environment OE.SecOEnv requiring the operational environment to protect the communication between ERS and TOE against manipulation and perturbation.

The threat *T.ManipTD Manipulation of Transaction Data* is mitigated by:

– The security objective for the TOE O.TEE requiring the TSF to test the presence and identity of the CTSS interface component connected to the TOE,

– The security objective for the operational environment OE.ERS requiring the taxpayer to use an electronic record-keeping system that provides correctly, completely and in real time all transaction data that are legally required for generation of *log messages* to the TOE,

– The security objective for the operational environment OE.SMAERSPlatform requiring the operational environment to protect the TOE against manipulation and misuse.

The threat *T.ManipDTBS Manipulation of Data-To-Be-Signed-And-Time-Stamped* is mitigated by:

– The security objective for the TOE O.TEE requiring the TSF to test the presence and identity of the CSP connected to the TOE.

– In case of the platform architecture, the OE.CSPPlatform "CSP as Secure Platform of the TOE" requires the CSP to provide a secure execution environment. In case of the client-server architecture, the OE.SMAERSPlatform.

– The security objective for the operational environment OE.SecCommCSP "Secure communication between TOE and CSP" ensures the protection of the integrity of the communication between the TOE and the cryptographic service provider. The operational environment shall protect the integrity of the communication between the TOE and the cryptographic service provider. In case of the client-server architecture, the TOE and the CSP component are physically separated components. The integrity of the communication between the TOE and the CSP shall be protected by means of a trusted channel as provided by the CSP according to [PPC-CSP-TS-Au][PPC-CSP-TS-Au-CL][PPC-CSPLight-TS-Au-Cl] and by the TOE claiming the package *trusted channel* between the TOE and the CSP, cf. Chapter 7.

The threat *T.ManipLM Manipulation of Log messages* is countered by:

– The security objective for the TOE O.GenLM "Generation of Log messages" by means of digital signatures generated by the CSP, which allows to detect manipulation of transaction data sets according to OE.Transaction.

– The security objective for the TOE O.IAA requiring the TSF to authenticate administrators by means of a password.

– The security objective for the TOE O.TEE "Test of External Entities" requiring the TSF to test the presence and identity of the CSP connected to the TOE.

– The security objective for the TOE O.TST "Self-Test and Secure State" detects failure and prevents generation of transaction data sets if time source is not available or the test of the CSP fails.

– The security objectives for the operational environment OE.CSP "Cryptographic Service Provider Component" ensures the availability of a certified CSP for generation of time stamps and digital signatures, and the distribution of the certificate linked to the taxpayer for signature verification.

– The security objective for the operational environment OE.SecOEnv "Secure Operational Environment" protecting the communication between ERS and TOE.

The threat T.ManipLMS *Manipulation of a Log Message Sequence* is countered by:

– The security objective for the TOE O.GenLM "Generation of *Log Messages"* requiring the TSF to generate *log messages* containing *transaction data* imported from the electronic record-keeping system, requiring the TSF to generate time stamps whenever a transaction starts, is completed or aborted, and requiring the

TSF to create a *transaction number* and a digital signature of the *transaction data* using the digital signature-creation service of the cryptographic service provider.

– The security objective for the TOE O.ImpExp “Import of *Transaction Data* from and Export of *Log Message* to CTSS Interface Component“ requiring the TSF to import *transaction data* from the electronic record-keeping system through the CTSS interface component and to export *log messages* to the CTSS interface component.

– The security objective for the TOE O.TEE “Test of External Entities” requiring the TSF to test the availability of the CTSS interface component and CSP connected to the TOE.

– The security objective for the operational environment OE.SecOEnv “Secure Operational Environment” protecting the communication between ERS and TOE.

The threat *T.ManipTN Manipulation of Transaction Number* is countered by the security objectives for the TOE O.SecMan TSF preventing management of *transaction number* generation.

The threat *T.FaUpD Faulty Update Code Package* is countered by:

– The security objectives for the TOE O.ImpExpUCP “Secure Import and Export of User Data” ensuring that user data are exported and imported after successful update process.

– The security objective for the TOE O.TST “Self-Test and Secure State” ensuring a correctly increased version number after installation of an update code package..

– The security objective for the operational environment OE.SUCP ensures that the authentic *update code package*s are signed and distributed with security attributes.

– The OE.SecUCP “Secure download and authorized use of *Update Code Package”* ensures that only authentic UCPs are installed.

– The OE.SMAERSPlatform ensures verifying the UCP.

The organizational security policy *OSP.SecERS Secure use of the electronic record-keeping system* is directly enforced by:

– The security objective for the TOE O.TEE requiring the TSF to test the presence and identity of the ERS as an external entity.

– The security objective for the operational environment OE.ERS “Trustworthy Electronic Record-Keeping System”.

– The security objective for the operational environment OE.SecOEnv “Secure Operational Environment” protecting the communication of ERS and TOE.

The organizational security policy *OSP.CertSecDev Certified Security Device* is directly enforced by the security objectives for the operational environment OE.CSP “Cryptographic Service Provider Component” and the certification conformant to this protection profile.

The organizational security policy *OSP.ProtDev Protection of ERS and Security Module* is directly ensured by the security objective for the operational environment OE.SecOEnv “Secure Operational Environment”.

The organizational security policy *OSP.ValidTrans Validation of transactions* is enforced by the security objectives for the TOE

– the security objective for the TOE O.GenLM “Generation of *Log messages”* requiring the TSF to generate *log messages* containing *transaction data* imported from the electronic record-keeping system, to generate time stamps whenever a transaction starts, is completed or aborted, and to generate *a transaction number* and a digital signature of the *transaction data* created using the digital signature-creation service of the cryptographic service provider,

– the security objectives for the TOE O.IAA “Authentication of Administrators” requiring the TSF to authenticate administrators by means of a password,

– the security objective for the TOE O.ImpExp “Import of *Transaction Data* from and Export of *Log Message* to CTSS Interface Component” requiring the TSF to import *transaction data* from the electronic record-keeping system through the CTSS interface component and to export *log messages* to the CTSS interface component.
– the security objective for the TOE O.SecMan “Security Management” preventing manipulation of the *transaction number*s and limiting the authorized manipulation of the time source to administrators.
– The security objective for the operational environment OE.Transaction “Verification of Transaction” ensures the condition for verification of the digital signature of the transaction data set.

The organizational security policy *OSP.Update Authorized Update Code Packages* is implemented by the security objective for the operational environment OE.SUCP “Signed *Update Code Package*s” ensuring a digital signature of a secure *update code package* together with its security attributes and the security objectives for the operational environment OE.SecUCP “Secure Download and Authorized Use of *Update Code Package*” ensuring the verification of the digital signature.

The assumption *A.CSP Cryptographic service provider* is directly implemented by the security objective for the operational environment OE.CSP ”Cryptographic service provider component”.

The assumption *A.SMAERSPlatform* is directly implemented by the security objective for the operational environment OE.SMAERSPlatform that requires secure storage of sensitive objects.

The assumption *A.ProtComCSP Protection of Communication between TOE and CSP* is directly implemented by the security objectives for the operational environment OE.SecCommCSP which requires the protection of the communication between the TOE and the CSP. In case of the platform architecture, the OE.CSPPlatform requires the CSP to provide a secure execution environment. In case of the client-server architecture, the TOE and the CSP component are physically separated components. The integrity of the communication between the TOE and the CSP shall then be protected by means of a trusted channel as provided by the CSP according to [PPC-CSP-TS-Au], [PPC-CSP-TS-Au-Cl], or [PPC-CSPLight-TS-Au-Cl] and by the TOE claiming the package *trusted channel*, cf. Chapter 7.

The assumption *A.ProtComERS Protection of Communication between TOE and Electronic Record-Keeping System* is directly implemented by the security objective for the operational environment OE.SecOEnv “Secure Operational Environment” protecting the integrity of the communication between the electronic record-keeping system and the TOE.

The assumption *A.VerifLMS Verification of Log Message Sequences* is directly implemented by the security objective for the operational environment OE.Transaction “Verification of Log message Sequences”.

The assumption *A.Admin Trustworthy Administrator* is directly implemented by the security objective for the operational environment OE.SecOEnv “Secure Operational Environment”.

5 Extended Component Definition

The extended components FIA_API.1 and FCS_RNG.1 are used only in the package package *trusted channel* between TOE and CSP, cf. Chapter 7.

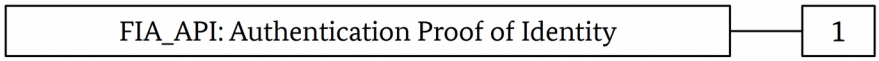
5.1 Authentication Proof of Identity (FIA_API)

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

Family Behaviour

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

Component Levelling:



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

Management: FIA_API.1

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

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

Audit: FIA_API.1

There are no auditable events foreseen.

FIA_API.1 Authentication Proof of Identity

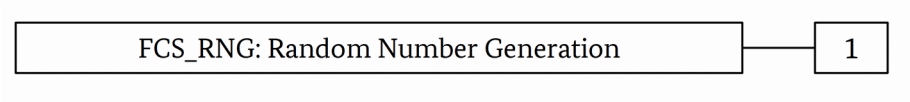
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *object, authorized user or role*] to an external entity.

5.2 Generation of Random Numbers (FCS_RNG)

Family Behaviour

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

Component Levelling:



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

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no auditable events foreseen.

FCS_RNG.1 Random number generation

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

6 Security Requirements

Common Criteria allows several operations to be performed on functional and assurance requirements: *refinement*, *selection*, *assignment*, and *iteration.* Each of these operations is used in this PP.
The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security and assurance requirements is (i) denoted by the word "refinement" in **bold** text and the added/changed words are in bold text, or (ii) directly included in the requirement text as **bold** text. In cases where words from a CC requirement component were deleted, these words are ~~crossed out~~.
The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as *italic* text and the original text of the component is given by a footnote. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicized*.
The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as *italic* text and the original text of the component is given by a footnote. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are *italicized*.
The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/" and the iteration indicator after the component identifier.

6.1 Security Functional Requirements

6.1.1 Security Management

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, administrator, CTSS interface role and CSP role [assignment: other roles]*[2].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

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 (cf. FMT_MOF.1)*, (2) *management of authentication reference data (cf. FMT_MTD.1/AD, FMT_MTD.3/PW),* (3) *management of security attributes (cf. FMT_MTD.3/PW, FMT_MSA.3, FMT_MSA.4),* (4) *[assignment: list additional of security management functions to be provided by the TSF]*[3].

2 [assignment: *authorised identified roles*]

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

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 and disable*[4] the function~~s~~ *password authentication according to FIA_UAU.5.2, clause (2) if defined*[5] to *administrator*[6],

(2) d*etermine the behaviour of and modify the behaviour of*[7] the function *FDP_ACF.1/LM by definition of a life time limit of ongoing transactions after which the transaction is terminated by the TSF*[8] to *administrator*[9],

(3) d*etermine the behaviour of* [10] the function *FPT_TEE.1 by definition of the identity and features to be tested of ERS*[11] to *administrator*[12],

(4) d*etermine the behaviour of* [13] the function *FPT_TEE.1 by definition of the identity and features to be tested of CSP*[14] to *administrator*[15],

(5) d*etermine the behaviour of and modify the behaviour of*[16] the function *FPT_TEE.1 in case the test of CTSS interface component or CSP fails*[17] to *administrator*[18],

(6) *determine the behaviour of and modify the behaviour of*[19] the functions *select the auditable events according to FAU_GEN.1/SYS*[20] to *administrator*[21],

(7) *determine the behaviour of and modify the behaviour of*[22] the functions *automatic export of audit trails according to FAU_STG.3.1/SYS clause (1)*[23] to *administrator*[24]

Application note 5: The refinements of FMT_MOF.1, bullet (2) to (7) are made in order to avoid iterations of the component. The life time of a transaction starts with receiving the *transaction data* with *type of operation* being *StartTransaction*.

4 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
5 [assignment: *list of functions*]
6 [assignment: *the authorised identified roles*]
7 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
8 [assignment: *list of functions*]
9 [assignment: *the authorised identified roles*]
10 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
11 [assignment: *list of functions*]
12 [assignment: *the authorised identified roles*]
13 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
14 [assignment: *list of functions*]
15 [assignment: *the authorised identified roles*]
16 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
17 [assignment: *list of functions*]
18 [assignment: *the authorised identified roles*]
19 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
20 [assignment: *list of functions*]
21 [assignment: *the authorised identified roles*]
22 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
23 [assignment: *list of functions*]
24 [assignment: *the authorised identified roles*]

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the *log message SFP and update SFP*[25] to restrict the ability to

(1) *define the set of accepted values of*[26] the security attributes *"clientID"*[27] to *CTSS interface role*[28],

(2) define depending on the clientID[29] the identity of the signature-creation key (keyID) to be used for the transaction log[30] to CTSS interface role[31],

(3) *define*[32] the *identity of the signature-creation key (keyID) to be used for the system log and audit logs* [33] to *CTSS interface role*[34],

(4) *increase by 1*[35] the *internally stored security attribute "transaction number" whenever a transaction is started*[36] to *subjects in CTSS interface role*[37],

(5 *modify*[38] the *TD security attribute "transaction number" imported from the TD*[39] to *none*[40],

(6) *increase*[41] the security attribute *"version number" of UCP*[42] *after successful installation* to *CSP role*[43].

Application note 6: The refinements of FMT_MSA.1 are made in order to avoid iteration of the component.

25 [assignment: *access control SFP(s), information flow control SFP(s)*]

26 [selection: *change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes]*]

27 [assignment: *list of security attributes*]

28 [assignment: t*he authorised identified roles*]

29 [selection: *change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes]*]

30 [assignment: *list of security attributes*]

31 [assignment: t*he authorised identified roles*]

32 [selection: *change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes]*]

33 [assignment: *list of security attributes*]

34 [assignment: t*he authorised identified roles*]

35 [selection: *change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes*]

36 [assignment: *list of security attributes*]

37 [assignment: t*he authorised identified roles*]

38 [selection: *change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes*]

39 [assignment: *list of security attributes*]

40 [assignment: t*he authorised identified roles*]

41 [selection: *change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes]*]

42 [assignment: *list of security attributes*]

43 [assignment: t*he authorised identified roles*]

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

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

FMT_MSA.3.1 The TSF shall enforce the *log message SFP and update SFP*[44] to provide *restrictive*[45] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *none*[46] to specify alternative initial values to override the default values when an object or information is created.

6.1.2 User Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

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

(1) *identity*,

(2) *authentication reference data,*

(3) *role*[47]

and

(a) security attribute *identity* [assignment: *additional security attributes*] belonging to the ERS

(b) security attribute *identity* [assignment: *additional security attributes*] belonging to the CSP.[48]

Application note 7: The refinements distinguish between the sets of security attributes maintained for authenticated users by an administrator, and the tested users ERS and CSP according to FTP_TEE.1. The security attributes are defined for users by the administrator according to FMT_MSA.1.

FMT_MTD.1/AD Management of TSF data - Authentication data

Hierarchical to: No other components.

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

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

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

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

46 [assignment: *the authorised identified roles*]

47 [assignment: *list of security attributes*]

48 [assignment: *list of security attributes*]

(1) *delete and create*[49] [50] the *authentication data record of all authorized users*[51] to *administrator*[52].

(2) ***modify***[53] **the *authentication reference data***[54] **to *the corresponding authorized user***[55].

FMT_MTD.3/PW Secure TSF data - Password

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data

FMT_MTD.3.1/PW The TSF shall ensure that only secure values are accepted for *passwords*[56] **and enforce changing initial passwords after first successful authentication of a user to a different secure operational password**.

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: *positive integer number*], *an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

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

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

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

(1) *identity*,

(2) *role*[57].

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*[58].

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:

49 "create" denotes initial creation and setting a new value in case a user forgot/lost their authentication data

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

51 [assignment: *list of TSF data*]

52 [assignment: *the authorised identified roles*]

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

54 [assignment: *list of TSF data*]

55 [assignment: *the authorised identified roles*]

56 [assignment: list of TSF data]

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

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

(1) *A subject is associated with attribute 'identity' and 'CTSS interface role' after the ERS is successfully tested according to FPT_TEE.1.*

(2) *A subject is associated with attribute 'identity' and 'CSP role' after the CSP is successfully tested according to FPT_TEE.1.*

(3) *A subject is associated with attribute 'identity' and 'administrator' role after successful authentication.*[59]

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow *self test according to FPT_TST.1* on behalf of the user to be performed before the user is identified.

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

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow

(1) *self test according to FPT_TST.1*,

(2) *testing of external entity ERS according to FPT_TEE.1 and starting the subject CTSS interface component if testing was successful and the role CTSS interface component is activated,*

(3) *testing of external entity CSP according to FPT_TEE.1 and start the subject* CSP *if testing was successful,*

(4) [assignment: *list of other TSF mediated actions*][60]

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

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide *password authentication*[61] to support user authentication.

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

(1) *password authentication shall be used for an administrator,*

(2) *[assignment: additional rules describing how the multiple authentication mechanisms provide authentication*][62].

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

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

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

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

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 *power on or reset*[63].

6.1.3 User data protection

FDP_ACC.1/LM Subset access control – Access to Logging

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/LM The TSF shall enforce the *log Message SFP*[64] on

(1) *subjects:*

(a) subject acting for CTSS interface component,

(b) subject acting for CSP;

(2) *objects:*

(a) transaction data,

(b) audit record,

(c) data-to-be-signed,

(d) protocolData with signature,

(e) log message,

(f) commands;

(3) *operations:*

(a) import,

(b) export[65].

FDP_ACF.1/LM Security attribute based access control – Access to TDS

Hierarchical to: No other components.

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

FDP_ACF.1.1/LM The TSF shall enforce the *log Message SFP*[66] to objects based on the following:

(1) *subjects:*

(a) *subject in CTSS interface role with security attribute activated or deactivated.*

(b) subject in CSP role;

(2) *objects:*

(a) transaction data,

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

64 [assignment: *access control SFP*]

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

66 [assignment: *access control SFP*]

(b) audit record,

(c) data-to-be-signed,

(d) protocolData with signature,

(e) log message

(f) commands[67].

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

(1) *A subject in activated CTSS interface role is allowed to*

(a) import the transaction data from the CTSS interface component according to FDP_ITC.2/TD,

(b) import commands from activated CTSS interface component,

(c) export the DTBS of transaction log and system log to the CSP according to FDP_ETC.2/DTBS,

(d) import the protocolData with signature from the CSP according to FDP_ITC.2/TSS,

(e) export the transaction log and system log to the CTSS interface component according to FDP_ETC.2/LM.

(2) *A subject in activated CTSS interface role is allowed to terminate the transaction after time limit defined according to FMT_MOF.1.1 clause (2) is reached.*

(3) *A subject in CSP role is allowed to import audit records from the CSP according to FDP_ITC.2/TSS and to export audit logs to the CTSS interface component according to FDP_ETC.2/LM*[68].

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

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

(1) a *user in other role than CTSS interface role is not allowed to perform actions listed in FDP_ACF.1.2/LM clause (1) and (2).*

(2) a *user in other role than CSP role is not allowed to perform actions listed in FDP_ACF.1.2/LM clause (3).*[69]

FDP_ITC.2/TD Import of user data with security attributes – Transaction 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

67 [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

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

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

FDP_ITC.2.1/TD The TSF shall enforce the *log message SFP*[70] when importing ~~user data~~ **transaction data** controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/TD The TSF shall use the security attributes associated with the imported ~~user data~~ **transaction data**.

FDP_ITC.2.3/TD The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the ~~user data~~ **transaction data** received.

FDP_ITC.2.4/TD The TSF shall ensure that interpretation of the security attributes of the imported ~~user data~~ **transaction data** is as intended by the source of the user data.

FDP_ITC.2.5/TD The TSF shall enforce the following rules when importing ~~user data~~ **transaction data** controlled under the SFP from outside of the TOE:

(1) *The TSF shall import the transaction data with the security attribute clientID if the clientID is in the set of accepted values according to FMT_MSA.1. If the clientID is not in the set of accepted values the TSF must not import the transaction data.*

(2) *The TSF shall import the transaction data with the security attribute 'type of the operation'.*

(3) *The transaction data shall be imported with the security attribute 'transaction number' if the 'type of the operation' is UpdateTransaction or FinishTransaction, and the transaction number meets a transaction number of an ongoing transaction.*

(4) *The TSF shall import audit records from the CSP.*[71]

FDP_ETC.2/DTBS 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/DTBS The TSF shall enforce the *log message SFP*[72] when exporting ~~user data~~ **data-to-be-signed**, controlled under the SFP(s), ~~outside of the TOE~~ **to the CSP**.

FDP_ETC.2.2/DTBS The TSF shall export the user data with the ~~user data's associated~~ security attributes **associated with the data-to-be-signed**.

FDP_ETC.2.3/DTBS The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported ~~user data~~ **data-to-be-signed**.

FDP_ETC.2.4/DTBS The TSF shall enforce the following rules when user data is exported from the TOE:

(1) *Data-to-be-signed shall be exported for generation of a log message with a security attribute identifying the private signature key to be used by FDP_DAU.2/TS according to [PPC-CSP-TS-Au][PPC-CSP-TS-Au-Cl][PPC-CSPLight-TS-Au-Cl].*[73]

FDP_ITC.2/TSS Import of user data with security attributes – Time stamp and signature

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]

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

71 [assignment: *additional importation control rules*]

72 [assignment: *access control SFP*]

73 [assignment: *additional exportation control rules*]

FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2.1/TSS The TSF shall enforce the *log message SFP*[74] when importing ~~user data~~ **protocolData with signature and audit records**, controlled under the SFP, from ~~outside of the TOE~~ **the CSP**.

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

FDP_ITC.2.3/TSS The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the ~~user data~~ **protocolData with signature and audit records** received.

FDP_ITC.2.4/TSS The TSF shall ensure that interpretation of the security attributes of the imported ~~user data~~ **protocolData with signature and audit records** is as intended by the source of the user data.

FDP_ITC.2.5/TSS The TSF shall enforce the following rules when importing ~~user data~~ **protocolData with signature and audit records** controlled under the SFP from ~~outside of the TOE~~ **the CSP** [assignment: *additional importation control rules*].

Application note 8: The CSP shall generate and return to the TOE at least the signature counter of the used signature-creation key, the time stamp and the signatures for the *data-to-be-signed* exported by the TOE according to FDP_ETC.2/DTBS. The CSP shall generate time stamps according to FDP_DAU.2/TS using a time source according to FPT_STM.1, cf. [PPC-CSP-TS-Au][PPC-CSP-TS-Au-Cl][PPC-CSPLight-TS-Au-Cl]. Note, the TOE of this protection profile may use the CSP to provide time stamps by an administrator settable internal clock; cf. selection clause (4) in FPT_STM.1.1. If the CSP meets [TR SE] for the *transaction logs,* then the CSP returns a *log message* to the TOE. If the CSP generates the time stamp and signatures with a signature counter, then the TOE shall compile the *log message* according to [TR TSEA]. The signature counter and the time stamp of *transaction logs* and of audit data received as audit logs may be used to test the CSP according to FPT_TEE.1.

FDP_ETC.2/LM Export of user data with security attributes – Log messages

Hierarchical to: No other components.

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

FDP_ETC.2.1/LM The TSF shall enforce the *log message SFP*[75] when exporting user data **log message**, controlled under the SFP(s), ~~outside of the TOE~~ **to CTSS interface component**.

FDP_ETC.2.2/LM The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3/LM 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/LM The TSF shall enforce the following rules when user data is exported from the TOE: *Log messages shall be exported with security attribute*

(1) transaction logs:

(a) transaction number of the transaction identifying the log messages which belongs to the transaction,

(b) signature counter of the private signature key used by FDP_DAU.2/TS according to [PPC-CSP-TS-Au][PPC-CSP-TS-Au-Cl][PPC-CSPLight-TS-Au-Cl] enumerating all log messages,

(c) type of the operation,

(d) time stamp when the log message was signed,

(e) keyID as hash value of the public key for verification of the signature,

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

75 [assignment: *access control SFP*]

(f) signature for verification of the authenticity of the certified data and protocol data.

(2) system logs:

(a) type of the operation or TSF security event

(b) signature counter of the private signature key used by FDP_DAU.2/TS according to [PPC-CSP-TS-Au][PPC-CSP-TS-Au-Cl][PPC-CSPLight-TS-Au-Cl] enumerating all log messages,

(c) time stamp when the log message was signed,

(d) keyID as hash value of the public key for verification of the signature,

(e) signature for verification of the authenticity of the certified data and protocol data.

(3) audit records of the CSP shall be exported unchanged as audit logs to the CTSS interface component.[76]

Application note 9: The CTSS interface component does not implement any security functionality addressed in this PP and imports and stores log message received from the TOE as user data.

FPT_TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret

(1) *clientID*,

(2) *type of the operation,*

(3) *transaction number,*

(4) *signature counter,*

(5) *time stamp,*

(6) *keyID as hash value of the public key,*

(7) *signature*[77]

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use *[TR SE] and [TR TSEA]*[78] when interpreting the TSF data from another trusted IT product.

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

(1) *transaction numbers building a strong increasing sequence without gaps,*

76 [assignment: *additional exportation control rules*]

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

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

(2) *Time stamps of the log messages building a non-decreasing sequence with consideration of adjustments of the CSP's time source*[79].

Application note 10: The rules may be enforced by internally storing of the *transaction Number* and last time stamp provided by the CSP in the log messages.

FMT_MSA.4 Security attribute value inheritance

Hierarchical to: No other components.

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

FMT_MSA.4.1 The TSF shall use the following rules to set the value of security attributes:

(1) T*he TSF uses the security attribute clientID imported with transaction data to determine the signature-creation key that is used by FDP_DAU.2/TS with ECDSA in [PPC-CSP-TS-Au][PPC-CSP-TS-Au-Cl][PPC-CSPLight-TS-Au-Cl] to sign the corresponding log message as defined according to FMT_MSA.1.*

(2) *If the type of the operation of imported transaction data is StartTransaction, then the last internally generated transaction number of the respective keyID shall be increased by 1, and this value shall be assigned to the ongoing transaction and the transaction log of imported transaction data.*

(3) *If the type of the operation of imported transaction data is UpdateTransaction or FinishTransaction and meets the transaction number of an ongoing transaction, then the transaction number of the imported transaction data shall be assigned to the protocol data of the transaction log.*[80]

6.1.4 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 according to FPT_TST.1 fails,*

(2) *test of ERS according to FPT_TEE.1 fails,*

(3) *test of CSP according to FPT_TEE.1 fails*[81].

The TSF shall exit the secure state only if the self-test, the test of the ERS and the test of the CSP are passed.

Application note 11: The self-test according to FPT_TST.1 and test of external entities according to FPT_TEE.1 cause the TOE to enter a secure state if the self-test or the tests of the ERS or CSP fail. The exit of the secure state requires all conditions listed in the refinement being fulfilled.

FPT_TEE.1 Testing of external entities

Hierarchical to: No other components.

Dependencies: No dependencies.

79 [assignment: *list of security attributes*]

80 [assignment: *rules for setting the values of security attributes*]

81 [assignment: *list of types of failures in the TSF*]

FPT_TEE.1.1 The TSF shall run a suite of tests *during start-up, periodically during normal operation, user initiated shutdown and before exiting the secure state according to FPT_FLS.1*[82] to check the fulfillment of

(1) ERS identity [assignment: list of properties of the ERS] and

(2) CSP identity [assignment: list of properties of the CSP][83].

The tests include the identification of the TOE to the tested device.

FPT_TEE.1.2 If the test fails, the TSF shall *enter the secure state according to FPT_FLS.1 [selection: none additional action, [assignment: additional action(s)]]*[84].

Application note 12: The administrator may by able to define the actions in FPT_TEE.1 according to FMT_MOF.1.1 (5). In case of a failure, additional actions may e.g. include reading the stored audit logs. The suite of tests determine whether the configured CSP is available for the TOE and log messages can be signed. The TOE may use the signature counter and time stamps received from the CSP to test it. The signature counter shall increase strong monotonically without gaps because any gap may indicate unauthorized signature-creation. The tests of the CSP should allow the CSP to identify the TOE as user of the CSP, cf. FIA_UID.1.1 clause (2) in [PP CSP][PP CSPLight]. Please refer for further explanations to the user notes and evaluator notes in CC part 2 [CCP2], Chapter J.12.

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, at the request of the authorised user, periodically during normal operation and before exiting the secure state according to FPT_FLS.1*[85] to demonstrate the correct operation of *parts of TSF*[86].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of *TSF data*[87].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of *TSF* ***implementation***[88].

Application note 13: The security attribute “version number” of the UCP is part of the TSF data. During TSF testing, the consistency of the version number has to be checked to detect upgrades or attempted downgrades of the installed code of the TOE. In case of a detected change of the version number, the TOE must follow the UCP SFP and log the events according to FAU_GEN.1/SYS.

6.1.5 Security Audit

FAU_GEN.1/SYS Audit data generation – System Log

Hierarchical to: No other components.

82 [selection: *during initial start-up, periodically during normal operation, at the request of an authorised user, [assignment: other conditions]*]

83 [assignment: *list of properties of the external entities*]

84 [assignment: *action(s)*]

85 [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions[assignment: conditions under which self test should occur]*]

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

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

88 [selection: [assignment: parts of TSF], TSF]

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1/SYS 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*[89] level of audit; and

c) *other auditable events*

(1) system operation commands as specified in [TR SE], Appendix A,

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

(3) failure with preservation of secure state (FPT_FLS.1): entering and exiting secure state,

(4) setting of the version number of the UCP and upgrade of stored data,

(5)[assignment: additional specifically defined auditable events][90]

FAU_GEN.1.2/SYS 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, [assignment: *other audit relevant information*].

Application note 14: The security relevant events that have to be logged according to FAU_GEN.1/SYS are part of the system log.

FMT_MTD.1/SYSCTSS Management of TSF data – System log – CTSS Interface Component

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

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

(1) *manual export,*

(2) *clear after manual export,*

the *system logs*[91] to *CTSS Interface Component*[92].

FMT_MTD.1/SYSAdmin Management of TSF data – System log -Administrator

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

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

(1) *select audited events in FAU_GEN.1/SYS,*

(2) *define the number of audit records causing automatic export and clearing of exported audit records according to FAU_STG.3.1/SYS clause (1),*

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

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

91 [assignment: *list of TSF data*]

92 [assignment: *the authorised identified roles*]

(3) *define the percentage of storage capacity of audit records if actions are assigned in FAU_STG.3.1/SYS clause (2)*[93]

the *system logs*[94] to *Administrator*[95].

FAU_STG.1/SYS Protected audit trail storage – System log

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

FAU_STG.1.2/SYS The TSF shall be able to *prevent*[96] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.3/SYS Action in Case of Possible Audit Data Loss – System log

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1/SYS The TSF shall

(1) *automatically export audit trails and clear automatically exported audit records*[97] if the audit trail exceeds *an Administrator defined number of audit records within [assignment: pre-defined range]*[98]

(2) ***[assignment: actions to be taken in case of possible audit storage failure]*** **if the audit trail exceeds an *Administrator settable percentage of storage capacity*[99]**.

Application note 15: The ST writer shall perform the open operations in FAU_STG.3.1/SYS 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).

Application note 16: The automatic export shall prevent loss of internal audit data due to storage constraints, by protecting the audit data and storing the signed and timestamped data in the CTSS interface component, i.e. outside the TOE.

6.1.6 Update Code Package

FDP_ACC.1/UCP Subset access control – Use of *Update Code Package*

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/UCP The TSF shall enforce the *update SFP*[100] on

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

94 [assignment: *list of TSF data*]

95 [assignment: *the authorised identified roles*]

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

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

98 [assignment: *pre-defined limit*]

99 [assignment: *pre-defined limit*]

100 [assignment: *access control SFP*]

(1) *subjects: CSP role;*

(2) *objects: stored data*;

(3) *operations: upgrade*[101].

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

Hierarchical to: No other components.

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

FDP_ACF.1.1/UCP The TSF shall enforce the *Update SFP*[102] to objects based on the following:

(1) *subjects: CSP role;*

(2) *objects: update code package with security attributes version number*[103].

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) *CSP role is allowed to upgrade the stored data if*

(a) the digital signature of the UCP generated by the issuer is successfully verified by the SMAERS platform.[104]

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

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

(1) a *CSP role is not allowed to upgrade the stored data if the verification of digital signature of the UCP by means of the SMAERS platform fails*;

(2) [*assignment: other rules, based on security attributes, that explicitly deny access of subjects to objects*].[105]

Application note 17: The CSP role should be allowed to apply the stored *update code package* if the version number of the *update code package* is higher than the version number of the TSF. The execution of UCP is outside the TSF-mediated functionality of the PP on hand.

FDP_ETC.2/UCP_UD Export 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]

FDP_ETC.2.1/UCP_UD The TSF shall enforce the *log message SFP*[106] when exporting user data, controlled under the SFP(s), ~~outside of the TOE~~ **to the storage of the platform**.

FDP_ETC.2.2/ UCP_UD The TSF shall export the user data with the user data's associated security attributes.

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

102 [assignment: *access control SFP*]

103 [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

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

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

106 [assignment: *access control SFP*]

FDP_ETC.2.3/ UCP_UD 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/ UCP_UD The TSF shall enforce the following rules when user data is exported from the TOE: [assignment: *additional exportation control rules*]

FDP_ITC.2/UCP_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/UCP_UD The TSF shall enforce the *update SFP*[107] when importing user data, controlled under the SFP, from ~~outside of the TOE~~ **the storage of the platform**.

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

FDP_ITC.2.3/UCP_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/UCP_UD The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/UCP_UD The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *additional importation control rules*]**.**

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 successful upgrade of the stored data***[108] the following objects: *previous code and data*[109].

6.2 Security Assurance Requirements

The PP requires the TOE to be evaluated according to EAL2 augmented with ALC_CMS.3 (Implementation representation CM coverage) and ALC_LCD.1 (Developer-Defined Lifecycle Model), and with specific refinements on ALC_CMS.3, ADV_ARC.1 and ATE_IND.2.

6.2.1 Assurance Refinements

Refinement on ALC_CMS.3.1C:

The implementation representation listed shall comprise the implementation representation of the TOE defining the TSF to a level of detail such that the compliance of the TOE and TSF to the requirements

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

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

109 [assignment: *list of objects*]

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 and software 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..

6.3 Security Requirements Rationale

6.3.1 Dependency Rationale

This chapter demonstrates that each dependency of the security requirements defined in Chapter 6.1 is either satisfied, or justifies the dependency not being satisfied.

SFR	Dependencies of the SFR	SFR components
FAU_GEN.1/SYS	FPT_STM.1 Reliable time stamps	FPT_STM.1 provided by the CSP PP Module Time Stamp Service and Audit
FAU_STG.1/SYS	FAU_GEN.1 Audit data generation	FAU_GEN.1/SYS
FAU_STG.3/SYS	FAU_STG.1 Protected audit trail storage	FAU_STG.1/SYS
FDP_ACC.1/LM	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/LM
FDP_ACC.1/UCP	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/UCP
FDP_ACF.1/LM	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/LM, FMT_MSA.3
FDP_ACF.1/UCP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/UCP, FMT_MSA.3
FDP_ETC.2/DTBS	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/LM
FDP_ETC.2/LM	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/LM
FDP_ETC.2/UCP_UD	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/UCP
FDP_ITC.2/TD	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/LM Dependency on FTP_ITC.1 or FPT_TRP.1 is not fulfilled because secure import is ensured by OE.SecOEnv. FPT_TDC.1
FDP_ITC.2/TSS	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/LM Dependency on FTP_ITC.1 or FPT_TRP.1 is not fulfilled because secure import is ensured by OE.SecCommCSP in case of the platform-architecture. In case of the client-server architecture FTP_ITC.1 is fulfilled, cf. Chapter 7 (FTP_ITC.1/TC).

SFR	Dependencies of the SFR	SFR components
FDP_ITC.2/UCP_UD	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/UCP, FTP_ITC.1 is not included for UCP transfer but FDP_ACC.1/UCP ensure integrity and confidentiality of UCP, FPT_TDC.1 is not included because the CSP uses the security attributes of UCP
FDP_RIP.1/UCP	No dependencies	
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_ATD.1	No dependencies	
FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.1
FIA_UAU.5	No dependencies	
FIA_UAU.6	No dependencies	
FIA_UID.1	No dependencies	
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1/LM, FDP_ACC.1/UCP FMT_SMR.1 FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FDP_ACC.1/LM, FDP_ACC.1/UCP, FMT_MSA.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1, FMT_SMR.1
FMT_MSA.4	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/LM
FMT_MTD.1/AD	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/SYSCTSS	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/SYSAdmin	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MTD.3/PW	FMT_MTD.1 Management of TSF data	FMT_MTD.1/AD

SFR	Dependencies of the SFR	SFR components
FMT_SMF.1	No dependencies	
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.1
FPT_TDC.1	No dependencies	
FPT_FLS.1	No dependencies	
FPT_TEE.1	No dependencies	
FPT_TST.1	No dependencies	

Table 3: Dependency Rationale

6.3.2 Security Functional Requirements Rationale

The tables trace each SFR defined in Chapter 6.1 back to the security objectives for the TOE.

	O.GenLM	O.ImpExp	O.IAA	O.SecMan	O.TEE	O.TST	O.ImpExpUCP
FAU_GEN.1/SYS	x						
FAU_STG.1/SYS	x						
FAU_STG.3/SYS	x						
FDP_ACC.1/LM	x	x					
FDP_ACC.1/UCP						x	
FDP_ACF.1/LM	x	x					
FDP_ACF.1/UCP						x	
FDP_ETC.2/DTBS	x						
FDP_ETC.2/LM		x					
FDP_ITC.2/TSS	x						
FDP_ITC.2/TD	x	x					
FDP_ITC.2/UCP_UD						x	x
FDP_ETC.2/UCP_UD						x	x
FDP_RIP.1/UCP						x	
FIA_AFL.1			x				
FIA_ATD.1			x		x		
FIA_UAU.1					x		
FIA_UAU.5			x				
FIA_UAU.6			x				
FIA_UID.1					x		

	O.GenLM	O.ImpExp	O.IAA	O.SecMan	O.TEE	O.TST	O.ImpExpUCP
FIA_USB.1			x				
FMT_MOF.1	x		x	x	x		
FMT_MSA.1	x			x	x		
FMT_MSA.2	x			x			
FMT_MSA.3	x			x			
FMT_MSA.4	x	x		x			
FMT_MTD.1/AD			x	x			
FMT_MTD.1/SYSCTSS	x						
FMT_MTD.1/SYSAdmin	x						
FMT_MTD.3/PW			x	x			
FMT_SMF.1	x	x		x			
FMT_SMR.1	x	x		x	x		
FPT_TDC.1	x	x					
FPT_FLS.1					x	x	
FPT_TEE.1					x	x	
FPT_TST.1						x	

Table 4: Security Functional Requirements Rationale

The following part of this chapter demonstrates that the SFRs meet all security objectives for the TOE.

The security objective for the TOE *O.GenLM Generation of Log Messages* is met by the following SFR:

– The SFR FDP_ACC.1/LM and FDP_ACF.1/LM require access control of import of TD and signatures, export of DTBS and log messages for roles defined by FMT_SMR.1.

– The SFR FDP_ITC.2/TD and FDP_ITC.2/TSS requires the TSF to import transaction data from CTSS interface component, audit records, time stamps, signature counter and signatures from CSP to generate log messages.

– The SFR FDP_ETC.2/DTBS requires the TSF to export data-to-be-signed to the CSP for time stamping and signature generation.

– The SFR FMT_MSA.1, clause (3) prevents the manipulation of the *transaction number*.

– The SFR FMT_MSA.2 ensures that the security attributes of a *log message* are generated in a way that the log message builds a valid transaction.

– The SFR FMT_MSA.3 ensures restrictive security attributes of *a log message* as defined, and prevents alternative initial values of the security attributes of a log message.

– The SFR FMT_MSA.4 describes the generation of security attributes which are included in a *log message*.

– The SFR FMT_MOF.1 clause (2), describes the behaviour of FMT_MSA.4 for *keyID* in a log message.

– The SFR FMT_MOF.1, FMT_MTD.3/PW, FMT_MSA.3, FMT_MSA.4 defined for SFR FDP_ACC.1/LM and FDP_ACF.1/LM are listed in SFR FMT_SMF.1.
– The SFR FPT_TDC.1 ensures that the security attributes of the imported *transaction data* and of the exported *log messages* are correctly interpreted.
– The SFR FAU_GEN.1/SYS, FMT_MTD.1/SYSCTSS, FMT_MTD.1/SYSAdmin, FAU_STG.1/SYS, FAU_STG.3/SYS decribes the generation and management of system logs.
– The security objective for the TOE O.ImpExp *Import of Transaction Data from and Export of Log message to CTSS Interface Component* is met by the following SFR:
– The SFR FDP_ACC.1/LM and FDP_ACF.1/LM require access control on the import of *transaction data*; and export of *log messages* to the CTSS interface component for roles defined by FMT_SMR.1.
– The SFR FDP_ITC.2/TD requires the TSF to import *transaction data* with security attributes in order to determine the security attributes of *log messages* according to FMT_MSA.4.
– The SFR FDP_ETC.2/LM requires the export of *log messages* with security attributes defined by FMT_MSA.4 to the CTSS interface component for generation of receipts and verification of *log messages*.
– The SFR FPT_TDC.1 ensures that the security attributes imported with *transaction data* and exported with *log messages* are correctly interpreted.

The security objective for the TOE O.IAA *Authentication of Administrators* is met by the following SFR:

– Administrator and CSP are requested to authenticate themselves according to FIA_UAU.5.
– The SFR FIA_UAU.5 defines the authentication mechanisms supported by the TSF.
– The SFR FMT_MOF.1.1, clause (1) defines the rule that additional authentication (except for the administrator itself) may be enabled and disabled by an administrator.
– The SFR FIA_UAU.6 defines the condition for re-authentication.
– The SFR FIA_AFL.1 defines required actions if password authentication fails.
– The SFR FIA_ATD.1 defines the security attributes of users known to the TSF and the SFR FIA_USB.1 requires binding these security attributes to successfully authenticated users.
– The SFR FMT_MTD.1/AD and FMT_MTD.3/PW require the TSF to manage authentication data of users.

The security objective for the TOE *O.SecMan Security Management* is met by the following SFRs:

– The SFR FMT_SMR.1 defines the roles known to TSF and requires the TSF to associate users with these roles.
– The SFR FMT_SMF.1 lists the management functions as management of functions FMT_MOF.1, management of TSF data FMT_MTD.1/AD and FMT_MTD.3/PW, and management of security attributes FMT_MSA.1, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4.
– The SFR FMT_MOF.1 restricts the ability to modify, enable, disable, determine the behaviour of and modify the behaviour of security functions to an administrator.
– The SFR FMT_MTD.1/AD and FMT_MTD.3/PW requires the TSF to manage authentication data of users.
– The SFR FMT_MSA.1 and FMT_MSA.3 describes the requirements for restrictive security attributes and limits the management of security attributes for the SFP *Log Message and Update*.
– The SFR FMT_MSA.2 and FMT_MSA.4 define requirements for the generation of security attributes of TDSs and TDSSs including the security attribute *time stamp*.
– The SFR FMT_MSA.4 prevents management of the *transaction numbers*.

The security objective for the TOE O.TEE *Test of External Entities* is met directly by the SFR FPT_TEE.1. The SFR FMT_MOF.1, clause (5), restricts the definition and modification of the behaviour of FPT_TEE.1 to the administrator. The O.TEE *Test of External Entities* is furthermore met by the following SFRs:

– The SFR FMT_SMR.1 lists the roles known to the TSF, where subject CTSS interface component is automatically started and identified only.

– The SFR FIA_UID.1 defines the self-test as the only TSF mediated action allowed before users and subjects are identified.

– The SFR FIA_UAU.1 defines the TSF mediated action allowed before users and subjects are authenticated. The subject CTSS interface component is allowed to perform automatically TSF mediated actions according to FPT_TST.1 and FPT_TEE.1 before users are authenticated.

– The SFR FIA_ATD.1 defines the security attribute *identity* for the ERS and the CSP tested by FPT_TEE.1. If any test fails, the TSF enters a secure state according to FPT_FLS.1.

The security objective for the TOE O.TST *Self-Test* is met by the following SFRs:

– The SFR FPT_TST.1 requires the TSF to perform self-tests and FPT_FLS.1 requires the TSF to enter a secure state if one of the self-tests fails.

– The SFR FPT_FLS.1 requires the TSF to enter a secure state if the self-test fails, or the test of the electronic record-keeping system fails, or the test of cryptographic service provider fails.

– The SFR FPT_TEE.1 requires the TSF to enter the secure state according to FPT_FLS.1 if the test of the CTSS interface component or the CSP fails.

– The SFR FDP_ACC.1/UCP and FDP_ACF.1/UCP requires the TSF to provide access control to enforce the update SFP. The SFR FMT_MSA.1 prevents the modification of security attributes “version number” of the UCP.

– The SFR FDP_RIP.1/UCP requires the TSF to remove the received UCP after unsuccessful verification of its authenticity. The verification must be done by means of the platform.

The security objective for the TOE O.ImpExpUCP *Secure Import and Export of User Data* is directly *met by the* SFR FDP_ITC.2/UCP_UD and FDP_ETC.2/UCP_UD that requires the TSF to export and import user data during an update process.

6.3.3 Security Assurance Requirements Rationale

Developers and users require for the TOE a low to moderate level of independently assured security in the absence of ready availability of the complete development record.

EAL2 was chosen because it provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE to understand the security behaviour. The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis – based upon the functional specification, TOE design, security architecture description and guidance evidence provided – demonstrating resistance to penetration attackers with a basic attack potential. EAL2 also provides assurance through the use of a configuration management system and evidence of secure delivery procedures.

ALC_CMS.3 has been augmented to include the implementation representation as needed for ADV_ARC and ATE_IND refinements, and to get evidence that the implementation representation provided is the one of the TOE. This means that the implementation representation is part of the configuration list.

The security target shall describe the complete life cycle of the TOE, including details necessary for the understanding of the interaction with and configuration of the CSP. Hence, ALC_LCD.1 has been augmented such that the lifecycle of the TOE is defined by the developer and thus made explicit.

For getting confidence that the platform of the TOE (operational environment) is used by the TOE in a way that the requirements on security as outlined in the platform documentation (guidance documentation and if available evaluation or certification results) have been followed in the TOE design and implementation, refinements of ADV_ARC, ATE_IND and ALC_CMS have been defined.

The goal is to ensure that the TOE implementation does not include obvious vulnerabilities caused by incorrect use of the platform, and that all relevant platform guidance requirements are adhered to. Therefore, only those requirements have to be considered that are related to the TOE functionality and security claims of the security target of the TOE.

The refinement of ADV_ARC ensures that the developer outlines how she has considered the requirements from the platform within his TOE security architecture and design concept. The evaluators task is to check consistency of the requirements considered against those outlined in the platform documentation.

As a second step of verification that the relevant platform requirements have been considered correctly, the independent evaluator activity at ATE_IND has been refined. The evaluator has to perform a specific „source code review“, by means of cross checking the requirements from the platform to the implementation representation of the TOE by examining the implementation representation of the TOE using appropriate tools and the evidence from ADV_ARC.

7 Package Trusted Channel between TOE and CSP

This package defines security functional requirements for trusted channel support between the TOE and the CSP. The package is mandatory if the security module follows the client-server architecture, i.e. the TOE and the CSP are physically separated components and the operational environment cannot ensure the integrity of the communication between the TOE and the CSP; cf. OE.SecCommCSP. In this case, the TOE and the CSP shall communicate through a trusted channel – cf. [PP CSP][PP CSPLight] – protecting the integrity of the communication between the TOE and the CSP, and preventing misuse of the CSP's signing and time stamping service provided for the TOE.

The trusted channel is a specific means to meet the assumption *A.ProtComCSP Protection of Communication between TOE and CSP*. The CSP provides one end point of the trusted channel according to [PP CSP][PP CSPLight], Chapter 6.1.5, and implements its part of the security objectives for the operational environment OE.SecCommCSP. The TOE provides the other end point of the trusted channel. This specific part of the security objectives for the operational environment OE.SecCommCSP is replaced by the security objective O.SecCommCSP defined in this package (cf. CEM paragraph 409, clause c, first bullet point).

O.SecCommCSP Trusted channel between TOE and CSP
The TOE shall protect the integrity of the communication between the TOE and the cryptographic service provider by means of a trusted channel.

In the client-server architecture, the TOE uses as the application component (in client role) the security services of the CSP (in server role). The SFRs are specific for the TOE in the client role enforcing the usage of the trusted channel but requiring integrity protection only. The security target may require additional confidentiality protection as provided by the CSP.

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

elliptic curve	**key size**	**standard**
brainpoolP256r1	*256 bits*	*RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR03111]*
brainpoolP384r1,	*384 bits*	*RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR03111]*
brainpoolP512r1	*512 bits*	*RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR03111]*
Curve P-256	*256 bits*	*FIPS PUB 186-4 B.4 and D.1.2.3 [NIST 2013]*
Curve P-384	*384 bits*	*FIPS PUB 186-4 B.4 and D.1.2.4 [NIST 2013]*
Curve P-521	*521 bits*	*FIPS PUB 186-4 B.4 and D.1.2.5 [NIST 2013]*

Table 5: Elliptic Curves, Key sizes and Standards

To perform mutual authentication using the PACE protocol, both endpoints need to share a static secret (PACE Password). The integrity and confidentiality of the shared secret have to be preserved by the TOE, using the secure storage of its platform.

Asset	**Protection**
PACE password	integrity, confidentiality

Table 6: Additional assets in package Trusted Channel to be protected by the TOE

FTP_ITC.1/TC Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/TC The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **the CSP** that is ~~logically distinct from other communication channels~~ [**selection: *logically distinct from other communication channels, using physical separated ports***] and provides assured identification of its end points ***TOE and CSP*** and protection of the channel data from modification ~~or disclosure~~.

FTP_ITC.1.2/TC The TSF shall permit *the TSF*[110] to initiate communication via the trusted channel.

FTP_ITC.1.3/TC The TSF shall initiate communication via the trusted channel for *communication with the CSP*[111].

Application note 18: Protection against modification is required for the trusted channel. If sensitive data is transferred over the trusted channel, the ST writer shall provide additional cryptographic operations to protect the exchanged data against disclosure.

FIA_UAU.5/TC Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/TC The TSF shall provide

(1) *PACE with Generic Mapping with user in PCD role with establishment of a trusted channel according to FTP_ITC.1/TC,*

(2) [assignment: *other method of mutual authentication with key establishment*],

(3) *message authentication by MAC verification of received messages*[112]

to support user authentication.

FIA_UAU.5.2/TC The TSF shall authenticate any user's claimed identity according to ~~the~~

(1) *PACE may be used for authentication of a CSP with establishment of a trusted channel according to FTP_ITC.1/TC,*

(2) *message authentication by MAC verification of received messages shall be used after initial authentication of a remote entity according to clause (1) for a trusted channel according to FTP_ITC.1/TC*[113].

Application note 19: The ST writer may assign another method of mutual authentication with key establishment in FIA_UAU.5.1/TC clause (2) if this method is supported by the certified CSP and therefore meets the OSP.SecCryM *Secure Cryptographic Mechanisms* as defined in [PP CSP][PP CSPLight].

FIA_API.1 Authentication Proof of Identity – PACE Authentication to Application Component

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a *PACE in PCD role*[114] to prove the identity of the *TOE*[115] to ~~an external entity~~ **a CSP and establishing a trusted channel according to FTP_ITC.1/TC**.

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

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

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

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

114 [assignment: *authentication mechanism*]

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

FCS_CKM.1 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 The TSF shall generate cryptographic keys ***for FCS_COP.1*** in accordance with a specified cryptographic generation algorithm *PACE with [selection: elliptic curves in table 5] and Generic Mapping in PCD role*[116] and specified cryptographic key sizes *256 bits*[117] that meet the following: *[ICAO], Section 4.4*[118].

Application note 20: PACE is used to authenticate the TOE and the CSP. It establishes a trusted channel with MAC integrity protection of the following communication through the trusted channel.

FCS_CKM.4 Cryptographic Key Destruction

Hierarchical to: No other components.

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

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

FCS_COP.1 Cryptographic Operation

Hierarchical to: No other components.

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

FCS_COP.1.1 The TSF shall perform *MAC calculation and MAC verification*[119] in accordance with a specified cryptographic algorithm *according to AES-256* [*FIPS197] in [selection: CMAC (NIST SP800-38B [NIST2005]), GMAC (NIST SP800-38D[NIST2007]), HMAC (FIPS PUB 198-1 [NIST2008])]*[120] and cryptographic key sizes *256 bits*[121] that meet the following: *the referenced standards above according to the chosen selection*[122].

The following extended components are defined in [PP CSP][PP CSPLight] and are used here for the generation of ephemeral keys during the execution of PACE according to FCS_CKM.1.

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*][123] random number generator that implements: [assignment: *list of security capabilities*].

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

117 [assignment: *cryptographic key sizes*]

118 [assignment: *list of standards*]

119 [assignment: *list of cryptographic operations*]

120 [assignment: *cryptographic algorithm*]

121 [assignment: *cryptographic key sizes*]

122 [assignment: *list of standards*]

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

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

Application note 21: The TOE may use an internal source or an external source or more than one source of randomness providing seeds of at least 125 bits entropy. The deterministic part of the RNG shall meet [TR CryAS] and must therefore be of class DRG.3 or higher according to [AIS20].

The dependencies are fulfilled:

SFR	Dependencies of the SFR	SFR components
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 FCS_CKM.4,
FCS_RNG.1	No dependencies	
FIA_API.1	No dependencies	
FIA_UAU.5/TC	No dependencies	
FTP_ITC.1/TC	No dependencies	

Table 7: Dependency Rationale for the Functional Package

The security objective for the TOE O.SecCommCSP *Trusted Channel between TOE and CSP* is implemented by the SFR

- FTP_ITC.1/TC Inter-TSF trusted channel directly requiring the trusted channel between the TOE and the CSP protecting the integrity for their communication.
- FIA_UAU.5/TC requires the TSF to authentication the CSP as communication end point of the trusted channel.
- FIA_API.1 requires the TSF to authentication themselves as communication end point of the trusted channel to the CSP.
- FCS_CKM.1 requires the TSF to generate MAC keys for FCS_COP.1.
- FCS_CKM.4 requires secure key destruction in order to fulfill the dependency of FCS_CKM.1.
- FCS_COP.1 requires the TSF to calculate MAC for the own messages and to verify MAC for the CSP messages.
- FCS_RNG.1 requires the TSF to implement a random number generator used for key generation according to FCS_CKM.1.

8 Reference Documentation

[CCP1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1, Revision 5, April 2017

[CCP2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017

[CCP3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components;CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

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

[FCG] Fiscal Code of Germany in the version promulgated on 1 October 2002 (Federal Law Gazette [Bundesgesetzblatt] I p. 3866; 2003 I p. 61), last amended by Article 6 of the Law of 18. July 2017 (Federal Law Gazette I p. 2745)

[KSV] Verordnung zur Bestimmung der technischen Anforderungen an elektronische Aufzeichnungs- und Sicherungssysteme im Geschäftsverkehr (Kassensicherungsverordnung – KassenSichV), Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 66, ausgegeben zu Bonn am 6. Oktober 2017

[PP CSP] Common Criteria Protection Profile Cryptographic Service Provider, BSI-CC-PP-0104-2019

[PP CSPLight] Common Criteria Protection Profile Cryptographic Service Provider Light, BSI-CC-PP-0111-2019

[PPC-CSP-TS-Au] Common Criteria Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit, BSI-CC-PP-0107-2019

[PPC-CSP-TS-Au-Cl] Common Criteria Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit - Clustering, BSI-CC-PP-0108-2019

[PPC-CSPLight-TS-Au-Cl] Common Criteria Protection Profile Configuration Cryptographic Service Provider Light – Time Stamp Service and Audit - Clustering, BSI-CC-PP-0113-2019

[TR03111] BSI, Elliptic Curve Cryptography, BSI Technical Guideline TR-03111, Version 2.10, 2018, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_V-2-1_pdf.pdf?__blob=publicationFile&v=2

[TR CryAS] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 5: Anwendungen der Secure Element API, 27. Januar 2020

[TR SE] Technical Guideline BSI TR-03151 Secure Element API (SE API), Version 1.0.1, 20. Dezember 2018

[TR TSEA] Technische Richtlinie BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, Version 1.0.1, 20. Dezember 2018

[AIS20] BSI AIS 20/31, A proposal for: Functionality classes for random number generators, Version 2.0, 2011

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

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

[NIST2005] NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication May 2005

[NIST2007] NIST Special Publication 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November, 2007

[NIST2008] FIPS PUB 198-1 The Keyed-Hash Message Authentication Code (HMAC), July 2008

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

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

Keywords and Abbreviations

Term	Description
Audit log/ Audit log message / Audit record	an audit log is a sequence of audit records. An audit log message incorporates an audit log in a specified format.
Authentication verification data	data used by the user to authenticate themselves to the TOE
authenticity	the property that ensures that the identity of a subject or resource is the one claimed (cf. ISO/IEC 21827:2008)
cryptographic service provider	component in the operational environment of the TOE providing cryptographic service for the TOE as defined in [PP CSP][PP CSPLight]
tax authorities	authority inspecting accounts and records in form of *Log messages*
certified technical security system (CTSS/"zertifizierte technische Sicherheitseinrichtung")	device dedicated to protect the electronic record-keeping system and digital records (cf. [FCG] section 146a sentence 2). It consists of a security module and a storage medium and providing the unified digital interface (cf. [FCG] section 146a sentence 3)
electronic record-keeping system	system that records each such business transaction or other procedure separately, completely (cf. FCG] section 146a paragraph 1)
taxpayer	taxpayer who is using an electronic record-keeping system for accounts and records (cf. [FCG] section 146a)
manufacturer	produces and sells the TOE
platform	hard- and software used to execute the software TOE. This includes mechanisms needed for installing and updating the TOE program code, e.g. systems to manage authenticated application delivery (AppStore, PlayStore etc.)
clientID	ID/serial number of the electronic record-keeping system, assumed to be unambiguous
keyID	ID of the signature creation key, specified in [TR TSEA] as the hash of the public key
update	installation of new program code
upgrade	(secure) import of persisted user data of a previous version of the TOE
UCP version number	current version number of the SMAERS software (TSF)

Table 8: Terminology

Abbreviations	Term
A.xxx	Assumption
CC	Common Criteria
CSP/CSPLight	cryptographic service provider (light), the TOE of [PP CSP][PP CSPLight]
CTSS	Certified Technical Security System according to [FCG] section 146a sentence 2 ("Zertifizierte Technische Sicherheitseinrichtung")
ERS	electronic record-keeping system according to [FCG] section 146a (1) sentence 1

Abbreviations	Term
	(“elektronisches Aufzeichnungssystem”)
n. a.	not applicable
O.xxx	Security objective for the TOE
OE.xxx	Security objective for the TOE environment
OSP.xxx	Organisational security policy
SAR	Security assurance requirements
SFR	Security functional requirement
T.xxx	Threat
TD	Transaction data
TDS	Transaction data set
TDSS	Transaction data set sequence
TOE	Target of Evaluation
TSF	TOE security functions
UCP	Update Code Package

Table 9: Abbreviations

Appendix: Operational Requirements for CSPLight

CSPLight [CSPLight] is a software component that requires a secure platform, i.e. a hardware component and/or operating system to run on (cf. Non-TOE Hardware/Software/Firmware available to the TOE as described below). An instantiation of CSPLight used in the context of the TOE must provide the same level of security as a certified CSP, however, some physical security requirements are satisfiable by the operational environment in combination with operational security requirements.

Hardware Certification

A certified hardware platform MUST be used to execute CSPLight. CSPLight MUST be executed in single-user mode. The certification MUST meet the following physical requirements:

- The hardware platform contains physical security mechanisms to prevent an attacker from gaining access to [CSPLight] in such a way that there is a HIGH probability that any physical tampering in order to gain physical access to or modify the hardware platform that [CSPLight] is run on is detected.
- The hardware platform MUST make use of tamper-evident coatings such as hard epoxy, seals, and pick-resistant locks on hatches and doors to prevent unauthorized access.
- The hardware platform MUST be implemented such that any physical attack has a HIGH probability of resulting in significant damage to the hardware platform and [CSPLight] such that [CSPLight] will not function, yet is stopped in a secure state.
- The hardware platform MUST include attack detection circuits such that all sensitive key material (e.g. plaintexts, and secret and private key material) is zeroized when a physical attack and tampering is detected, or when hatches and doors are opened without proper authorization.
- The hardware MUST be designed in such a way, that any holes or ventilation openings make physical probing impossible, e.g. by covering the holes with a dedicated material, or by bending ventilation shafts.

Security Audit

The following aspects MUST be considered for the operation of a CSPLight within the security audit according to ISO/IEC 27001:

- The hardware platform on which CSPLight runs MUST be certified.
- The operating environment of CSPLight MUST be protected such that loss or theft of CSPLight and its underlying hardware platform is prevented.
- Inspections at regular intervals MUST be conducted to ensure that CSPLight and its underlying hardware platform has not been physically tampered with, that CSPLight and its underlying software platform is in a trusted state, and that CSPLight and its underlying hardware/software platform is running in the intended configuration.
- Audit trails that are generated by CSPLight and its underlying hardware/software platform MUST be collected and regularly reviewed by the system administrator according to a specified audit process.
- The CSPLight MUST be configured to disallow external backup of private keys, instead clustering MUST be used to provide business continuity.
- Access to CSPLight and/or its underlying platform MUST enforce the principle of dual control.

For all of the above, guidance given in the controls of ISO/IEC 27002 SHOULD be taken into account.

Appendix: Log Message Structure and Data Dependency

The following figure provides an overview of the different types of log messages, their purpose, content and data dependency. Normative specification is provided in [TR SE] only. This table will be included in the next version of [TR SE] and not in the PP anymore.

		Transaction Log Message	System Log Message	Audit Log Message
Description				
Content		Contains **transaction data** (fiscal data) from the ERS to be signed by the TSE.	Contains **security related event data of the SMAERS** component or CTSS-Interface.	Contains **security related event data of the CSP** component (audit records*).
Triggered by		ERS on behalf of the tax payer.	SMEARS itself (e. g. self-test) or as a reaction to user interaction by e.g. Administrator or CTSS-Interface.	CSP itself (e. g. self-test) or as a reaction to (administrative) user interaction.
Log Message Content (see TR-03151 for details)				
Data field	Description	Field content and its (source)		
version	Version of log message format.	version (static value, SMAERS)	version (static value, SMAERS)	version (static value, SMAERS)
certifiedDataType	Type of log message.	OID of transaction logs (static value, SMAERS)	OID of system logs (static value, SMAERS)	OID of audit logs (static value, SMAERS)
certifiedData	Actual content of transaction and system logs.	operationType (ERS)	operationType (event depending SMAERS and/or CTSS-Interface)	(empty)
		clientID (ERS, validated by SMAERS)		
		processData (ERS)	systemOperationData (event depending SMAERS, CTSS-Interface and/or CSP)	
		processType (ERS)		
		additionalExternalData (RFU, ERS)	additionalInternalData (opt., SMAERS)	
		transactionNumber (SMAERS for startTransaction; ERS (validated by SMAERS) for updateTransaction and finishTransaction)		
		additionalInternalData (opt., SMAERS)		
serialNumber	CTSS serial number.	keyID (SMAERS)	keyID (SMAERS)	keyID (SMAERS)
signatureAlgorithm	Used algorithm and parameters for signature creation.	algorithm (SMAERS)	algorithm (SMAERS)	algorithm (SMAERS)
		parameters (SMAERS)	parameters (SMAERS)	parameters (SMAERS)
seAuditData	Actual content of audit logs.	(empty)	(empty)	event data according to PP-CSP (CSP)
signatureCounter	Current usage counter of the signature private key.	counter value (CSP)	counter value (CSP)	counter value (CSP)
logTime	Timestamp representing the log message creation time.	e.g. UnixTime (CSP)	e.g. UnixTime (CSP)	e.g. UnixTime (CSP)
signatureValue	Signature output using all of the preceding fields as input data.	digital signature (CSP)	digital signature (CSP)	digital signature (CSP)

* Assuming a CSP exporting audit records as audit logs, cf. PP-SMAERS p. 7, footnote 1. i.e.: the audit record (seAuditData, signatureCounter, logTime and signatureValue) is formatted acc. to TR-03151.