Federal Office
for Information Security

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

BSI-CC-PP-0105-V3-2025

Version 3.0.2

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

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

Table of Contents

Figures

Tables

1 PP introduction

In order to combat tax-fraud, electronic record-keeping systems in Germany must be equipped with a certified 'Technical Security System' (TSS; 'Technische Sicherheitseinrichtung') that consists of a storage medium, a security module, and a standardized 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. A generic and reusable cryptographic component that implements the required core cryptographic functionality. This component is called C*ryptographic Service Provider* (CSP).
2. An application component that uses the services provided by the CSP to implement the logic and functionality required to serve as the security module for the TSS. This component is the S*ecurity Module Application for Electronic Record-keeping Systems* (SMAERS).

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 used interchangeably for all allowed configurations mentioned.

Regarding major security features of the TOE, note that the TOE's implementation representation is subject to evaluation, and aspects such as flaw remediation and a developer-defined life cycle model are considered as well.

1.1 PP Reference

Title:	Common Criteria Protection Profile Security Module Application for Electronic Record-keeping Systems (SMAERS)
Sponsor:	BSI
CC Version:	CC:2022 Revision 1
Assurance Level:	EAL2 augmented with ALC_LCD.1 ALC_FLR.1 and ALC_CMS.3; with refinements on ALC_LCD.1, ALC_CMS.3, ADV_ARC.1 and ATE_IND.2
General Status:	Final
Version Number:	3.0.2
Registration:	BSI-CC-PP-0105-V3-2025
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 CSP-platform (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 cannot directly rely on the CSP platform, a platform with secure storage must be used for TOE execution. This platform 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 most cryptographic operations, specifically:

- The creation, destruction and usage of the signature-creation key used to sign log messages.
- The management and use of the signature counter associated with the signature creation key.
- Time management and inclusion of timestamps into signed log messages.

TOE Definition

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

The TSS consists at the minimum of a security module, a storage medium, a distribution logic and a standardized digital interface (TSS interface) for integration into a electronic record-keeping system. The ERS records business processes as transactions or other audit-relevant processes. The TOE generates log messages from provided data to obtain traceable and secure logging of all relevant processes. The log messages are stored in the TSS storage medium and also sent back to the ERS.

The security module is required to provide

- the point in time when the process is started[1],
- a transaction number for each new transaction,
- the point in time when the process is completed or aborted
- the check value, i.e. a signature over the logged data, and
- a signature counter, i.e. a unique and continuously incremented number assigned to each signature created.

Of the above, only the transaction number is implemented and managed by the TOE itself. For time stamping and signature creation the TOE relies on the CSP.

The security module provides the logging of all relevant processes in the form of log messages using the cryptographic services of the CSP, cf. [TR-03153-1].

1 Technically, when securing the business process is triggered - which coincides with the point in time of the start of the process when that securing is triggered immediately upon the start of the business process.

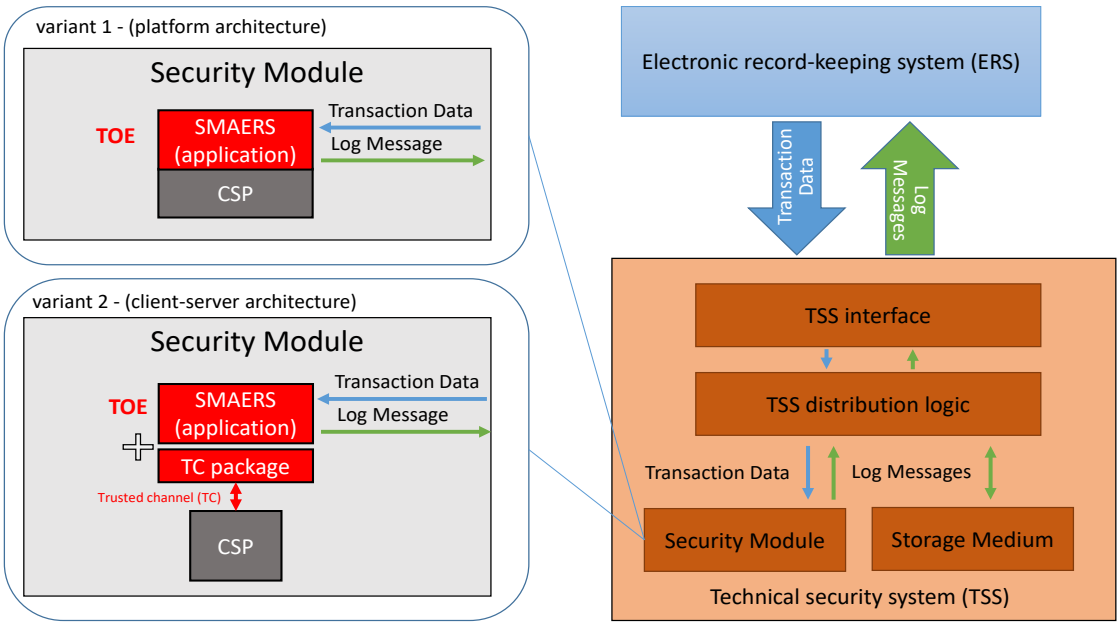

Figure 1: Description and interaction between the TOE and the relevant non-TOE components. The Log Messages sent from the security module include transaction log messages as well as system and audit log messages.

Log messages in general consist of a type-specific payload, as well as protocol data and a signature. There are three types of *log messages*, cf. [TR-03151-1] and [TR-03153-1]:

- *Transaction logs* are created to protect the transaction data originating from the electronic record-keeping system as type-specific payload. Transaction logs are generated whenever a transaction is started, updated or finished. In case of updateTransaction, the TOE may accumulate transaction data before the corresponding transaction log is generated. The protocol data of *transaction logs* includes the transaction number of the transaction.
- *System logs* are generated to log the execution of system operations and events as described in [TR-03151-1] and TSF security events as type-specific payload.
- *Audit logs* are generated to document management or configuration operations of the CSP. Their type-specific payload is comprised of audit data that provide information for the interpretation of the *transaction logs,* e.g. providing information about changes of the CSP-configuration and related assets.

The protocol data of *transaction logs, system logs* and *audit logs* include meta data to identify the log type and used signature algorithm as well as the serial number of the TSS, the signature counter and a time stamp. [TR-03153-1], A.2 offers an overview of the different data fields of a log message and their respective source.

The TOE

- imports transaction data provided by the TSS distribution logic and includes it as type-specific payload in a *transaction log*,
- manages part of the protocol data for the *log messages,* including
  - the transaction number implemented and managed by the TSF used in *transaction logs*,
  - the TSS 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 type-specific payload and the protocol data in the transaction log and system log, if the CSP does not provide complete transaction or system logs,
- imports audit records from the CSP (cf. FDP_ITC.2/AR and FAU_GEN.1) as *audit logs*[2] and exports them as *audit logs*,
- generates a *system log* consisting of commands and TSF audit data of TSF security events as payload,
- exports all types of *log messages* to the TSS distribution logic,
- provides secure identification and authentication of local users, access control and security management of the TSF for authorized users
  - as TSF functionality (client-server-architecture), or
  - by using cryptographic services of the CSP (platform architecture),
- relays identification data, authentication data and command data for users of the CSP component to the CSP, if needed.

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

The main part of the protection profile at 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]). In this case, the security target shall claim the package *trusted channel* between the TOE and the CSP in chapter 6. 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.

Within this document 'the TOE' refers to a discrete and separate component of a single TSS, i.e. a distinct instance of SMAERS. However, a security target may widen the scope of the TOE to reflect the possibility to allow SMAERS to incorporate multiple (virtually) separated SMAERS *units* sharing the same implementation, c.f. [TR-03153-1]. In this approach, each unit must independently manage its own set of assets, specifically including authentication reference data for local users and the trusted channel towards the CSP, excluding only the Update Code Packages that change the implementation of all units at the same time. Self-tests carried out by a SMAERS unit that check the integrity of the singular SMAERS implementation may refer to the same check result.

Note: The TOE must be compliant to [TR-03153-1], its subordinate guidelines and must use cryptographic services of the CSP compliant with [TR-03116-5].

Method of Use

The TOE is part of the security module of the TSS protecting accounts and records of one or more electronic record-keeping systems.

The TOE generates time stamped and signed log messages using the CSP's cryptographic services in order to generate verifiable sequences of transaction and event data. The TOE generates log messages sequentially and one at a time.

The TOE may provide security management features of the TSF for administrators. If implemented, the security management features are used to configure certain security features of the TOE such as the

2 A CSP meeting BSI TR-03153-1 [TR-03153-1] shall export complete audit logs as audit record.

communication channels between the TOE with the TSS distribution logic and the CSP. The TOE may further 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 and/or the CSP to support receiving and verifying the integrity of update code packages (UCPs) for installation of a new certified TOE.

TOE states and error handling

The TOE has the capability to track, detect, report and (if possible) automatically recover from error conditions.

The TSF can be in different states in its operational life cycle phase:

- In the *idle state* the TSF waits for input data from the TSS distribution logic or a local user. This should be the default state of the TOE if all self-tests succeed, no operation is currently performed by the TOE and no communication with the CSP is ongoing. Depending on the implementation, the TOE may also idle in a non-executed state waiting to be called.
- In the *waiting state* the TSF has sent data to the CSP and is waiting for conclusion of CSP communication. In this state the TSF shall reject new input from the distribution logic. I.e. the waiting state is a blocking state enforcing sequential data processing of the security module to generate log messages.
- If a TSF self-test fails or an unexpected failure during creation of a system log or transaction log occurs, the TSF enters a *secure error state* and tries to automatically recover from it. The secure error state is a blocking state, rejecting new input from the distribution logic other than requests for self-tests.

Detectable errors in the idle state include invalid or rejected input and the failure of self-tests. Invalid input leads to TSS behavior as defined in [TR-03151-1] and [TR-03153-1].

Detectable errors in the waiting state include the unavailability of the CSP when data is sent to the CSP and a corresponding log message is expected.

In the secure error state, the TOE resets the secure channel to the CSP (if used). The TSF exits the secure error state only if a self-test passes, the connection to the CSP is recovered, all remaining data are successfully sent to the CSP for signing, received and imported as system log(s) or transaction log, respectively, and eventually exported to the TSS distribution logic.

To also be able to recover from non-temporary issues, secure management of the TSF by the administrator is allowed in the secure error state as well as requesting self-tests of the TSF.

CSP communication

The TOE to CSP communication is implemented such that data loss, and subsequently data inconsistency in the log trail, is only possible in rare circumstances that cannot be reliably exploited.

Architectures relying on non-permanent or intrinsically unreliable transportation channels, i.e. using the client-server architecture with the TOE and the CSP connected via networking devices, shall implement additional measures to prevent data loss. Such additional measures should aim to preserve the integrity of log message sequences by protecting the related assets, i.e. counters and timestamps. The means of communication w.r.t. log message creation should provide:

- Detection of lost messages and recovery of their content.
- Local, persistent storing of unacknowledged message content.

To achieve this, implementations may utilize

- message acknowledgment (explicit or implicit), e.g. by implementing a three-way-handshake and

- idempotent message handling.

It is up to the ST author to find a suitable implementation. Communication unrelated to the creation of signed log messages may refrain from utilizing those measures.

Interrupting the CSP communication lets the presence check for the CSP fail and leads to the TOE entering a secure error state, as described above.

TOE Life Cycle

The TOE life cycle is part of the life cycle of the TSS. The life cycle documentation shall describe the complete life cycle of the TSS including details necessary for the understanding of the interaction with and configuration of the CSP. The additional documentation has to be provided within the certification process and shall be evaluated according to the Supporting Document for this Protection Profile [SD].

The additional documentation must address the following life cycle considerations (informal, for a detailed list of requirements see [SD]):

- The provisioning of the TOE and the CSP within the life cycle of the TSS describing the initial personalization, 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 security of the underlying hard- and software platform.

If any steps within the TSS 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 cryptographic asset used to protect the trusted channel between the TOE and the CSP and authentication reference data for the local SMAERS admin 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 security audit for the operating environment of the CSPLight is specified in the [SD]. The operator must implement and continuously maintain an information security management system (ISMS) with security level *high* according to chapter 10 of [SD].

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 the requirements specified in [TR-03153-1].
- a TSS distribution logic that provides the transaction data and other data and receives signed 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-03116-5].

2 Conformance Claims

2.1 CC Conformance Claims

The PP claims conformance to CC:2022 Revision 1 [CC:2022] .

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

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

2.2 PP Conformance Claim

This PP does not claim conformance to any other PP.

2.3 Package Claim

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

2.4 Conformance Claim Rationale

The dependencies of security assurance components of the package EAL2 are solved within the package [CC-Part-5]. The components ALC_LCD.1, ALC_FLR.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.

2.6 Reference to Evaluation methods/activities

This PP requires the use of evaluation methods/ evaluation activities defined in [CEM] augmented with evaluation activities defined in [SD]. In particular, individual Evaluation Activities (EA) associated with the augmentations ALC_LCD.1 and ALC_CMS.3 shall be performed as specified in the Assurance Refinements in chapter 5.2.1. Further, additional Evaluation Activities associated with the life cycle of the security module of the TSS shall be performed according to the *Supporting Document for Protection Profile SMAERS* [SD].

3 Security Problem Definition

3.1 Introduction

Assets

The assets of the TOE are

- the transaction data, including the *type of operation* provided by the TSS distribution logic. Here, integrity - including completeness of the transaction data - shall be protected. Verification of the transaction log messages by the operational environment shall determine whether the transaction data was received from the TSS distribution logic, and modifications and gaps shall be detectable,
- the transaction counter, i.e. the current transaction number that enumerates transactions. The transaction number must be continuously increasing without gaps,
- the list of open transactions, i.e. transaction numbers generated by the TSF indicating transactions that are neither completed or abandoned,
- the audit records imported from the CSP and exported as audit logs to the TSS distribution logic, the system logs and transaction logs,
- the UCP version number, i.e. the version number of the currently executed implementation,
- the authentication reference data used to authenticate an user as SMA administrator, i.e. a password or public key, if the administrative functionality is implemented,
- the signature-verification key, i.e. the public part of the signature key pair used to sign and verify log messages, and a hash thereof acting as the TSS serial number (keyID),
- the cryptographic asset, i.e. the PACE AES key 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	integrity
transaction number	authenticity, integrity
list of open transactions	integrity
audit logs/audit records, system logs and transaction logs	authenticity, integrity
signature-verification key and/or its hash	integrity
UCP version number	integrity
password as authentication reference data (conditional, if used for administrative access)	integrity, confidentiality
public authentication key as authentication reference data (conditional, if used for administrative access)	integrity
Trusted Channel authentication reference data (conditional, if package Trusted Channel is claimed)	integrity, confidentiality

Table 1: Assets to be protected by the TOE

The assets operated by the external CSP component are

- the signature-creation key, i.e. the private part of the signature key pair used to sign and verify log messages
- the signature counter, i.e. the usage counter associated to the signature-creation key
- the time included as protocol data to the data-to-be-signed by the CSP

The Update Code Package (UCP) is an asset operated by the SMAERS' platform that verifies its authenticity and integrity prior to upgrading the TSF.

Users and Subjects

The users and subjects defined below are distinct from the role model in [TR-03151-1]. Users and roles defined in the latter, including e.g. the taxpayer acting as TSS administrator, converge in the TSS interface communicating via the distribution logic with the TOE.

The TOE knows users as external entities actively communicating, either directly or indirectly, with the TOE as

- *electronic record-keeping system (ERS),*
- *TSS distribution logic implementing the TSS interface and distributing data between the components of the TSS*,
- *CSP*,
- SMA *administrator (if management functionality is implemented).*

The *ERS* communicates with the TOE using the *TSS interface* and *distribution logic*. The TOE also uses the *TSS distribution logic* as an external entity that further uses the TSS storage component to store transaction logs, system logs, and audit logs. The TOE uses the CSP as external entity providing security services and audit records.

An SMA administrator is only required if the TOE implements functionality for TSF management. The SMA 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. 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 of the TOE if such functionality is implemented. The SMA administrator subject is acting on behalf of a human user after successful authentication as administrator until (automatic) logout.
- *TSS interface role*: A subject in this role is allowed to import *transaction data* from the *TSS distribution logic*, to generate *transaction logs and system logs*, and to export *transaction logs and system logs* to the *TSS distribution logic*. A subject in this role is started automatically after start-up of the TOE if the *TSS interface role* is *activated* and the *TSS distribution logic* and the *CSP* are successfully tested according to FPT_TEE.1/EXT or FPT_TEE.1/TC.
- *Crypto role*: A subject in this role is allowed to import audit records from CSP and to export *Audit logs* to the *TSS distribution logic*. In addition the Crypto role is allowed to start the upgrade process of the TOE. A

subject in *Crypto role* is started automatically after start-up of the TOE if the *CSP* is successfully tested according to FPT_TEE.1/EXT or FPT_TEE.1/TC.

Objects

The TSF operates on the following types of user data objects:

- *data-to-be-signed (DTBS)*, compiled by the TSF and sent to the CSP for signing and time stamping. The content of the DTBS is depending on the operation and type of resulting log message:
  - In case of a *transaction log*: the asset *transaction data* (TD)[3] imported from the distribution logic, the asset *transaction number* either generated by the TSF (startTransaction operation) or imported from the distribution logic and verified as open transaction by the TSF (updateTransaction and finishTransaction operations), and the payload type *transaction log* according to [TR-03151-1],
  - in case of a *system log*: the event data and the payload type *system log* according to [TR-03151-1].

  In addition, the DTBS for all types of log messages contain according to [TR-03151-1]:
  - *additionalInternalData*,
  - the *keyID* as the hash value of the signature-verification key,
  - additional protocol data (algorithm, parameters), if those are not added by the CSP.
- *log messages* (LM)[4] as *transaction log, system log* or *audit log*. The content of the log messages is depending on the type of log message:
  - In case of a *transaction log* or *system log*: The *data-to-be-signed* for the respective log message type,
  - in case of an *audit log*: The audit record including the payload type *audit log* as data imported from the CSP.

  All types of log messages contain *protocolData* generated by the CSP:
  - The point in *time* when the log message was signed,
  - the *signature counter* that enumerates the signatures created with the signature-creation key and
  - the *signature*.
- *TSF audit events* as auditable system events that shall be logged and exported as a signed *system log*
- *update code package* (UCP)
- *commands*, including the *type of operation* imported as transaction data

Note: Refer to [TR-03151-1] and [TR-03153-1] for a definition 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 securely exporting and importing TSF data into the new TOE.

3 The format of *transaction data* is assumed to meet [TR-03151-1].
4 The format of *log messages* shall meet [TR-03151-1].

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 *TSS distribution logic* known to the TOE has at least the security attribute *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

- *type of the operation* to determine the operation to be executed as s*tartTransaction, updateTransaction or finishTransaction*.
- *transaction number* to assign the TD to an open transaction and enumerating the transactions continuously increasing without gaps (only for updateTransaction and finishTransaction).

The TOE manages the last assigned transaction number and the transaction numbers of the open 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 incremented value in the *data-to-be-signed* and adds this value to the list of open transactions.
- If the *type of the operation* is *updateTransaction* or f*inishTransaction* and meets the *transaction number* of an open transaction, the *transaction number* in the transaction data is imported and assigned to the *data-to-be-signed* .
- If the *type of the operation* is *finishTransaction*, the *transaction number* is removed from the list of open transactions cf. [TR-03151-1].

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:

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

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 used to record TSF audit events 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 TSS interface and distribution logic 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

The attacker generates forged or manipulates d*ata-to-be-signed* sent for signing and time stamping to the CSP. A forged *transaction log* may result in forged transaction. A forged *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 TSS distribution logic. 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 TSS distribution logic. 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.UnauthSign Unauthorized Signature Creation

The attacker gains access to the signature service of the CSP and uses the signature-creation key to sign arbitrary data.

T.SMConInt Security Module Connection Integrity Disruption

The attacker manipulates, disturbs or disrupts the connection between the TOE and CSP to provoke gaps in the transaction or log message sequence or conceal forged transaction data.

T.FaUCP 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/or operates the ERS and TSS (either directly or indirectly). The taxpayer is assumed to use an ERS equipped with a TSS, 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 assessment of the validity of those parts of the transaction data that are not security attributes is out of scope of the TOE. This includes the assessment of the appropriateness of transaction flow managed by the ERS and/or taxpayer. The taxpayer is however also

considered as potential attacker, who may use a manipulated TSS or manipulates logs after they were produced by the TSS.

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.

OSP.CertSecDev Certified Security Device

The accounts and records generated by the electronic record-keeping system shall be protected by a certified security device (the TSS). The security module of the certified security device generates time stamps of the start, update, and finish of a transaction, as well as a transaction number.

OSP.ProtDev Protection of ERS and Certified Security Device

The taxpayer shall correctly operate the electronic record-keeping system and correctly protect the electronic record-keeping system and the certified security device.

OSP.ValidTrans Validation of transactions

A sequence of transactions is valid if all log messages meet the requirements for content defined in [KSV] their check values are valid digital signatures and the transaction numbers are consecutive increasing without gaps . The sequence of log messages support detection of incomplete transactions and manipulations.

OSP.VerifyLogs Verification of log messages and Sequences

A tax inspector shall check the digital signatures, the transaction numbers, signature counters and the time stamps of *log messages* in given sequences in order to detect forged or missing *log messages*. For this, the certificate of the signature-verification key is securely distributed to the tax inspector. The tax inspector ensures that the transactions are created by a genuine certified security module, e.g. by verifying that the TSS is part of a trustworthy PKI.

OSP.CSPConfig Valid CSP configuration and interface description

The CSP shall be configured according to [SD] to provide cryptographic services for the TOE as needed. The CSP shall provide a fully defined and conclusive or standardized API description the TOE shall adhere to.

OSP.Update Authorized *Update Code Package*s

*Update Code Package*s shall be 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

The platform that executes the TOE provides 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 [TR-03153-1] as well as the requirements in [SD] chapter 10 “Operational Requirements for CSPLight”
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 compliant to or in form of audit logs meeting [TR-03151-1].

A.ProtComCSP Protection of Communication between TOE and CSP

The integrity and confidentiality of the communication data between TOE and CSP in the client-server architecture is protected by a trusted channel, and the security target must claim the package *Trusted Channel*, defined in chapter 6. In case of the platform architecture, the CSP provides a secure execution environment for the TOE and protects the integrity and confidentiality of communication data with the TOE directly using the security services of the CSP.

A.ProtComERS Protection of Communication between TOE and ERS

The electronic record-keeping system provides transaction data whenever a transaction starts, transaction data are updated, or when the transaction is finished. 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.Admin Trustworthy Administrator

The TOE may provide management functionality to be used by an administrator. This SMA administrator acts in a trustworthy way and must be independent of the taxpayer (cf. Application note 1).

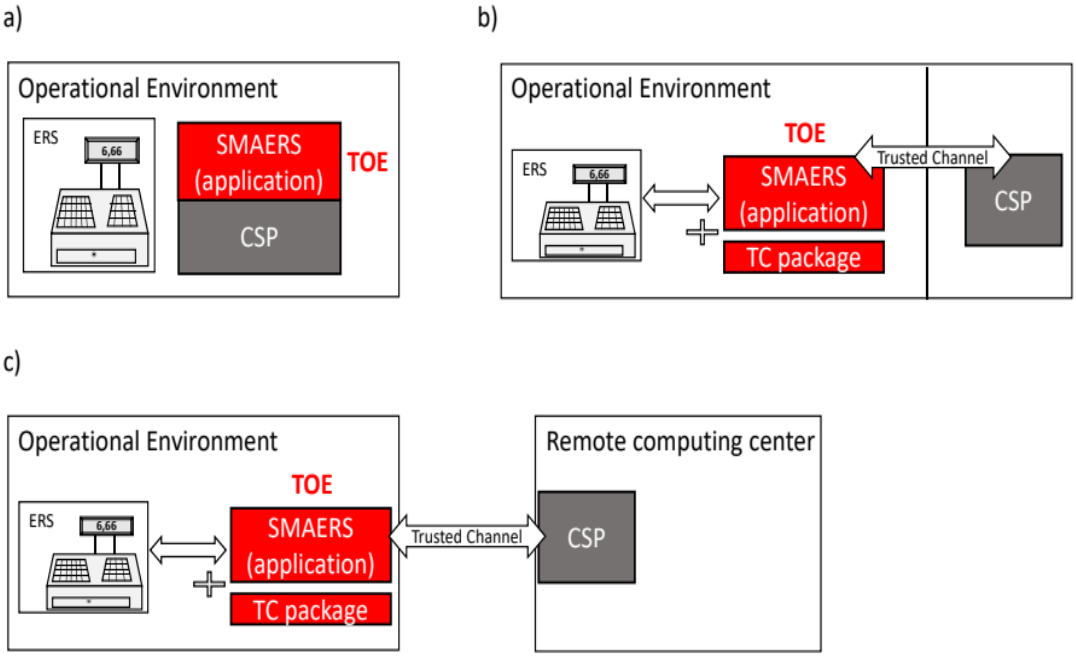

Figure 2: The TOE is always operated as a local component. a) platform architecture b) client-server architecture with local computing center c) client-server architecture with remote computing center

4 Security Objectives

4.1 Security Objectives for the TOE

O.GenLM Generation of *log messages*

The TSF shall generate *transaction logs* and *system logs* containing

- the *data-to-be-signed* for the respective log type, and
- *protocol data* created by the cryptographic service provider.

O.ImpExp Import of *Transaction Data* from and Export of *log messages* to TSS distribution logic

The TSF shall import *transaction data* from the electronic record-keeping system through the TSS distribution logic, import *audit records* from the CSP and export all kinds of *log messages* to the TSS distribution logic.

O.IAA Authentication of Administrators

If the TOE provides management functionality, the TOE shall verify the claimed identity of the SMA administrators by means of a shared secret, e.g. a password, or by verifying the possession of a secret only known to the SMA administrator, e.g. via a secure asymmetric authentication protocol using private and public authentication keys.

O.SecMan Security Management

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

O.TEE Test of External Entities

The TSF shall test the presence of the TSS distribution logic and of the cryptographic service provider.

O.TST Self-Test and Secure Error State

The TSF shall perform self-tests.

The TSF enters a secure error state if:

- Any of the self-tests fail, or
- the test of the presence of the TSS distribution logic fails, or
- the test of the presence of the cryptographic service provider fails.

In the secure error state the import of transaction data and commands forwarded by the distribution logic other than to authenticate SMA administrators and subsequent TSF re-configuration shall be disabled.

The TSF shall also test for new successfully installed update code packages and the correctness of the increased version number.

O.ImpExpUCP Secure Import and Export of User Data during UCP

Before updating the TOE, 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 upgrade process.

4.2 Security Objectives for the Operational Environment

OE.ERS Compliant Electronic Record-Keeping System

The electronic record-keeping system provides all required *transaction data* to the TOE separately, correctly, completely and in real time that are required for the generation of *log messages* (cf. Application Note 1).

OE.SMAERSPlatform Secure Platform

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 [TR-03151-1].

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-03151-1]. The assets and services of the CSP must be configured according to [SD] to appropriately match the intended usage by the TOE. The CSP must provide a fully defined and conclusive or standardized API description the TOE shall adhere to.

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 *data-to-be-signed* and for time services. The CSP audit records shall be exported meeting [TR-03151-1] in order to avoid a transformation of an audit record into a log message. The vendor of the TOE may provide the TOE bundled 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 6) to protect the integrity of the communication between the TOE and the CSP.

OE.Transaction Verification of Transaction

The operational environment, i.e. a tax inspector, shall verify the validity of *log message sequences* by verification of the corresponding digital signatures and the signature counter as being consecutive without gaps. Further, the operational environment shall verify the *transaction number*s of startTransactions as being consecutive without gaps. The tax inspector shall verify that the TSS is part of a trustworthy PKI and the certificate shall be securely distributed to the tax inspector. The tax inspector shall verify the points in time when the transaction starts as being consecutively increasing with increasing t*ransaction number*s with considerations of the adjustment of the CSP time source .

OE.SecOEnv Secure Operational Environment

The operational environment shall protect the integrity of the communication between the electronic record-keeping system and the TOE.

OE.Admin Trustworthy administrator

The TOE may provide management functionality to be used by an administrator. The SMA administrator shall act in a trustworthy way and is assumed to be the manufacturer or integrator. The SMA 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 6) to mutually authenticate the TOE and CSP and protect the integrity and confidentiality of the communication between the TOE and the CSP in the client-server architecture.

In case of the platform architecture, the operational environment shall intrinsically and appropriately match the TOE and CSP and protect the integrity and confidentiality 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 including 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.UnauthSign	T.SMConInt	T.FaUCP	OSP.SecERS	OSP.CertSecDev	OSP.ProtDev	OSP.ValidTrans	OSP.VerifyLogs	OSP.CSPConfig	OSP.Update	A.CSP	A.SMAERSPlatform	A.ProtComCSP	A.ProtComERS	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											
O.TST				x					x												
O.ImpExpUCP									x												
OE.CSP				x							x				x		x				
OE.SMAERSPlatform		x	x			x		x	x									x			
OE.CSPPlatform		x	x			x		x											x		
OE.ERS	x	x								x											
OE.SecUCP									x							x					
OE.SecCommCSP			x	x			x	x											x		
OE.Transaction				x	x								x	x							
OE.SecOEnv	x									x		x								x	
OE.Admin																					x

	T.EvadTD	T.ManipTD	T.ManipDTBS	T.ManipLM	T.ManipLMS	T.ManipTN	T.UnauthSign	T.SMConInt	T.FaUCP	OSP.SecERS	OSP.CertSecDev	OSP.ProtDev	OSP.ValidTrans	OSP.VerifyLogs	OSP.CSPConfig	OSP.Update	A.CSP	A.SMAERSPlatform	A.ProtComCSP	A.ProtComERS	A.Admin
OE.SUCP									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 or validated by the TSF and *system logs* containing security relevant event data possibly indicating a manipulation attempt, therefore allowing to decide whether presented transaction data have corresponding transaction logs in the examined transaction log sequence.
- 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 of the TSS distribution logic 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,
- In case of the platform architecture, the security objective for the operational environment 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 security objective for the operational environment OE.SMAERSPlatform “Secure Platform” requires the operational environment to protect the TOE against manipulation and misuse.

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

- The security objective for the TOE O.TEE requiring the TSF to test the presence 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 security objective for the operational environment OE.SMAERSPlatform “Secure Platform” requires the operational environment to protect the TOE against manipulation and misuse.
- The security objective for the operational environment OE.SecCommCSP “Secure communication between TOE and CSP” ensures use of a genuine cryptographic service provider and the protection of the integrity and confidentiality 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 and confidentiality 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 6.

The threat *T.ManipLM Manipulation of a 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 or an asymmetric authentication protocol.
- The security objective for the TOE O.TEE "Test of External Entities" requiring the TSF to test the presence of the CSP connected to the TOE.
- The security objective for the TOE O.TST "Self-Test and Secure Error State" detects failure and prevents generation of transaction data sets if the test of the presence 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.SecCommCSP "Secure Communication between TOE and CSP" ensures the authenticity of the CSP connected to the TOE.
- The security objective for the operational environment OE.Transaction "Verification of Transaction" ensures detection of forged or missing log message signatures.

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

- The security objective for the TOE O.GenLM "Generation of *Log M*essages" requiring the TSF to generate *log messages* , requiring the TSF to generate time stamps whenever a transaction starts, is updated or is finished, and requiring the TSF to create *transaction numbers, signature counters* and digital signatures 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 TSS distribution logic" requiring the TSF to import *transaction data* from the electronic record-keeping system through the TSS interface and TSS distribution logic and to export *log messages* to the TSS distribution logic.
- The security objective for the TOE O.TEE "Test of External Entities" requiring the TSF to test the availability of the TSS distribution logic and CSP connected to the TOE.
- The security objective for the operational environment OE.Transaction "Verification of Transaction" ensures detection of missing log messages.

The threat *T.ManipTN Manipulation of Transaction Number* is countered by:

- The security objectives for the TOE O.SecMan "Security Management" requiring the TSF to prevent management of the *transaction number* generation.
- In case of the platform architecture, the security objective for the operational environment 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 security objective for the operational environment OE.SMAERSPlatform "Secure Platform" requires the operational environment to protect the TOE against manipulation and misuse.

The threat *T.UnauthSign Unauthorized Signature Creation* is countered by the security objective for the operational environment OE.SecCommCSP "Secure Communication between TOE and CSP" mutually authenticating the TOE and CSP.

In case of the client-server architecture this is enforced by claiming the package *trusted channel* using cryptographic authentication mechanisms during secure channel establishment, cf. chapter 6.
In case of the platform architecture, the operational environment intrinsically authenticates TOE and CSP.

The threat *T.SMConInt Security Module Connection Integrity Disruption* is countered by:

- In case of the platform architecture, the security objective for the operational environment 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 security objective for the operational environment OE.SMAERSPlatform "Secure Platform" requires the operational environment to protect the TOE against manipulation and misuse, including attacks against the integrity of stateful communication protocols.
- The security objective for the operational environment OE.SecCommCSP "Secure Communication between TOE and CSP" protecting the integrity of the communication between TOE and CSP.
  In case of the client-server architecture this is enforced by claiming the package *trusted channel* using a stateful communication protocol implementing message acknowledgment, idempotence and persistent storage of the content of unacknowledged message, cf. chapter 6.
  In case of the platform architecture, the operational environment sufficiently protects the communication between the TOE and CSP.

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

- The security objectives for the TOE O.ImpExpUCP "Secure Import and Export of User Data during UCP" ensuring that user data are exported and imported after successful upgrade process.
- The security objective for the TOE O.TST "Self-Test and Secure Error 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 "Secure Platform" 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 operational environment OE.ERS "Compliant 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 objective 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 or is finished, and to generate *a transaction number, signature counter* 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 or an asymmetric authentication protocol,
- the security objective for the TOE O.ImpExp “Import of *Transaction Data* from and Export of *Log Message* to TSS distribution logic” requiring the TSF to import *transaction data* from the electronic record-keeping system through the TSS interface and TSS distribution logic and to export *log messages* to the TSS distribution logic.
- the security objective for the TOE O.SecMan “Security Management” preventing manipulation of the *transaction number*s and limiting the authorized manipulation of the TSF configuration 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.VerifyLogs Verification of Log Messages and Sequences* is directly implemented by the security objective for the operational environment OE.Transaction “Verification of Transaction”.

The organizational security policy *OSP.CSPConfig Valid CSP configuration and interface description* is directly implemented by the security objective for the operational environment OE.CSP ”Cryptographic Service Provider Component”.

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 and confidentiality of the communication between the TOE and the CSP shall then be protected by means of a trusted channel, implemented 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 6.

The assumption *A.ProtComERS Protection of Communication between TOE and ERS* 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.Admin Trustworthy Administrator* is directly implemented by the security objective for the operational environment OE.Admin “Trustworthy administrator”.

5 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.

5.1 Security Functional Requirements

5.1.1 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, TSS interface role and Crypto role [assignment: other roles]*[5].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

The following SFR FMT_SMR.1/Admin shall be included in the ST if the ST authors selects *'full or partial management of security functions behaviour (cf. FMT_MOF.1)'* in FMT_SMF.1.1 clause (1):

FMT_SMR.1/Admin Security roles - Administrator

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1/Admin	The TSF shall maintain the role~~s~~: *administrator*[6].
FMT_SMR.1.2/Admin	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.

5 [assignment: *authorized identified roles*]
6 [assignment: *authorized identified roles*]

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

(1) *[selection: full or partial management of security functions behaviour (cf. FMT_MOF.1), none]*,

(2) *management of authentication reference data (cf. [selection: FMT_MTD.1/AD, FMT_MTD.1.1/AD clause (2)])*,

(3) [selection: management of audit function behavior (cf. FMT_MTD.1/SYSAdmin), none],

(4) *[assignment: list additional of security management functions to be provided by the TSF]*[7].

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*[8] the function~~s~~ *[selection: password authentication, asymmetric authentication] according to FIA_UAU.5.2 clause (1) and any additional rules according to FIA_UAU.5.2 clause (2), if defined*[9], to *[selection: administrator, none]*[10],

(2) d*etermine the behaviour of* [11] the function~~s~~ *FPT_TEE.1/EXT by definition of the features to be tested of TSS distribution logic*[12] to *[selection: administrator, none*][13],**

(3) d*etermine the behaviour of* [14] the function~~s~~ *FPT_TEE.1/EXT by definition of the features to be tested of CSP*[15] to *[selection: administrator, none*][16],**

(4) d*etermine the behaviour of and modify the behaviour of*[17] the function~~s~~ *FPT_TEE.1/EXT in case the test of TSS distribution logic or CSP fails*[18] to *[selection: administrator, none*][19],**

(5) *determine the behaviour of and modify the behaviour of*[20] the function~~s~~ *select the auditable events according to FAU_GEN.1/SYS*[21] to *[selection: administrator, none]*[22],**

7 [assignment: *list of management functions to be provided by the TSF*]
8 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
9 [assignment: *list of functions*]
10 [assignment: *the authorized identified roles*]
11 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
12 [assignment: *list of functions*]
13 [assignment: *the authorized identified roles*]
14 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
15 [assignment: *list of functions*]
16 [assignment: *the authorized identified roles*]
17 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
18 [assignment: *list of functions*]
19 [assignment: *the authorized identified roles*]
20 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
21 [assignment: *list of functions*]
22 [assignment: *the authorized identified roles*]

(6) ***determine the behaviour of and modify the behaviour of***[23] **the function *automatic export of audit trails according to FAU_STG.4/SYS clause (1)***[24] **to [selection*: administrator, none*]**[25]

(7) ***determine the behaviour of and modify the behaviour of***[26] ***the function updateTransaction regarding the update interval according to FMT_MSA.4***[27] **to [selection*: administrator, none*]**[28]

Application note 5: To preserve consistency, if the selection in FMT_SMF.1.1 (1) is "none", the selection of the authorized identified roles in FMT_MOF.1 must also be "none" in all clauses. The ST author may decide to select a subset of functions to be modified by an administrator.

Application note 6: The refinements of FMT_MOF.1, are made in order to avoid iterations of the component.

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 upgrade SFP*[29] to restrict the ability to

(1) increase by 1[30] the security attributes internally stored security attribute "transaction number" whenever a transaction is started[31] to subjects in TSS interface role[32],

(2) add or remove[33] **the security attributes *"transaction numbers" to or from the list of open transactions whenever a transaction is started or finished***[34]***, respectively,* to *subjects in TSS interface role***[35]**,**

(3) *modify*[36] **the *TD* security attributes *"transaction number" imported from the TD***[37] **to *none***[38]**,**

(4) *increase*[39] **the security attributes *"version number" of UCP***[40] ***after successful installation* to *Crypto role***[41]**.**

23 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
24 [assignment: *list of functions*]
25 [assignment: *the authorized identified roles*]
26 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
27 [assignment: *list of functions*]
28 [assignment: *the authorized identified roles*]
29 [assignment: *access control SFP(s), information flow control SFP(s)*]
30 [selection: *change_default, query, modify, delete, [assignment: other operations]]*
31 [assignment: *list of security attributes*]
32 [assignment: t*he authorized identified roles*]
33 [selection: *change_default, query, modify, delete, [assignment: other operations]]*
34 [assignment: *list of security attributes*]
35 [assignment: t*he authorized identified roles*]
36 [selection: *change_default, query, modify, delete, [assignment: other operations]]*
37 [assignment: *list of security attributes*]
38 [assignment: t*he authorized identified roles*]
39 [selection: *change_default, query, modify, delete, [assignment: other operations]]*
40 [assignment: *list of security attributes*]
41 [assignment: t*he authorized identified roles*]

Application note 7: The refinements of FMT_MSA.1 are made in order to avoid iteration of the component.

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 upgrade SFP*[42] to provide *restrictive*[43] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the *none*[44] to specify alternative initial values to override the default values when an object or information is created.

5.1.2 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~~ **the TSS distribution logic:** (1) *identity*, (2) *[assignment: additional security attributes]*[45] **and, if the ST author chooses to implement administrative capabilities:** **(a) identity** **(b) authentication reference data,** **(c) role belonging to the SMA administrator.**

Application note 8: The refinements distinguish between the sets of security attributes maintained for authenticated users for an administrator and the distribution logic. FMT_MTD.1/AD Management of TSF data - Authentication data

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 (1) *delete and create*[46] [47] the *authentication data record of all authorized users*[48] to [**selection*: administrator, none***]*[49].

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

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

44 [assignment: *the authorized identified roles*]

45 [assignment: *list of security attributes*]

46 “create” denotes initial creation and setting a new value in case a user forgot/lost their authentication data

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

48 [assignment: *list of TSF data*]

49 [assignment: *the authorized identified roles*]

(2) ***modify***[50] **the** ***authentication reference data***[51] **to** ***the corresponding authorized user***[52].

The following SFR FMT_MTD.3/PW shall be included in the ST if the ST authors selects '*password authentication*' in FIA_UAU.5.2 clause (1):

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 *password as authentication reference data for SMA administrator*[53] **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*[54].

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*[55].

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

(1) *A subject is associated with attribute 'identity' and 'TSS interface role' after the TSS distribution logic is successfully tested according to FPT_TEE.1/EXT.*

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

51 [assignment: *list of TSF data*]

52 [assignment: *the authorized identified roles*]

53 [assignment: list of TSF data]

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

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

(2) *A subject is associated with attribute 'Crypto role' or attributes 'identity' and 'Crypto role' after the CSP is successfully tested according to FPT_TEE.1/EXT or FPT_TEE.1/TC, respectively.*

(3) *A subject is associated with attribute 'identity' and 'administrator' role after successful authentication according to FIA_UAU.5.2 clause (1).*[56]

Application note 9: The attribute 'identity' shall only be associated to the subject being in 'Crypto role' if the CSP identity is tested according to FPT_TEE.1/TC, i.e. if the package trusted channel is claimed.

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 TSS distribution logic according to FPT_TEE.1/EXT and starting the subject TSS distribution logic if testing was successful and the role TSS interface is activated,*

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

(4) [assignment: *list of other TSF mediated actions*][57]

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.

The following SFR FIA_UAU.5 shall be included in the ST if the ST authors selects '*full or partial management of security functions behaviour (cf. FMT_MOF.1)*' in FMT_SMF.1.1 clause (1):

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [selection: *password authentication*[58]*, asymmetric authentication protocol*[59]] to support user authentication.

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

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

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

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

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

(1) *[selection: password authentication, asymmetric authentication protocol] shall be used for an administrator,*

(2) *[assignment: additional rules describing how the multiple authentication mechanisms provide authentication*][60].

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*[61].

5.1.3 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*[62] on

(1) *subjects:*

(a) subject acting for TSS distribution logic,

(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

(g) TSF audit events;

(3) *operations:*

(a) import,

(b) export[63].

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

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

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

62 [assignment: *access control SFP*]

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

FDP_ACF.1.1/LM The TSF shall enforce the *log message SFP*[64] to objects based on the following:

(1) *subjects:*

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

(b) subject in Crypto role;

(2) *objects:*

(a) transaction data,

(b) audit record,

(c) data-to-be-signed,

(d) protocolData with signature,

(e) log message

(f) commands

(g) TSF audit events[65].

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 TSS interface role is allowed to*

(a) import the transaction data from the TSS distribution logic according to FDP_ITC.2/TD,

(b) import commands from activated TSS distribution logic, excluding commands defined in (c),

(c) import commands requesting self-tests of the TSF, login or logout of a user in administrator role and management of TSF functionality by a user in administrator role from activated TSS distribution logic,

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

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

(f) export the transaction log and system log to the TSS distribution logic according to FDP_ETC.2/LM.

(g) [selection: export and import of TSF audit events to external storage according to FDP_ETC.2/AE and FDP_ITC.1/AE, no other activity].

(2) *A subject in Crypto role is allowed to import audit records from the CSP according to FDP_ITC.2/TSS and to export audit logs to the TSS distribution logic according to FDP_ETC.2/LM*[66].

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

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

64 [assignment: *access control SFP*]

65 [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*]

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

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

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

(3) no user is allowed to perform actions listed in FDP_ACF.1.2/LM clause (1) (a) and (b) if the TSF is waiting for data to be imported from the CSP after exporting data-to-be-signed to the CSP or the TSF is in the secure error state.

(4) no user is allowed to perform actions listed in FDP_ACF.1.2/LM clause (1) (g) if the TSF is in a state other than the secure error state.[67]

Application note 10: FDP_ACF.1.4/LM (3) shall effectively enforce the intended sequential execution of commands, transaction processing and TOE audit functionality. External command and transaction queuing and related management is out of scope of the TOE. The TSF shall always be in one of three possible operational states: idle state (waiting for input), blocked state (processing input) and the secure error state.

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
FDP_ITC.2.1/TD	The TSF shall enforce the *log message SFP*[68] 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 'type of the operation'.*

(2) *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 in the list of open transactions.*[69]

FDP_ITC.2/AR Import of user data with security attributes – Audit Records

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

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

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

69 [assignment: *additional importation control rules*]

[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/AR The TSF shall enforce the *log message SFP*[70] when importing ~~user data~~ **audit records** controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/AR The TSF shall use the security attributes associated with the imported ~~user data~~ a**udit records**.

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

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

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

(1) *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~~ **data-to-be-signed** 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 ensure that interpretation of the security attributes of the exported ~~user data~~ **data-to-be-signed** is as intended by the owner of the ~~user data~~ **data-to-be-signed**.

FDP_ETC.2.5/DTBS The TSF shall enforce the following rules when ~~user data~~ **data-to-be-signed** 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]

FPT_TDC.1 Inter-TSF basic TSF data consistency

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*]

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~~ **protocolData** .

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~~ **protocolData** .

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 11: The CSP shall generate and return to the TOE at least the signature counter of the 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-03151-1], 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-03153-1]. *Audit records* are always returned as *audit logs* by the CSP. The signature counter and the time stamp of *transaction logs* and of audit records received as audit logs may be used to test the CSP according to FPT_TEE.1/EXT.

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 the TSS distribution logic**.

FDP_ETC.2.2/LM The TSF shall export the ~~user data~~ **log message** 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~~ **log message** .

FDP_ETC.2.4/LM The TSF shall ensure that interpretation of the security attributes of the exported ~~user data~~ **log message** is as intended by the owner of the ~~user data~~ **log message**.

FDP_ETC.2.5/LM The TSF shall enforce the following rules when ~~user data~~ **log message** is exported from the TOE: *Log messages shall be exported with security attributes*

(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,

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

75 [assignment: *access control SFP*]

(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,

(f) signature for verification of the authenticity of the type-specific payload 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 type-specific payload and protocol data.

(3) audit records of the CSP shall be exported unchanged as audit logs to the TSS distribution logic.[76]

Application note 12: The TSS interface and distribution logic do not implement any security functionality addressed in this PP. The distribution logic imports log messages received from the TOE as user data and stores these in the TSS storage component.

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) *type of the operation,*

(2) *transaction number,*

(3) *signature counter,*

(4) *time stamp,*

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

(6) *signature*[77]

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use *[TR-03151-1] and [TR-03153-1]*[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

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*]

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,*

(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 13: The rules may be enforced by internally storing of the *transaction Number* and last time stamp provided by the CSP in the log messages. The adjustment strategy for the CSP time source should take into account the range of typical platform-dependent inaccuracies as well as the possibility that some platforms start with time 0 (zero) after boot.

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) *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 added to the list of open transactions and the transaction log of imported transaction data.*

(2) *If the type of the operation of imported transaction data is updateTransaction or finishTransaction and the transaction number is in the list of open transactions, then the transaction number of the imported transaction data shall be assigned to the protocol data of the transaction log.*

(3) If the type of operation of imported transaction data is finishTransaction, the transaction number of the imported transaction data is in the list of open transactions and the corresponding protocol data including signature was successfully imported from the CSP, then the transaction number shall be removed from the list of open transactions.[80]

Application note 14: When receiving the *updateTransaction* command, the TOE implementation may choose to not directly send the data-to-be-signed to the CSP but wait for additional *updateTransaction* calls or a *finishTransaction* call, cf [TR-03153-1].

Application note 15: The TSF shall not distinguish between the different reasons a transaction might be finished, i.e. the finishTransaction operation can also be used to close abandoned transactions and remove the associated transaction number from the list of open transactions.

5.1.4 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 TSS distribution logic according to FPT_TEE.1/EXT fails,*

79 [assignment: *list of security attributes*]

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

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

The TSF shall exit the secure error state only if the tests according to clauses (1) – (3) are passed and all remaining tasks are processed. The latter include the task performed while entering the secure error state and all subsequent audit tasks including the generation of system log messages triggered at the beginning, end and during the secure error state. In the secure error state command execution, except requests for self-tests, is blocked and shall be rejected. Management of the TSF configuration by a subject in administrator role, including related login and logout requests, is allowed in the secure error state.

Application note 16: The self-test according to FPT_TST.1 and test of external entities according to FPT_TEE.1/EXT cause the TOE to enter a secure error state if the self-test, the tests of the TSS distribution logic or CSP fail. The exit of the secure error state requires all conditions listed in the refinement being fulfilled, effectively enforcing the TSF to recover into a fully operable state only after finishing all tests and appropriately logging all incidents. Also in the secure error state, management of TSF configuration and related tasks shall generate audit events.

FPT_TEE.1/EXT Testing of external entities

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TEE.1.1/EXT The TSF shall run a suite of tests *during start-up and before exiting the secure error state according to FPT_FLS.1*[82] to check the fulfillment of

(1) TSS distribution logic presence [assignment: list of properties of the TSS distribution logic] and

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

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

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

Application note 17: The administrator may be able to define the actions in FPT_TEE.1/EXT according to FMT_MOF.1.1 (4). 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], chapter J.15.

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 authorized user, periodically during normal operation and before exiting the secure error state*

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

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

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

84 [assignment: *action(s)*]

according to FPT_FLS.1[85] to demonstrate the correct operation of [assignment: *parts of TSF]*[86]: [assignment: *list of self-tests run by the TSF*].

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

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

Application note 18: 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. Furthermore, the integrity of the TSF implementation shall be tested by means of the platform according to OE.SMAERSPlatform.

5.1.5 Security Audit

FAU_GEN.1/SYS Audit data generation – System Log

Hierarchical to: No other components.

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-03151-1],

(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 error state,

(4) start and finish of the execution of the UCP, indicating the 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 auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-module, functional package or ST, [assignment: *other audit relevant information*].

85 [selection: *during initial start-up, periodically during normal operation, at the request of the authorized 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]

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

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

Application note 19: The security relevant events that have to be logged according to FAU_GEN.1/SYS are part of the system log. All system logs shall be compliant to [TR-03151-1]. The 'start-up and shutdown of the audit function' log shall only be generated when the audit functionality is reconfigured, including the start or stop of logging of specific audit events, and shall not be logged on every start-up of the TOE. Generation of audit events shall continue if the TOE is in the secure error state.

FMT_MTD.1/SYSTSS Management of TSF data – System log – TSS distribution logic

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

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

(1) *manually export to the TSS distribution logic,*

(2) *clear after manual export*[91]

the system logs[92], **and**

(3) clear after signature creation[93]

the corresponding audit records[94]

to *TSS interface role*[95].

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.4.1/SYS clause (1),*

(3) *define the percentage of storage capacity of audit records if actions are assigned in FAU_STG.4.1/SYS clause (2)*[96]

the *system logs*[97] to *[selection: administrator, none]*[98].

Application note 20: To preserve consistency, if the selection in FMT_SMF.1.1 (3) is "none", the selection of the authorized identified roles in FMT_MTD.1 must also be "none".

FAU_STG.2/SYS Protected audit trail storage – System log

Hierarchical to: No other components.

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

92 [assignment: *list of TSF data*]

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

94 [assignment: *list of TSF data*]

95 [assignment: *the authorized identified roles*]

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

97 [assignment: *list of TSF data*]

98 [assignment: *the authorized identified roles*]

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.2.1/SYS The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.2.2/SYS The TSF shall be able to *prevent*[99] unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.4/SYS Action in case of possible audit data loss – System log

Hierarchical to: No other components.

Dependencies: FAU_STG.2 Protected audit trail storage

FAU_STG.4.1/SYS The TSF shall

(1) *automatically export audit trails and clear automatically exported audit records*[100] if the audit data storage exceeds *a defined number of audit records within [assignment: pre-defined range]*[101]

(2) ***[assignment: actions to be taken in case of possible audit storage failure]*** **if the audit data storage exceeds a *defined percentage of storage capacity*[102].**

Application note 21: The ST writer shall perform the open operations in the FAU_STG.4.1/SYS element. If the number of audit records in clause (1) is set to 1 then the TSF exports 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 22: The automatic export according to clause (2) shall also prevent loss of internal audit data due to storage constraints in case the TOE is unable to sign data, e.g. if the CSP is not present, by protecting the audit data and storing the audit events outside the TOE. This functionality shall only be used if the TOE is in the secure error state and audit events cannot be properly signed and exported as system logs directly. In this case, clause (2) must include an integrity protected export to e.g. the SMAERS platform, the re-import of unsigned audit events, proper signing of audit data in order of occurrence and subsequent export of the associated log message once the CSP is available again and before leaving the secure error state.

The following SFRs FDP_ETC.2/AE and FDP_ITC.2/AE shall be included in the ST if the ST authors selects '*export and import of TSF audit events to external storage according to FDP_ETC.2/AE and FDP_ITC.1/AE*' in FDP_ACF.1.2/LM clause (f):

FDP_ETC.2/AE Export of user data with security attributes – TSF Audit Events

Hierarchical to: No other components.

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

FDP_ETC.2.1/AE The TSF shall enforce the *log message SFP*[103] when exporting ~~user data~~ **TSF audit events**, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2/AE The TSF shall export the ~~user data~~ **TSF audit events** with the ~~user data's associated~~ security attributes **associated with the TSF audit events**.

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

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

101 [assignment: *pre-defined limit*]

102 [assignment: *pre-defined limit*]

103 [assignment: *access control SFP*]

FDP_ETC.2.3/AE The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported ~~user data~~ **TSF audit events**.

FDP_ETC.2.4/AE The TSF shall ensure that interpretation of the security attributes of the exported ~~user data~~ **TSF audit events** is as intended by the owner of the ~~user data~~ **TSF audit events**.

FDP_ETC.2.5/AE The TSF shall enforce the following rules when ~~user data~~ **TSF audit events** is exported from the TOE:

(1) *TSF audit events shall be exported only to prevent bricking the TOE in case the secure error state leads to exhaustive accumulation of audit events (FAU_STG.4/SYS). Exported audit event shall be integrity protected.*[104]

FDP_ITC.2/AE Import of user data with security attributes – TSF Audit Events

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/AE The TSF shall enforce the *log message SFP*[105] when importing ~~user data~~ **TSF audit events** controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/AE The TSF shall use the security attributes associated with the imported ~~user data~~ T**SF audit events**.

FDP_ITC.2.3/AE The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the ~~user data~~ T**SF audit events** received.

FDP_ITC.2.4/AE The TSF shall ensure that interpretation of the security attributes of the imported ~~user data~~ T**SF audit events** is as intended by the source of the user data.

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

(1) *The TSF shall import TSF audit events that were exported due to exhausted audit event storage while being in the secure error state. The TSF shall check the integrity including completeness of the imported TSF audit records.*[106]

5.1.6 Update Code Package – Upgrade Functionality

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 *upgrade SFP*[107] on

(1) *subjects: Crypto role;*

(2) *objects: stored user data and TSF data*;

104 [assignment: *additional exportation control rules*]

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

106 [assignment: *additional importation control rules*]

107 [assignment: *access control SFP*]

(3) *operations: upgrade*[108].

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 *upgrade SFP*[109] to objects based on the following:

(1) *subjects: Crypto role;*

(2) *objects: update code package with security attribute: version number*[110].

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) *Crypto role is allowed to upgrade the stored user data and TSF data if*

(a) the digital signature of the UCP generated by the issuer is successfully verified by the SMAERS' platform,

(b) the version number of the UCP is larger than the version number of the TSF[111]

FDP_ACF.1.3/UCP The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize 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 *Crypto role is not allowed to upgrade the stored user data and TSF data if:*

(a) the verification of digital signature of the UCP by means of the SMAERS platform fails,

(b) the version number of the UCP is smaller than or equal to the version number of the TSF;

(2) [*assignment: other rules, based on security attributes, that explicitly deny access of subjects to objects*].[112]

Application note 23: The execution of UCP, i.e. the *update* of the TOE implementation, is outside the TSF-mediated functionality of the PP on hand. The *upgrade*, i.e. conduction of changes to user data or TSF data structures or other TSF related tasks, including upgrade of the security attribute *version number*, is in scope of the TSF.

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 *upgrade SFP*[113] when exporting user data **and TSF data**, controlled under the SFP(s), ~~outside of the TOE~~ **to the storage of the platform**.

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

109 [assignment: *access control SFP*]

110 [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*]

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

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

113 [assignment: *access control SFP*]

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

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 **and TSF data**.

FDP_ETC.2.4/UCP_UD The TSF shall ensure that interpretation of the security attributes of the exported user data **and TSF data** is as intended by the owner of the user data **and TSF data**.

FDP_ETC.2.5/ UCP_UD The TSF shall enforce the following rules when user data **and TSF 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 *upgrade SFP*[114] when importing user data **and TSF 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 **and TSF 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 **and TSF data** received.

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

FDP_ITC.2.5/UCP_UD The TSF shall enforce the following rules when importing user data **and TSF 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 user data and TSF data***[115] the following objects: *previous stored user data and TSF data*[116].

5.2 Security Assurance Requirements

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

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

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

116 [assignment: *list of objects*]

The supporting document for this TOE [SD] is used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying the TOE. Although evaluation activities (EAs) are defined mainly for the evaluator to follow, the definitions in the [SD] aim to provide a common understanding for developers, evaluators and other interested parties as to what aspects of the TOE are tested in an evaluation against this protection profile, and to what depth the testing is carried out. This common understanding in turn contributes to the goal of ensuring that evaluations against SMAERS-PP achieve comparable, transparent and repeatable results. In general, the definition of EAs will also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in EAs may in some cases clarify the meaning of the TOE Definition, the SFRs, and may identify particular requirements for the content of Security Targets (STs) and further documentation.

5.2.1 Assurance Refinements

Refinement on ALC_LCD.1.1E:

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence in accordance to the [SD].

Refinement on ALC_CMS.3.1C:

The implementation representation listed shall comprise the implementation representation of the TOE defining the TSF to a level of detail such that the compliance of the TOE and TSF to the requirements imposed by the platform guidances on which the TOE is designed to run on, can be verified by that evidence.

Refinement on ADV_ARC.1.3D:

The security guidance documentation of each platform (hardware 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.

5.3 Security Requirements Rationale

5.3.1 Dependency Rationale

This chapter demonstrates that each dependency of the security requirements defined in chapter 5.1 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.2/SYS	FAU_GEN.1 Audit data generation	FAU_GEN.1/SYS
FAU_STG.4/SYS	FAU_STG.2 Protected audit trail storage	FAU_STG.2/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_ETC.2/AE	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/LM

SFR	Dependencies of the SFR	SFR components
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/AR	[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/AE	[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 6 (FTP_ITC.1/TC).
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

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

Table 3: Dependency Rationale

5.3.2 Security Functional Requirements Rationale

The tables trace each SFR defined in chapter 5.1 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.2/SYS	x						
FAU_STG.4/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_ETC.2/AE				x		x	
FDP_ITC.2/TSS	x						
FDP_ITC.2/TD	x	x					
FDP_ITC.2/AR	x						
FDP_ITC.2/AE				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		
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/SYSTSS	x						
FMT_MTD.1/ SYSAdmin	x						

	O.GenLM	O.ImpExp	O.IAA	O.SecMan	O.TEE	O.TST	O.ImpExpUCP
FMT_MTD.3/PW			x	x			
FMT_SMF.1	x	x		x			
FMT_SMR.1	x	x		x	x		
FMT_SMR.1/Admin	x			x			
FPT_TDC.1	x	x					
FPT_FLS.1					x	x	
FPT_TEE.1/EXT					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 and FMT_SMR.1/Admin.
- The SFR FDP_ITC.2/TD, FDP_ITC.2/AR and FDP_ITC.2/TSS requires the TSF to import transaction data from TSS distribution logic, 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 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, and FMT_MTD.1/SYSAdmin 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/SYSTSS, FMT_MTD.1/SYSAdmin, FAU_STG.2/SYS, FAU_STG.4/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 TSS distribution logic* 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 TSS distribution logic 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 TSS distribution logic 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 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 authentication by password or asymmetric authentication protocol 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 and SFR FMT_SMR.1/Admin define 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 management of audit functionality FMT_MTD.1/SYSAdmin.
- 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 SFR FDP_ETC.2/AE and FDP_ITC.2/AE prevent exhaustion of the TSF audit event storage due to TSF management by the administrator while the TSF is in the secure error state.

The security objective for the TOE O.TEE *Test of External Entities* is met directly by the SFR FPT_TEE.1/EXT. The SFR FMT_MOF.1, restricts the definition and modification of the behaviour of FPT_TEE.1/EXT 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 TSS distribution 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 TSS distribution logic is allowed to perform automatically TSF mediated actions according to FPT_TST.1 and FPT_TEE.1/EXT before users are authenticated.

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 error state if one of the self-tests fails.
- The SFR FPT_FLS.1 requires the TSF to enter a secure error state if the self-test fails, or the test of the TSS distribution logic fails, or the test of cryptographic service provider fails.
- The SFR FPT_TEE.1/EXT requires the TSF to enter the secure error state according to FPT_FLS.1 if the test of the TSS distribution logic 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 upgrade SFP. The SFR FMT_MSA.1 prevents the modification of security attributes “version number” of the UCP.
- The SFR FDP_ETC.2/AE and FDP_ITC.2/AE prevent exhaustion of the TSF audit event storage while the TSF is in the secure error state.

The security objective for the TOE O.ImpExpUCP *Secure Import and Export of User Data during UCP* is directly *met by the SF*R FDP_ITC.2/UCP_UD, FDP_ETC.2/UCP_UD and FDP_RIP.1/UCP that requires the TSF to export and import user data during an upgrade process and securely remove the old stored data afterwards.

5.3.3 Security Assurance Requirements Rationale

Developers and users require for the TOE a low to moderate level of independently assured security.

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.

ALC_FLR.1 has been augmented to match the intended longevity of the TOE in the field, to increase transparency and trust into the security guarantees the TOE provides and to be compliant with possible further changes to the EUCC certification scheme.

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, ALC_LCD 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.

6 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 and confidentiality 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.

Security Objectives

The trusted channel is a specific means to meet the assumption *A.ProtComCSP Protection of Communication between TOE and CSP*. The objectives for the TOE defined in this chapter directly counter the threats T.UnauthSign and T.SMConInt which were only covered by objectives for the environment in the base PP. 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.

The security objective O.SecCommCSP is accompanied by the security objective O.TST2, an extension to the security objective O.TST that defines additional triggers for the TSF to enter a secure error state.

If the trusted channel between the TOE and CSP is not protected against perturbation of the availability by the operational environment, i.e. the TOE platform is not physically connected with the CSP in a rigid and persistent manner, the security objective O.SecCommCSP shall be additionally strengthened by the security objective O.LLCommCSP. In this case, all parts of the security objective for the environment OE.SecCommCSP are replaced by the security objectives O.SecCommCSP and O.LLCommCSP defined in this package.

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. The establishment of the trusted channel shall support mutual authentication of the TOE and CSP and shall allow the TSF to identify the CSP.

O.TST2 CSP Connection Test and Secure Error State

In addition to the triggers defined in O.TST, the TSF enters a secure error state if:

- The test of identity of the cryptographic service provider fails, or
- an interruption of the connection between the TOE and the CSP is detected.

O.LLCommCSP Lossless communication between TOE and CSP

The TOE shall protect against disruption of the established trusted communication channel to provoke gaps in the sequences of transaction numbers and signature counters. In the context of log message creation, a lossless stateful communication protocol shall be used that should implement explicit or implicit message acknowledgment, idempotence and persistent storage of the content of unacknowledged messages.

Application note 24: O.LLCommCSP shall be considered specifically if the connection between the TOE and the CSP involves, or could involve, non-persistent connections and/or additional active components needed for the connection to operate. Typical use cases are those where the TOE and CSP are operated in different operational environments, e.g. a CSP operated in a remote data center. The TOE may use other means than message acknowledgement, idempotence and persistent storage to achieve lossless communication of comparable assurance.

Security Objective Rationale

The rationale presented in chapter 4.3 is modified by this package regarding the additional security objectives O.SecComCSP and O.TST2 in the following:

	T.ManipDTBS	T.ManipLM	T.ManipLMS	T.UnauthSign	T.SMConInt
O.TST2			x	x	x
O.SecCommCSP	x	x		x	
O.LLCommCSP			x		x

Table 5: Security Objective Rationale changes for package trusted channel

The security objective for the TSF O.TST2 *CSP Connection Test and Secure Error State* supports mitigation of:

- The threat T.ManipLMS “Manipulation of a Log Message Sequence” by indicating disruptions of the communication between the TOE and the CSP.
- The threat T.UnauthSign “Unauthorized Signature Creation” by indicating failed tests of the identity of the CSP.
- The threat T.SMConint “ Security Module Connection Integrity Disruption” by indicating disruptions of the communication between the TOE and the CSP.

The security objective for the TSF O.SecCommCSP *Trusted Channel between TOE and CSP* supports mitigation of:

- The threat T.ManipDTBS “Manipulation of data-to-be-signed” by enforcing usage of a genuine CSP by authentication the CSP during the connection establishment of the trusted channel and by enforcing integrity and confidentiality protection by the trusted channel between the TOE and the CSP.
- The threat T.ManipLM “Manipulation of a Log Messages” by enforcing the use of a genuine CSP by authentication the CSP during the connection establishment of the trusted channel between the TOE and the CSP.
- The threat T.UnauthSign “Unauthorized Signature Creation” by enforcing mutual authentication during connection establishment of the trusted channel between the TOE and the CSP.

The security objective for the TSF O.LLCommCSP *Lossless communication between TOE and CSP* supports mitigation of:

- The threat T.ManipLMS “Manipulation of a Log Message Sequence” by enforcing a protection against disruption of the communication between the TOE and the CSP by implementing a lossless communication protocol in the context of log message creation.
- The threat T.SMConInt “Security Module Connection Integrity Disruption” by enforcing a protection against disruption of the communication between the TOE and the CSP by implementing a lossless communication protocol in the context of log message creation.

Security Requirements targeting O.SecCommCSP

In the client-server architecture, the TOE is the application component (in client role) that uses 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.

For mutual authentication of the TOE and CSP as well as the derivation of shared ephemeral session keys for confidentiality and integrity protection the PACE protocol according to *[TR-03110-2]* must be used.

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

elliptic curve	key size	standard
brainpoolP256r1	*256 bits*	*RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111]*
brainpoolP384r1,	*384 bits*	*RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111]*
brainpoolP512r1	*512 bits*	*RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111]*
Curve P-256	*256 bits*	*NIST SP 800-186, section 3.2.1 and G.1.2. [NIST-SP800-186]*
Curve P-384	*384 bits*	*NIST SP 800-186, section 3.2.1 and G.1.3. [NIST-SP800-186]*
Curve P-521	*521 bits*	*NIST SP 800-186, section 3.2.1 and G.1.4. [NIST-SP800-186]*

Table 6: Elliptic Curves, Key sizes and Standards

The PACE protocol involves different static and ephemeral keys:

- PACE key: This static, symmetric key coincides with the static PACE AES key or is a passphrase. The PACE key is a shared secret known to the TOE and CSP. The PACE key shall be generated by the CSP or externally, cf. [SD]. If a passphrase is used, it is recommended to generate passphrases with at least 120 bit entropy, cf. BSI [TR-02102-1], Bemerkung 7.4, (iii). If the PACE AES key coincides with the PACE key, it is recommended that the PACE AES key = PACE key is generated by a random number generator of class DRG.3 or higher according to [AIS20] with at least 256 bit entropy as specified in FIA_SOS.1.
- PACE AES key: Static or derived symmetric key used to encrypt the nonce. The PACE AES key is derived from the PACE key by hashing (cf. BSI TR-03110) if a passphrase is used as the PACE key. The derived PACE AES key may directly be stored and used by the CSP or SMAERS component and TSF without re-hashing during each protocol run. The TOE is provisioned with the PACE AES key with a key size specified in FIA_SOS.1 and by using the PACE key as specified in [SD].
- PACE DH keys: Ephemeral private keys to derive a shared secret using the Diffie-Hellman key agreement steps of the PACE protocol in FCS_CKM.1.
- PACE session keys: Ephemeral symmetric keys used for message encryption and integrity protection. The security properties of the key generation are specified in FCS_CKM.1 and used for message encryption in FCS_COP.1/ENC, MAC calculation and MAC verification in FCS_COP.1/MAC.

To perform mutual authentication using the PACE protocol, both endpoints need to share a static PACE AES key. 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 key	integrity, confidentiality
PACE AES key	integrity, confidentiality
ephemeral keys: PACE-DH Key und PACE Session Key	integrity, confidentiality

Table 7: 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*[117] 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*[118].

Application note 25: Protection against modification and disclosure is always required for the trusted channel. The secure channel should meet the following: *[ICAO], Section 9.8.*

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 for mutual authentication during key establishment,*

(2) *message authentication by MAC verification of received messages*[119]

to support user authentication.

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

(1) *PACE shall 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*[120].

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 ~~an~~ *PACE in PCD role*[121] to prove the identity of *the TOE*[122] by including the following properties [assignment: *list of properties*] to ~~an external entity~~ **a CSP and establishing a trusted channel according to FTP_ITC.1/TC**.

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

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

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

121 [assignment: *authentication mechanism*]

122 [assignment: *entity*]

FIA_SOS.1.1 The TSF shall ~~provide a mechanism to verify that secrets~~ **only support static keys as shared secret (i.e. PACE key, PACE AES key) that** meet [assignment: *cryptographic key sizes of* [selection: *128 bits, 192 bits, 256 bits*]][123].

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_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation]
[FCS_RGB.1 Random bit generation, or FCS_RNG.1 Generation of random numbers]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys ***for FCS_COP.1/MAC and FCS_COP.1/ENC*** in accordance with a specified cryptographic generation algorithm *PACE with [selection: elliptic curves in table 6] and Generic Mapping in PCD role*[124] and specified cryptographic key sizes *256 bits*[125] that meet the following: *[ICAO], Section 4.4*[126].

Application note 26: If *PACE AES key* is used as authentication reference data, the derivation of the key used to decrypt the nonce shall be omitted.

FCS_CKM.6 Timing and event of 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, or FCS_CKM.5 Cryptographic key derivation]

FCS_CKM.6.1 The TSF shall destroy [assignment: *list of cryptographic keys (including keying material)*] when [selection: *no longer needed, [assignment: other circumstances for key or keying material destruction]*].

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 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/MAC 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, or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/MAC The TSF shall perform *MAC calculation and MAC verification*[127] in accordance with a specified cryptographic algorithm *according to AES-256* [FIPS-197] *in [selection: CMAC [NIST-SP800-38B], GMAC [NIST-SP800-38D], HMAC [FIPS-198-1]]*[128] and cryptographic

123 [assignment: *a defined quality metric*]
124 [assignment: *cryptographic key generation algorithm*]
125 [assignment: *cryptographic key sizes*]
126 [assignment: *list of standards*]
127 [assignment: *list of cryptographic operations*]
128 [assignment: *cryptographic algorithm*]

key sizes *256 bits*[129] that meet the following: *the referenced standards above according to the chosen selection*[130].

FCS_COP.1/ENC 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, or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/ENC The TSF shall perform *secure messaging – encryption and decryption*[131] in accordance with a specified cryptographic algorithm *according to AES-256 in CBC and [selection: CTR, OFB, CFB, no other] mode*[132] and cryptographic key sizes *256 bits*[133] that meet the following: [*TR-03110-3], [FIPS197], [NIST-SP800-38A], [ISO/IEC 18033-3], [ISO/IEC 10116]*[134].

The following requirement FCS_RNG.1 is 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*][135] random number generator that implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2 The TSF shall provide *random numbers*[136] that meet [assignment: *a defined quality metric according to [TR-03116-5]*].

Application note 27: 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.

FIA_ATD.1/TC User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

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

(1) *identity*,

(2) *authentication reference data*[137]

129 [assignment: *cryptographic key sizes*]

130 [assignment: *list of standards*]

131 [assignment: *list of cryptographic operations*]

132 [assignment: *cryptographic algorithm*]

133 [assignment: *cryptographic key sizes*]

134 [assignment: *list of standards*]

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

136 [selection: *bits, octets of bits, numbers* [assignment: *format of the numbers*]]

137 [assignment: *list of security attributes*]

Application note 28: The authentication reference data of the CSP is the *PACE key* or *PACE AES key* if key derivation is omitted.

FAU_GEN.1/TC Audit data generation – System Log Trusted Channel

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1/TC 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 [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit;~~

c) *Auditable events in addition to FAU_GEN.1/SYS:*

(1) unrecoverable (w.r.t. to [assignment: TOE internal metric or time]) loss of connection to the CSP and subsequent renewal of the trusted channel connection,

(2) failure to authenticate the CSP during establishment of the trusted channel[138]

FAU_GEN.1.2/TC 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 auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-module, functional package or ST, [assignment: *other audit relevant information*].

Application note 29: The security relevant events extend the list presented in FAU_GEN.1/SYS. All events shall be logged as part of a system log according to [TR-03151-1].

FPT_TEE.1/TC Testing of external entities – CSP via Trusted Channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TEE.1.1/TC The TSF shall run a suite of tests *during establishment of the trusted channel, periodically during normal operation and before exiting the secure error state according to FPT_FLS.1*[139] to check the fulfillment of

(1) CSP presence and identity [assignment: list of properties of the CSP][140].

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

FPT_TEE.1.2/TC If the test fails, the TSF shall *enter the secure error state according to FPT_FLS.1 [selection: none additional action, [assignment: additional action(s)]]*[141].

Application note 30: FPT_TEE.1/TC augments FPT_TEE.1/EXT with tests of the identity of the CSP. The TOE and CSP shall mutually authenticate each other via establishment of the trusted channel. Tests during normal operation may be covered by performing massage authentication according to FCS_COP.1/MAC.

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

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

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

141 [assignment: *action(s)*]

Security Requirements for Lossless Communication

FPT_ITA.1 Inter-TSF availability within a defined availability metric

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITA.1.1 The TSF shall ensure the availability of

(1) *data-to-be-signed*,

(2) commands imported from TSS distribution logic,

(3) *[assignment: other data exported to the CSP]*[142]

provided to another trusted IT product within *normal operation, including all foreseeable situations allowing for a reliable exploitation*[143] given the following conditions:

(1) loss of connection before sending data to the CSP,

(2) loss of connection before receiving a response from the CSP,

(3) shut-down of the TOE before sending data to the CSP,

(4) shut-down of the TOE before receiving a response from the CSP,

(5) [assignment: additional conditions to ensure availability][144]

Application note 31: The TSF shall implement a communication protocol within the trusted channel to ensure availability of communication data under conditions typically assumed prevalent considering the TOEs operational environment. This explicitly covers physical or logical interruption of the transportation layer and unannounced shut-down of the TOE. Mitigations would typically include a secure persistent storage for data to be exported to the CSP in the context of log message creation.

FPT_TDC.1/LLTC Inter-TSF basic TSF data consistency – Lossless Trusted Channel

Hierarchical to: No other components.

Dependencies: No dependencies.

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

(1) *data-to-be-signed,*

(2) log messages,

(3) audit records,

(4) protocolData with signature,

(5) response messages,

(6) [assignment: other data exchanged with the CSP][145]

when shared between the TSF and another trusted IT product.

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

143 [assignment: *defined availability metric*]

144 [assignment: *conditions to ensure availability*]

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

FPT_TDC.1.2/LLTC The TSF shall use *idempotent logic and explicit or implicit message authentication*[146] when interpreting **and acknowledging reception of** the TSF data from another trusted IT product.

Application note 32: The TSF shall implement a communication protocol within the trusted channel to ensure correct interpretation of (re-)sent data in the context of log message creation and provide explicit or implicit message status indicators to the CSP. Implementations may typically include a three-way-handshake and an idempotent interpretation of message content, e.g. by including a secure implementation of a message identifier.

Security Requirements Rationale

The dependencies are fulfilled:

SFR	Dependencies of the SFR	SFR components
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction	FCS_COP.1/MAC and FCS_COP.1/ENC, FCS_RNG.1 FCS_CKM.6 FCS_CKM.6 is omitted as the PACE session keys are ephemeral and are not allowed for further cryptographic key access.
FCS_CKM.6	[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, or FCS_CKM.5 Cryptographic key derivation]	FCS_CKM.1
FCS_COP.1/MAC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction	FCS_CKM.1 FCS_CKM.6 is omitted as the PACE session keys are ephemeral and are not allowed for further cryptographic key access.
FCS_COP.1/ENC	[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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction	FCS_CKM.1 FCS_CKM.6 is omitted as the PACE session keys are ephemeral and are not allowed for further cryptographic key access.
FCS_RNG.1	No dependencies	
FIA_SOS.1	No dependencies	
FIA_API.1	No dependencies	
FIA_UAU.5/TC	No dependencies	
FTP_ITC.1/TC	No dependencies	

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

FIA_ATD.1/TC	No dependencies	
FAU_GEN.1/TC	FPT_STM.1 Reliable time stamps	FPT_STM.1 provided by the CSP PP Module Time Stamp Service and Audit
FPT_TEE.1/TC	No dependencies	
FPT_ITA.1	No dependencies	
FPT_TDC.1/LLTC	No dependencies	

Table 8: Dependency Rationale for the Functional Package

The security objective for the TOE O.TST2 *CSP Connection Test and Secure Error State* is implemented by the SFRs

- FPT_TEE.1/TC requires the TSF to test the presence and identity of the CSP and enter a secure error state if any of the tests fails.
- FIA_API.1 requires the TSF to prove the identity of the CSP by mutual authentication provided by the PACE protocol.
- FTP_ITC.1/TC with FCS_COP.1/MAC require the TSF to implement a secure channel with message authentication to the CSP.
- FAU_GEN.1/TC requires the TSF to generate auditable events in case of connection loss and authentication failures.

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

- FTP_ITC.1/TC directly requiring the trusted channel between the TOE and the CSP to protect the integrity and confidentiality of their communication.
- FIA_UAU.5/TC requires the TSF to authenticate the CSP as communication end point of the trusted channel.
- FIA_API.1 requires the TSF to authenticate itself as communication end point of the trusted channel to the CSP.
- FIA_ATD.1/TC defines the security attribute *identity* for the CSP tested by FPT_TEE.1/TC. If any test fails, the TSF enters a secure error state according to FPT_FLS.1.
- FIA_SOS.1 requires the TSF to verify the cryptographic key size of the PACE AES key.
- FCS_CKM.1 requires the TSF to generate MAC keys for FCS_COP.1/MAC and encryption keys for FCS_COP.1/ENC.
- FCS_CKM.6 requires secure key destruction in order to fulfill the dependency of FCS_CKM.1.
- FCS_COP.1/MAC requires the TSF to calculate MAC for the own messages and to verify MAC for the CSP messages.
- FCS_COP.1/ENC requires the TSF to encrypt messages sent to the CSP and decrypt messages from the CSP to support confidentiality of the communication data.
- FCS_RNG.1 requires the TSF to implement a random number generator used for key generation during PACE key establishment according to FCS_CKM.1.
- FAU_GEN.1/TC requires the TSF to generate audit events to be signed by the CSP and exported as system logs in the case of CSP connection loss and CSP authentication failure.

The security objective for the TOE O.LLCommCSP *Lossless communication between TOE and CSP* is implemented by the SFRs

- FPT_ITA.1 requires the TSF to ensure availability of the data to be exported to the CSP preventing data loss in case of connectivity problems and unexpected shut-down of the TOE in the context of log message creation.
- FPT_TDC.1/LLTC requires the TSF to ensure data consistency for the communication with the CSP, specifically while dealing with connectivity issues in the context of log message creation.

7 Reference Documentation

[AEAO] AEAO zu § 146a Ordnungsvorschriften für die Buchführung und für Aufzeichnungen mittels elektronischer Aufzeichnungssysteme

[BSI-GS-200] BSI IT-Grundschutz, Informationssicherheit und IT-Grundschutz, BSI-Standards 200-1, 200-2, 200-3

[CC:2022] Common Criteria for information Technology Security Evaluation, Parts1 to 5 November 2022, reference CC:2022 Revision 1

[CC-Part-1] Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model, Version CC:2022 Revision 1 Part 1, November 2022, reference CCMB-2022-11-001

[CC-Part-2] Common Criteria for information Technology Security Evaluation, Part 2: Security Functional requirements, Version CC:2022 Revision 1 Part 2, November 2022, reference CCMB-2022-11-002

[CC-Part-3] Common Criteria for information Technology Security Evaluation, Part 3: Security assurance components, Version CC:2022 Revision 1 Part 3, November 2022, reference CCMB-2022-11-003

[CC-Part-5] Common Criteria for information Technology Security Evaluation, Part 5:Pre-defined packages of security requirements, Version CC:2022 Revision 1 Part 5, November 2022, reference CCMB-2022-11-005

[CEM] Common Evaluation Methodology, Version CEM:2022 Revision 1, November 2022, reference CCMB-2022-11-006

[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)

[ISO/IEC 27001] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, Edition 3, 2022

[ISO/IEC 18033-3] ISO/IEC 18033-3, Information technology – Security techniques, Encryption algorithms – Part 3: Block Ciphers, 2010

[ISO/IEC 10116] ISO/IEC 10116, Information technology – Security techniques, Modes of operation for an n-bit block cipher 2017

[KSV] Verordnung zur Bestimmung der technischen Anforderungen an elektronische Aufzeichnungs- und Sicherungssysteme im Geschäftsverkehr (Kassensicherungsverordnung – KassenSichV)

[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

[SD]	Supporting Document for Common Criteria Protection Profile SMAERS in its most recent version
[TR-02102-1]	BSI, Kryptographische Verfahren: Empfehlungen und Schlüssellängen – Part 1, BSI Technical Guideline TR-02102-1, Version 2023-01
[TR-03110-2]	BSI, Readable Travel Documents and eIDAS token – Part 2, BSI Technical Guideline TR-03110-2, Version 2.21, 2016
[TR-03110-3]	BSI, Readable Travel Documents and eIDAS token – Part 3, BSI Technical Guideline TR-03110-3, Version 2.21, 2016
[TR-03111]	BSI, Elliptic Curve Cryptography, BSI Technical Guideline TR-03111, Version 2.10
[TR-03116-5]	Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 5: Anwendungen der Secure Element API, 24. April 2023
[TR-03151-1]	Technical Guideline BSI TR-03151-1 Secure Element API (SE API), Version 1.1.1
[TR-03153-1]	Technische Richtlinie BSI TR-03153-1 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, Version 1.1.1
[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
[NIST-SP800-38A]	NIST Special Publication 800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques
[NIST-SP800-38B]	NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication May 2005
[NIST-SP800-38D]	NIST Special Publication 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November, 2007
[FIPS-198-1]	FIPS PUB 198-1 The Keyed-Hash Message Authentication Code (HMAC), July 2008
[NIST-SP800-186]	NIST Special Publication 800-186 Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters, 2023
[FIPS-197]	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
(certified) technical security system (TSS/(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.)
keyID	ID of the signature creation key, specified in [TR-03153-1] 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 9: Terminology

Abbreviations	Term
A.xxx	Assumption
CC	Common Criteria
CSP/CSPLight	cryptographic service provider (light), the TOE of [PP CSP][PP CSPLight]
TSS	(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 ("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
SMA	Security Module Application
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 10: Abbreviations