Federal Office
for Information Security

Common Criteria Protection Profile

Security Module Application for Electronic Record-keeping Systems

BSI-CC-PP-0105-2019

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

The Fiscal Code of Germany [FCG] section146a requires that an electronic record-keeping system, the accounts and the records must be protected by a certified technical security system. The Federal Office for Information Security defines requirements for the components of the certified technical security system, i. e. for the security module in form of Common Criteria Protection Profiles, and for the storage medium and the unified digital interface in form of Federal Office's technical guidelines (cf. [KSV] section 5). The security module consists of the security module application and the cryptographic service provider (CSP). The Protection Profile in hand defines security requirements of the security module application. The security requirements for the CSP are defined in the Protection Profile Cryptographic Service Provider [PP CSP].

1.1 PP reference

Title:	Common Criteria Protection Profile Security Module Application for Electronic Record-keeping Systems (SMAERS)
Sponsor:	BSI
CC Version:	3.1 Revision 5
Assurance Level:	EAL2
General Status:	Final
Version Number:	0.7.5
Registration:	BSI-CC-PP-0105
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 running on the CSP platform (referred as Platform architecture in [PP CSP]) or as device (referred as Client-server architecture in [PP CSP]).

TOE definition

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

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

- tamper-proof determination of the point in time when the transaction starts (cf. [KSV] section 2 sentence 2 number 1),
- the transaction number (cf. [KSV] section 2 sentence 2 number 2),
- the point in time when the transaction is completed or terminated (cf. [KSV] section 2 sentence 2 number 6), and
- the check value (cf. [KSV] section 2 sentence 2 number 7).

The security module provides the logging of accounts, records and security management activities in form of Log messages (cf. [TR TSEA], chapter 3.1). The Log messages are created by TOE using the CSP.

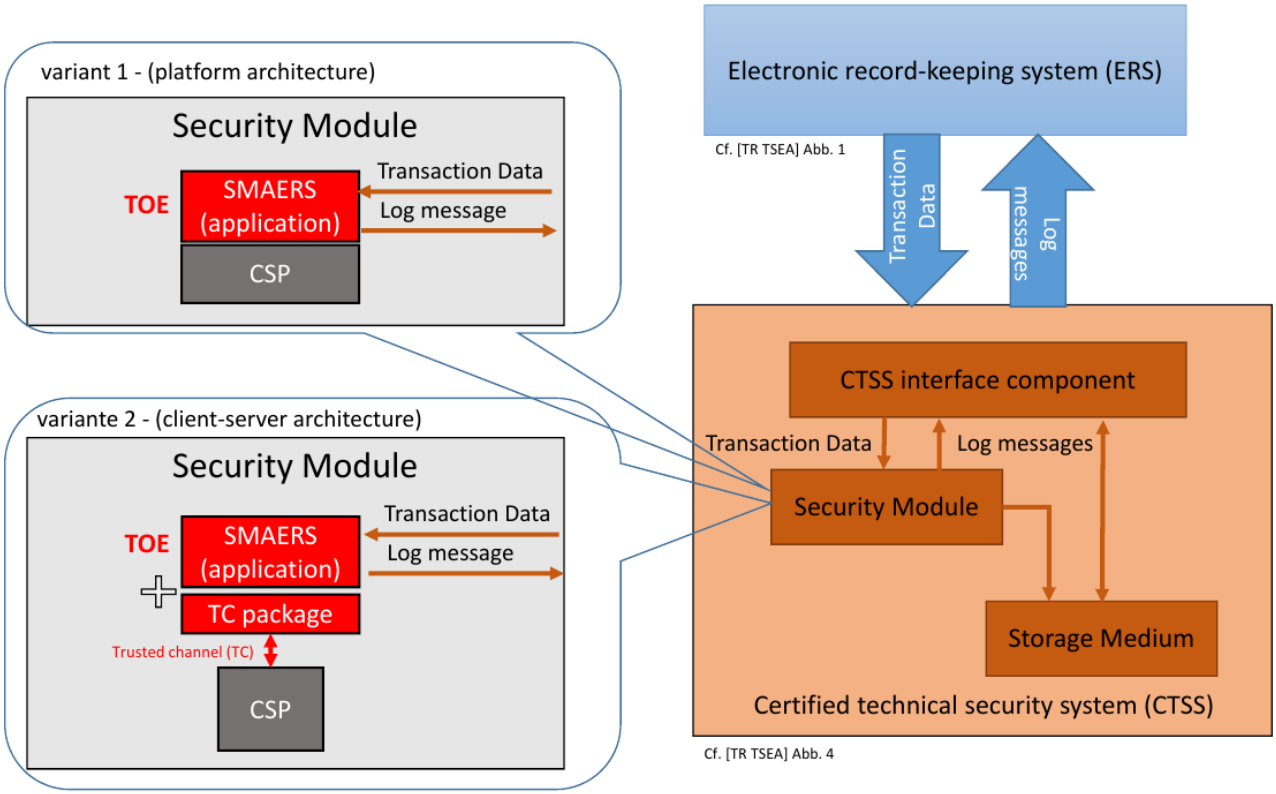


Figure 1: Description and interaction between the TOE and the relevant non-TOE components

The Log messages consist of the certified data, the protocol data and the signature. There are two types of *Log messages*, i. e. *Transaction logs* and *System logs*, cf. [TR SE]. *Transaction logs* are created to protect the actual transaction data of the electronic record-keeping system as certified data. They will be created when the transaction is started, the transaction is finished (i. e. completed or terminated), and may be generated when transaction data are updated. The protocol data of *Transaction logs* contain the transaction number of the actual transaction and time stamps. All *Transaction logs* with the same transaction number build together the transaction data defined in [KSV] section 2 sentence 2. *System logs* are generated to document management or configuration operations of the security module. The certified data of the S*ystems logs* provide information for interpretation of the *Transaction logs* e. g. setting of the time source for the time stamps. The signature is generated for the certified data and the protocol data. It contains information about the signature algorithm and the signature value.

The TOE

- imports transaction data from the CTSS interface component as certified data of *Transaction logs*,
- generates part of the protocol data in the *Transaction log* including
  - the transaction number generated by the TSF,
  - the serial number as hash value of the public key included by the TSF for verification of the digital signature,
- includes to the *Transaction log* the digital signature created by the CSP over the certified data and the protocol data,
- imports audit records from the CSP (cf. [PPC-CSP-TS-Au], FAU_GEN.1) and exports them as system log[1],
- exports *Log messages* to the CTSS interface component,

1 A CSP meeting BSI TR-03151 [TR SE] shall export audit records in form of system logs.

– provides identification and authentication of users, access control and security management of the TSF for authorized users.

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

The TSF may generate information about TSF security events as certified data of system logs exported to the CTSS interface component, e. g. about entering and exiting the secure state according to FPT_FLS.1. This optional security functionality is not required for conformance to the PP in hand but may be described in the security target.

The main part of the protection profile in hand assumes the TOE being implemented as software running on the CSP as secure execution platform (cf. Platform architecture [PP CSP]). In case of the Client-server architecture (cf. [PP CSP]) the security target shall claim additionally the package Trusted Channel between the TOE and the CSP in chapter 7. The trusted channel is necessary because the TOE and the CSP are implemented as separated devices and shall interact through a trusted channel in order to protect the integrity of the communication data and to prevent misuse of the CSP signing and time stamping service provided for the TOE.

The TOE meets the BSI Technical Guidance TR-03153 [TR TSEA] and uses cryptographic services of the CSP compliant with BSI TR-03116-5 [TR CryASE].

Method of use

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

The TOE generates time stamped and signed Log messages using the CSP cryptographic services in order to generate verifiable sequences of transaction data and Log messages for cash inspection (cf. [FCG] section146b).

The TOE provides security management of the TSF for administrators. The administrator starts and stops the normal operation of the TOE for import of transaction data, generation and export of Log messages and communication with the CSP. The security management configures the communication channels between the TOE with the CTSS interface component and the CSP. The TOE may support the security management of the CSP by providing a communication interface to an administrator or other services (e. g. to a time server).

The TOE supports receiving and integrity verification of Update Code Packages for installation of a new certified TOE sample or a non-certified security module application for electronic record-keeping system.

Non-TOE hardware/software/firmware available to the TOE

The TOE requires

– the CSP certified according to Common Criteria Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit [PPC-CSP-TS-Au] providing cryptographic security services and exporting audit records,

– the CTSS interface component providing the transaction data, and receiving Log messages.

The CSP shall meet BSI TR-03116-5 [TR CryASE]. The CSP shall export audit records in form of system logs meeting BSI TR-03151 [TR SE].

2 Conformance claims

2.1 CC conformance claims

The PP claims conformance to CC version 3.1 revision 5.

Conformance of this PP with respect to CC Part 2 [CCp2] (security functional components) is CC Part 2 extended.

Conformance of this PP with respect to CC Part 3 [CCp3] (security assurance components) is CC Part 3 conformant.

2.2 Package claim

This PP claims conformance to EAL2.

2.3 PP claim

This PP does not claim conformance to any other PP.

2.4 Conformance rationale

The PP requires exactly the components of EAL2 defined in CC part 3 [CCp3].

2.5 Conformance statement

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

3 Security problem definitions

3.1 Introduction

Assets

The assets of the TOE are

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

– the audit records imported from the CSP and exported to the CTSS interface component,

– the Update Code Package (UCP) imported and verified as user data..

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

Users and subjects

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

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

– *CTSS interface component*,

– *CSP* as sender of audit records,

– *Administrator*.

The *ERS* is tested by the TOE as external entity and communicating with the TOE through the *CTSS interface component*. The TOE uses also the *CTSS interface component* as passive external entity for storage of system logs. The TOE uses the CSP also as external entity providing security services (i. e. the CSP is passive communicating with the TOE).

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

Objects

The TSF operates the following types of user data objects

– *Transaction Data* (TD),

– *Audit records,*

– *Data To Be Signed* (DTBS),

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

– *Log message* (LM) as *Transaction log* or *System log,*

– *Update Code Package* (UCP).

The formats of *Transaction Data* and *Log messages* meet the BSI TR-03151 [TR SE].

The CTSS interface component provides *Transaction Data* as data to be certified by means of *Transaction logs* containing

– the clientID with the Identity of the CTSS interface device,
– the processData with
  - the *Transaction Type*,
  - the *Transaction Data*,
  - the *Monetary Type of Transaction*,
  - the *Serial number of ERS*
– the *Type of the Operation* as *StartTransaction*, *UpdateTransaction* or *FinishTransaction* provided by the command sent by the CTSS interface component to the TOE.

Audit records are data imported from CSP or may be generated by the TSF about TSF security events.

The *Data to be Signed* compiled by the TSF and sent to the CSP for signing and time stamping consists of

– certified data i. e.
  - in case of *Transaction log*: the *Transaction Data* with type of the certified data *Transaction log*, object identifier (id-SE-API-transaction-log): bsi-de (0.4.0.127.0.7.0) applications (3) sE-API (7) sE-API-dataformats(1) 1 (cf. [TR SE], chapter 2.3.1)
  - in case of *System log*: the *Audit Record* with type of the certified data *system log,* object identifier (id-SE-API-system-log): bsi-de (0.4.0.127.0.7.0) applications (3) sE-API (7) sE-API-dataformats(1) 2
– protocol data generated by the TSF
  - the *Transaction Number*,
  - the S*erial Number* as hash value of the signature-verification key,
  - the *Type of the Operation* as name of the API function whose execution is recorded by the *Log message*, i. e. *StartTransaction*, *UpdateTransaction* or *FinishTransaction*,
  - the *Optional protocol data* (may be empty).

The CSP adds to the *Data to be Signed*

– the *Time*, when the *Log message* is created,
– the *Signature counter* enumerating the signatures created with the signature-creation key.

The *Log message* consists of the

– the *Log message tag* and *Version of the Log message format*,
– the certified data,
– the protocol data,
– the signature consisting of the identifier of the signature algorithm, parameters as defined by the signature algorithm and the signature value (cf. [TR TSEA]).

Refer to [TR TSEA] for details of the Log messages format.

The *UCP* are user data which are imported by the TOE for installation a new cash register security module application.

Security attributes

Administrators known to the TOE have the security attributes stored in an *Authentication Data Record*

– *User Identity* (User-ID),

– *Authentication Reference Data*,

– *Role* with detailed access rights gained after successful authentication.

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

Passwords as *Authentication Reference Data* have the security attributes

– *status*: values initial password, operational password,

– *number of unsuccessful authentication attempts.*

The user uses authentication verification data to prove its identity to the TOE. The TSF uses Authentication Reference Data to verify the claimed identity of a user. The TSF supports human user authentication by knowledge where the authentication verification data is a password and the authentication reference data is a password or an image of the password e. g. a salted hash value.

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

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

– *Administrator role*: User in this role is allowed to perform management functions. The Administrator subject is acting on behalf of a human user after successful authentication as Administrator until logout. The *Administrator* is allowed to activate and to deactivate the role *CTSS interface*.

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

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

The *Transaction Data* have the security attributes

– *Serial number of the ERS* to determine the signature-creation key to be used for signing the *Transaction log* and the *Serial number* to be included in the protocol data of the *Transaction log,*

– *Type of the Operation* to determine the actual transaction as *StartTransaction, UpdateTransaction or FinishTransaction*.

– *Transaction number* to assign the TD to an ongoing transaction and enumerating the transactions continuously increasing without gaps.

The TOE accepts *Transaction Data* only if the serial number of the ERS is known, a signature key in the CSP and the *Serial number* is assigned to this ESR.

If the *Type of the Operation* is *StartTransaction* or *FinishTransaction* the TOE generates a *Transaction log* for the imported *Transaction Data*. If the *Type of the Operation* is *UpdateTransaction* the TOE may collect the imported *Transaction Data* and include them immediately or later on in one and only one *Transaction log* (cf. [TR SE]).

The TOE manages for each known ESR a list of the last assigned transaction number and the transaction numbers of the ongoing transactions of this ESR. If the *Type of the Operation* of imported *Transaction Data* is *StartTransaction* then a new transaction is started and the TOE generates a new *Transaction Number* by addition of 1 to the last assigned *Transaction Number*, includes this value in the protocol data of the *Transaction log* returned to the CTSS interface component, and add this value to the list of ongoing

transaction. If the *Type of the Operation* is *UpdateTransaction* or F*inishTransaction* and meets the *Transaction Number* of an ongoing transaction the *Transaction Number* in the Transaction Data is imported and assigned to the protocol data of the *Transaction log*. If the *Type of the Operation* is *FinishTransaction* or the transaction is terminated by the TOE the *Transaction Number* is removed from the list of ongoing transactions.

The *Log messages* have the security attributes in the protocol data and the signature used by the verifier of the cash inspection

– *Transaction number* assigning the *Log message* to the transaction of the electronic record-keeping system.
– *Signature counter* enumerating the *Log message* continuously increasing without gaps,
– *Time stamp* as time when the *Log message* was created,
– *Type of the Operation* to determine whether the *Log message* was created for the start, update and finishing the transaction of the electronic record-keeping system,
– *Serial number* to determine the certificate to be used for verification of the digital signatures as check value of the transaction data..

The verifier of the cash inspection should interpret the *Log message* to determine a transaction [KSV] section 2 sentence 2 as follows:

– number 1: the point in time when the transaction starts is the *Time stamp* of the *Log message* with the *Type of the Operation* equal to *StartTransaction* and the transaction number identified as number 2.
– number 2: the transaction number is the *Transaction number* in the protocol data of the *Log message*.
– number 3 the transaction type, number 4 the transaction data and number 5 the monetary type of transaction are contained in the certified data of all *Log messages* with the transaction number identified as number 2.
– number 6: the point in time when the transaction is completed or terminated is the *Time stamp* of the *Log message* with *Type of the Operation* equal to *FinishTransaction* and the transaction number identified as number 2.
– number 7: the check value is a set of signatures in the protocol data of all *Log messages* with the same *Transaction number* identified as number 2.
– number 8: the serial number of the security module generated for the transaction is contained in the protocol data of the *Log messages*.

The 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.

The UCP may have a version number.

3.2 Threats

T.EvadTD Evading *Transaction Data*
The attacker evades 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 though the CTSS interface component to the TOE, or generates forged *Transaction Data* and sends them to the TOE in order to generate wrong *Transaction logs*.

T.ManipDTBS Manipulation of Data To Be Signed and time stamped
The attacker generates forged or manipulates *Data To Be Signed* sent for signing and time stamping to CSP. A forged *Transaction log* may result in forged transaction data provided for cash inspection. A forged *system log* may result in faulty interpretation of the transaction data.

T.ManipLM Manipulation of a *Log message*
The attacker manipulates undetected a *Log message* exported to the CTSS interface component and used for cash inspection.

T.ManipLMS Manipulation of a *Log message sequence*
The attacker manipulates undetected the *Log message sequence* exported to the CTSS interface component and used for cash inspection.

T.ManipTN Manipulation of *Transaction Number*
The attacker manipulates the TOE internal *Transaction Number* used in *Log messages*.

T.FaUpD Faulty *Update Code Package*
An unauthorized entity provides an unauthorized faulty *Update Code Package* enabling attacks against integrity of TSF implementation, confidentiality and integrity of user data or TSF data after installation of the faulty *Update Code Package*.

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 on all transactions that are legally required (cf. [FCG] section 146a (1) sentence 1). The receipt shall include besides the transaction data the points in time when the transaction is started, completed or terminated, and the transaction number provided by the certified security device (cf. [KSV] section 6 sentence 1).

OSP.CertSecDev Certified security device
The electronic record-keeping system and the accounts and records generated by the electronic record-keeping system shall be protected by a certified security device (cf. [FCG] section 146a (1) sentence 2). The security module of the certified security device generates the time stamps, when the transaction starts and when the transaction is completed or terminated, and the transaction number (cf. [KSV] section 2 sentence 3).The security module of the certified security device shall be certified according to Federal Office's Common Criteria Protection Profiles.

OSP.ProtDev Protection of electronic record-keeping system and certified security device
The taxpayer shall use correctly the electronic record-keeping system (cf. [FCG] section 379 (1) sentence 1 number 4), and protect correctly the electronic record-keeping system and the certified security device (cf. [FCG] section 379 (1) sentence 1 numbers 5).

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

OSP.Update Authorized *Update Code Package*s
*Update Code Package*s are delivered to the TOE in encrypted form and signed by the authorized issuer. The TOE verifies the authenticity of the received *Update Code Package* using the CSP before storing in the TOE.

3.4 Assumptions

A.CSP Cryptographic service provider
The operational environment provides a cryptographic service provider certified according to a security target compliant the Common Criteria Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit [PPC-CSP-TS-Au]. The CSP exports audit records in form of system logs meeting BSI TR-03151 [TR SE].

A.ProtComCSP Protection of communication between TOE and CSP
The operational environment protects the integrity of communication data between the TOE and the CSP. In case of platform architecture of the CSP the CSP provides a secure execution environment for the TOE and protects the integrity of communication data with the TOE directly using the security services of the CSP.

Application note 1: The main part of the protection profile in hand assumes the TOE being implemented as software running on the CSP as secure execution platform (cf. Platform architecture [PP CSP]). In case of the Client-server architecture (cf. [PP CSP]) the security target shall claim additionally the package Trusted Channel between the TOE and the CSP in chapter 7. If the security module follows the client-server architecture, the CSP is assumed to use the trusted channel provided by the TOE.

A.ProtComERS Protection of communication between TOE and electronic record-keeping system
The electronic record-keeping system provides transaction data when the transaction starts, transaction data are updated, and the transaction is completed or terminated. The operational environment protects the integrity of communication data between the TOE and the electronic record-keeping system.

A.VerifLMS Verification of Log message Sequences
The operational environment verifies the digital signatures, the transaction numbers and the time stamps of the *Log messages* in the sequence in order to detect forged or missing *Log messages*. The certificate of the signature-verification data is securely distributed to the verifier.

4 Security objectives

4.1 Security objectives for the TOE

O.GenLM Generation of *Log messages*
The TSF shall generate *Transaction logs* containing

– *Transaction Data*, *Transaction Number* created by the TSF, and

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

O.ImpExp Import of *Transaction Data* from and Export of *Log message* to CTSS interface component
The TSF shall import *Transaction Data* from the electronic record-keeping system through the CTSS interface component, import *Audit records* from CSP and export *Log messages* to the CTSS interface component.

O.IAA Identification of external entities and authentication of Administrators
The TOE shall identify and test the external entities electronic record-keeping system and cryptographic service provider, and verify the claimed identity of the Administrators by means of password.

O.SecMan Security management
The TOE shall restrict the security management of TSF and TSF data to authenticated Administrators. The TSF prevents management of the *Transaction Number* generation.

O.TEE Test of external entities
The TSF shall test on electronic record-keeping system and cryptographic service provider connected to the TOE, allow generation of *Log messages* only if both pass the tests, and enter a secure state if any test fails.

O.TST Self-test and secure state
The TSF shall perform self-tests. The TSF enters a secure state if the self-test fails, the test of electronic record-keeping system fails, or the test of cryptographic service provider fails.

O.SecUCP Secure download and authorized use of *Update Code Package*
The TSF shall verify the authenticity of received encrypted *Update Code Package* and decipher authentic *Update Code Package* by means of the cryptographic service provider before it stores the *Update Code Package*. The TOE shall allow only authenticated Administrators to install *Update Code Package* for creation of a new security module application.

4.2 Security objectives for the operational environment

OE.ERS Trustworthy electronic record-keeping system
The taxpayer shall use correctly an electronic record-keeping system that provides separately, correctly, completely and in real time all *Transaction Data* that are legally required for generation of *Log messages* to the TOE. The electronic record-keeping system shall support its testing as external entity by the TOE. The electronic record-keeping system shall produce receipt including besides the transaction data the points in time when the transaction is started, completed or terminated, and the transaction number provided by the certified security device (i. e. the CSP).

OE.CSP Cryptographic service provider component
The operational environment shall provide a cryptographic service provider for the TOE that is certified as compliant with Common Criteria Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit [PPC-CSP-TS-Au]. The CSP shall export audit records in form of system logs meeting BSI TR-03151 [TR SE].

Application note 2: The Common Criteria Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit [PPC-CSP-TS-Au] requires the cryptographic service provider to provide security services for digital signing of *Transaction Data*, verification of signature of *Update Code Package*s, decryption of *Update Code Package*s, and time service. The CSP audit records shall be exported meeting [TR SE] in order to avoid transformation of the audit record into a Log message. The vendor of the TOE may provide the TOE together with a certified cryptographic service provider.

OE.CSPPlatform CSP as 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 3: In case of client-server architecture the TOE and the CSP are physically separated components and the TOE does not need the CSP as secure execution platform.

OE.Transaction Verification of Transaction
The operational environment shall verify the validity of *Log message Sequences* by verification of the digital signatures, the *Transaction Number*s as being consecutive without gaps, the points in time when the transaction starts as being consecutive increasing with increasing *Transaction Number*s and consider the *Log messages*. The taxpayer shall ensure that the cryptographic service provider holds digital signature creation data and a corresponding valid certificate that is linked to the taxpayer. The certificate shall be securely distributed to the verifier.

OE.SecOEnv Secure operational environment
The operational environment shall protect the electronic record-keeping system and the certified technical security system including the TOE against manipulation, perturbation and misuse. It protects the integrity of the communication between the electronic record-keeping system and the TOE.

OE.SecCommCSP Secure communication between TOE and CSP
The operational environment shall protect the integrity of the communication between the TOE and the cryptographic service provider.

Application note 4: The main part of the protection profile in hand assumes the TOE being implemented as software running on the CSP as secure execution platform (cf. Platform architecture [PP CSP]). In case of the Client-server architecture (cf. [PP CSP]) the security target shall claim additionally the package Trusted Channel between the TOE and the CSP in chapter 7. 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, the TOE shall support trusted channel functionality between the TOE and the CSP. The usage of the trusted channel is a specific form how the operational environment meets OE.SecCommCSP.

OE.SUCP Signed Update Code Packages
The issuer shall issue encrypted and digital signed secure *Update Code Package*s together with its security attributes.

4.3 Security objective rationale

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

	T.EvadTD	T.ManipTD	T.ManipDTBS	T.ManipLM	T.ManipLMS	T.ManipTN	T.FaUpD	OSP.SecERS	OSP.CertSecDev	OSP.ProtDev	OSP.ValidTrans	OSP.Update	A.CSP	A.ProtComCSP	A.ProtComERS	A.VerifLMS
O.GenLM	x			x	x						x					
O.IAA											x					
O.ImpExp					x						x					
O.SecMan						x					x					
O.SecUpCP							x					x				
O.TEE	x	x	x	x	x			x								
O.TST				x												
OE.CSP				x					x				x			
OE.CSPPlatform			x											x		
OE.ERS	x	x						x								
OE.SecCommCSP			x											x		
OE.SecOEnv	x	x	x	x	x			x		x					x	
OE.SUCP							x					x				
OE.Transaction											x					x

Table 1: 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 *Transaction logs* containing *Transaction Data*, *Transaction Number* generated by the TSF, and time stamps and digital signatures, therefore allowing to decide whether presented TD have corresponding TDS in the TDSS.

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

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

– The security objective for the operational environment OE.SecOEnv requiring the operational environment to protect the electronic record-keeping system, the TOE and the communication between them 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 on CTSS interface component connected to the TOE.

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

– The security objective for the operational environment OE.SecOEnv requiring the operational environment to protect the electronic record-keeping system and the TOE against manipulation and misuse,

The threat T.ManipDTBS “Manipulation of Data To Be Signed and time stamped” is mitigated by:

– The security objective for the TOE O.TEE requiring the TSF to test on CSP connected to the TOE.

– The security objective for the operational environment OE.SecOEnv “Secure operational environment” protecting the CSP and the certified technical security system including the TOE against manipulation, perturbation and misuse. 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.

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

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

– The security objective for the TOE O.GenLM “Generation of *Log messages“* by means of digital signature generated by CSP, which allows to detect manipulation of TDS according to OE.Transaction.

– The security objective for the TOE O.TEE “Test of external entities” requiring the TSF to test on CSP connected to the TOE.

– The security objective for the TOE O.TST “Self-test and secure state” detects failure and prevents generation of TDS if time source is not available or the test of CSP fails.

– The security objectives for the operational environment OE.CSP “Cryptographic service provider component” ensures the availability of certified CSP for generation of time stamps and digital signatures, and distribution of the certificate linked to the taxpayer for signature verification.

– The security objective for the operational environment OE.SecOEnv “Secure operational environment” protecting the CSP and the TOE against manipulation, perturbation and misuse of signature-creation service.

The threat T.ManipLMS “Manipulation of a *Log message sequence*” is countered by:

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

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

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

– The security objective for the operational environment OE.SecOEnv “Secure operational environment” protecting the CSP and the TOE against manipulation, perturbation and misuse of signature-creation service.

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

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

– The security objectives for the TOE O.SecUCP "Secure download and authorized use of *Update Code Package"* ensuring that only authentic *Update Code Package*s are stored and installed by authorized Administrators only.

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

– The security objective for the TOE O.TEE requiring the TSF to test the ERS as external entity.

– The security objective for the operational environment OE.ERS "Trustworthy electronic record-keeping system".

– The security objective for the operational environment OE.SecOEnv "Secure operational environment" protecting the CSP and the TOE against manipulation, perturbation and misuse of signature-creation service.

The organizational security policy OSP.CertSecDev "Certified security device" is directly enforced by the security objectives for the operational environment OE.CSP "Cryptographic service provider component" and the certification conform to the protection profile in hand.

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, TSF time stamps when the transaction starts, is completed or aborted, TSF *Transaction Number* and a digital signature of the *Transaction Data* created using the digital signature-creation service of cryptographic service provider,

– the security objectives for the TOE O.IAA "Identification of external entities and authentication of Administrators" requiring the TSF to authenticate the Administrators by means of password,

– the security objective for the TOE O.ImpExp "Import of *Transaction Data* from and Export of *Log message* to CTSS interface component" requiring the TSF to import *Transaction Data* from the electronic record-keeping system through the CTSS interface component and export *Log messages* to the CTSS interface component.

– the security objective for the TOE O.SecMan "Security management" preventing manipulation of the *Transaction Number*s and limiting the authorized manipulation of the time source to Administrators.

– The security objective for the operational environment OE.Transaction "Verification of Transaction" ensures the condition for verification of the digital signature of the TDS.

The organizational security policy OSP.Update "Authorized *Update Code Package*s" is implemented by the security objective for the operational environment OE.SUCP "Signed *Update Code Package*s" ensuring digital signature of secure *Update Code Package*s together with its security attributes and the security objectives for the TOE O.SecUCP "Secure download and authorized use of *Update Code Package*" ensuring verification of 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.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. In case of the platform architecture the OE.CSPPlatform requiring the CSP to provide a secure execution environment. In case of the client-server architecture the TOE and the CSP component are physically separated components. The integrity of the communication between the TOE and the CSP shall be protected by means of a trusted channel as provided by the CSP according to [PPC-CSP-TS-Au] and by the TOE claiming the package Trusted Channel between the TOE and the CSP, cf. chapter 7.

The assumption A.ProtComERS “Protection of communication between TOE and electronic record-keeping system” is directly implemented by the security objectives for the operational environment OE.SecOEnv “Secure operational environment” protecting the integrity of the communication between the electronic record-keeping system.

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

5 Extended component definition

The extended components FIA_API.1 and FCS_RNG.1 are used only in the package Package Trusted Channel between TOE and CSP, cf. chapter 7.

5.1 Authentication Proof of Identity (FIA_API)

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

Family Behaviour

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

Component levelling:

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

Management: FIA_API.1

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

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

Audit: FIA_API.1

There are no auditable events foreseen.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

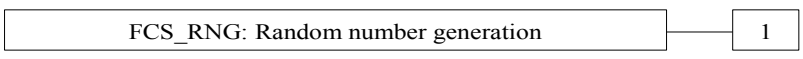
FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *object, authorized user or role*] to an external entity.

5.2 Generation of random numbers (FCS_RNG)

Family Behaviour

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

Component levelling:



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

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no auditable events foreseen.

FCS_RNG.1 Random number generation

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

6 Security requirements

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

6.1 Security functional requirements

6.1.1 Security Management

FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles: *Unidentified User, Administrator, CTSS interface role and CSP role [assignment: other roles]*[2].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: (1) *management of security functions behaviour (cf. FMT_MOF.1)*, (2) *management of Authentication Reference Data (cf. FMT_MTD.1/AD, FMT_MTD.3/PW),* (3) *management of security attributes (cf. FMT_MTD.3/PW, FMT_MSA.3, FMT_MSA.4),* (4) *[assignment: list additional of security management functions to be provided by the TSF]*[3].

2 [assignment: *authorised identified roles*]

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

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to

(1) *enable and disable*[4] the functions *password authentication according to FIA_UAU.5.2, clause (2) if defined*[5] to *Administrator*[6],

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

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

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

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

Application note 5: The refinements of FMT_MOF.1, bullet (2) to (5) are made in order to avoid iterations of the component. The life time of a transaction starts with receiving the *Transaction Data* with Type of Operation *StartTransaction*.

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the *Log message SFP and Update SFP*[19] to restrict the ability to

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

5 [assignment: *list of functions*]

6 [assignment: *the authorised identified roles*]

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

8 [assignment: *list of functions*]

9 [assignment: *the authorised identified roles*]

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

11 [assignment: *list of functions*]

12 [assignment: *the authorised identified roles*]

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

14 [assignment: *list of functions*]

15 [assignment: *the authorised identified roles*]

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

17 [assignment: *list of functions*]

18 [assignment: *the authorised identified roles*]

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

(1) *define the set of accepted values of*[20] the security attributes ~~*"Serial number of ERS"*~~[21] to *Administrator*[22],

(2) ***define depending on the Serial number of ERS***[23] **the** ***identity of the signature-creation key to be used for the Transaction log*** [24] ***to Administrator***[25]**,**

(3) ***define depending on the Serial number of ERS***[26] **the** ***Serial number in the protocol data of Transaction log***[27] ***to Administrator***[28]**,**

(4) ***define***[29] **the** ***identity of the signature-creation key to be used for the System logs and the Serial number in the protocol data of System logs*** [30] ***to Administrator***[31]**,**

(5) ***increase by 1***[32] **the** ***internally stored security attribute "Transaction Number" when transaction is started***[33] **to** ***subjects in CTSS interface role***[34]**,**

(6) ***modify***[35] **the** ***TD security attribute "Transaction Number" imported from the TD***[36] **to** ***none***[37]**,**

(7) ***modify***[38] **the** ***security attributes of UCP***[39] **to** ***none***[40]**.**

Application note 6: 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.

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

21 [assignment: *list of security attributes*]

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

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

24 [assignment: *list of security attributes*]

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

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

27 [assignment: *list of security attributes*]

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

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

30 [assignment: *list of security attributes*]

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

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

33 [assignment: *list of security attributes*]

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

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

36 [assignment: *list of security attributes*]

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

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

39 [assignment: *list of security attributes*]

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

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

FMT_MSA.3.1 The TSF shall enforce the *Log message SFP and Update SFP*[41] to provide *restrictive*[42] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *none*[43] to specify alternative initial values to override the default values when an object or information is created.

6.1.2 User identification and authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

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

(1) *Identity*,

(2) *Authentication Reference Data,*

(3) *Role*[44]

and

(a) security attribute *Identity* [assignment: *additional security attributes*] belonging to the ERS[45]

(b) security attribute *Identity* [assignment: *additional security attributes*] belonging to the SCP.

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

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

Hierarchical to: No other components.

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

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

(1) *delete and create*[46] [47] the *Authentication Data Record of all authorized users*[48] to *Administrator*[49].

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

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

43 [assignment: *the authorised identified roles*]

44 [assignment: *list of security attributes*]

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 authorised identified roles*]

(2) ***modify***[50] **the** ***Authentication Reference Data***[51] **to** ***the corresponding authorized user***[52].

FMT_MTD.3/PW Secure TSF data - Password

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data

FMT_MTD.3.1/PW The TSF shall ensure that only secure values are accepted for *passwords*[53] **and enforce changing initial passwords after first successful authentication of the 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 CTSS interface role after the ERS is successfully tested according to FPT_TEE.1.*

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

(3) *A subject is associated with attribute Identity and Administrator role after successful authentication.*

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

51 [assignment: *list of TSF data*]

52 [assignment: *the authorised identified roles*]

53 [assignment: list of TSF data]

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

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

(4) *The Administrator is allowed to activate and deactivate the CTSS interface role.*[56]

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

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

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

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

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide *password authentication*[58] to support user authentication.

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

(1) *password authentication shall be used for Administrator,*

(2) *[assignment: additional rules describing how the multiple authentication mechanisms provide authentication*][59].

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*[60].

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

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

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

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

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

6.1.3 User data protection

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

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/LM The TSF shall enforce the *Log Message SFP*[61] on

(1) *subjects:*

(a) subject acting for CTSS interface component,

(b) subject acting for CSP;

(2) *objects:*

(a) Transaction Data,

(b) Audit record,

(c) Data To Be Signed,

(d) protocolData with Signature,

(e) Log message;

(3) *operations:*

(a) import,

(b) export[62].

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

Hierarchical to: No other components.

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

FDP_ACF.1.1/LM The TSF shall enforce the *Log Message SFP*[63] to objects based on the following:

(1) *subjects:*

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

(b) subject in CSP role;

(2) *objects:*

(a) Transaction Data,

(b) Audit record,

(c) Data To Be Signed,

(d) protocolData with Signature,

(e) Log message[64].

61 [assignment: *access control SFP*]

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

63 [assignment: *access control SFP*]

64 [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*]

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

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

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

(b) export the DTBS of Transaction log to the CSP according to FDP_ETC.2/DTBS,

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

(d) export the Transaction log to the CTSS interface component according to FDP_ETC.2/LM.

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

(3) *A subject in CSP role is allowed to import Audit records from the CSP according to FDP_ITC.2/TSS and to export System logs to the CTSS interface component according to FDP_ETC.2/LM*[65].

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

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

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

(2) *User in other role than CSP role is not allowed to perform actions listed in FDP_ACF.1.2/LM clause (3).*[66]

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*[67] 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:

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

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

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

(1) *The TSF shall import the Transaction Data with the security attribute Serial Number of the ERS if the Serial Number of the ERS is in the set of accepted values according to FMT_MSA.1. If the Serial Number of the ERS is not in the set of accepted values the TSF must not import the Transaction Data.*

(2) *The TSF shall import the Transaction Data with the security attribute Type of the Operation.*

(3) *The Transaction Data shall be imported with the security attribute Transaction Number if the Type of the Operation is UpdateTransaction or FinishTransaction and the Transaction Number meets a Transaction Number of an ongoing transaction.*

(4) *The TSF shall import Audit records from CSP.*[68]

Application note 8: If the TOE is used by more than one taxpayer than each taxpayer shall use its own signature key identified by the serial numbers of ERS.

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*[69] when exporting ~~user data~~ **Data To Be Signed**, controlled under the SFP(s), ~~outside of the TOE~~ **to CSP**.

FDP_ETC.2.2/DTBS The TSF shall export the user data with the ~~user data's associated~~ s**ecurity attributes associated with Data To Be Signed**.

FDP_ETC.2.3/DTBS The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported ~~user data~~ **Data To Be Signed**.

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

(1) *Data To Be Signed shall be exported for generation of a Log message with security attribute identifying the private signature key to be used by FDP_DAU.2/TS according to [PPC-CSP-TS-Au].*[70]

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

FDP_ITC.2.1/TSS The TSF shall enforce the *Log message SFP*[71] when importing ~~user data~~ **protocolData with Signature and audit records**, controlled under the SFP, from ~~outside of the TOE~~ **CSP**.

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

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

68 [assignment: *additional importation control rules*]

69 [assignment: *access control SFP*]

70 [assignment: *additional exportation control rules*]

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

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

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

Application note 9: The CSP shall generate and return to the TOE at least the signature counter of the used signature-creation key, the time stamp and the signatures for the *Data To Be Signed* exported by the TOE according to FDP_ETC.2/DTBS. The CSP shall generate time stamps according to FDP_DAU.2/TS using time source according to FPT_STM.1 (cf. [PPC-CSP-TS-Au]). Note, the TOE of the protection profile in hand may use CSP providing time stamps by administrator settable internal clock (sf. Selection clause (4) in FPT_STM.1.1). If the CSP meets TR-03151 [TR SE] for the *Transaction logs* then the CSP returns a *Log message* to the TOE. If the CSP generates the time stamp and signatures with signature counter then the TOE shall compile the *Log message* according to TR-03153 [TR TSEA]. The signature counter and the time stamp of T*ransaction logs* and of audit data received as system logs may be used to test the CSP according to FPT_TEE.1.

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

Hierarchical to: No other components.

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

FDP_ETC.2.1/LM The TSF shall enforce the *Log message SFP*[72] when exporting user data **Log message**, controlled under the SFP(s), ~~outside of the TOE~~ **to CTSS interface component**.

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

FDP_ETC.2.3/LM The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4/LM The TSF shall enforce the following rules when user data is exported from the TOE: *Log messages shall be exported with security attribute*

(1) *Transaction logs:*

(a) Transaction number of the ERS transaction and 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] enumerating all Log messages,

(c) Type of the Operation,

(d) Time stamp when the Log message was signed,

(e) Serial Number as hash value of the public key for verification of the Signature,

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

(2) *Audit records of the CSP shall be exported unchanged as system logs to the CTSS interface component.*[73]

Application note 10: The CTSS interface component does not implement any security functionality addressed in this PP and imports and stores Log message received from the TOE as user data. The ERS uses the TDS fields 1,2, 6 and 8 for creation of receipts only. The TDS data fields number 1, 2, 6, 7 and 8 are used as security attributes of Log messages by the verifier of transactions for cash inspection.

72 [assignment: *access control SFP*]

73 [assignment: *additional exportation control rules*]

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) *Serial Number of the ERS*,

(2) *Type of the Operation,*

(3) *Transaction Number,*

(4) *Signature Counter,*

(5) *Time stamp,*

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

(7) *Signature*[74]

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use *BSI TR-03151 [TR SE] and BSI TR-03153 [TR TSEA]*[75] when interpreting the TSF data from another trusted IT product.

FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

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

FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes

(1) *Transaction Numbers building a strong increasing sequence without gaps,*

(2) *Time stamps of the Log messages building a not decreasing sequence with consideration of adjustments of the CSP time source*[76].

Application note 11: The rules may be enforced by internal storing of the *Transaction Number* and last time stamp provided by the CSP in the Log messages.

FMT_MSA.4 Security attribute value inheritance

Hierarchical to: No other components.

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

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

(1) T*he TSF uses the security attribute Serial Number of the ERS imported with Transaction Data to determine the signature-creation key be used by FDP_DAU.2/TS with ECDSA in [PPC-CSP-TS-Au] to sign the corresponding Log message as defined according to FMT_MSA.1.*

(2) *If the Type of the Operation of imported Transaction Data is StartTransaction then the last internally generated Transaction Number shall be increased by 1 and this value shall be assigned to the ongoing transaction and the Transaction log of imported Transaction Data.*

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

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

76 [assignment: *list of security attributes*]

(3) *If the Type of the Operation of imported Transaction Data is UpdateTransaction or FinishTransaction and meets the Transaction Number of an ongoing transaction then the Transaction Number of the imported Transaction Data shall be assigned to the protocol data of the Transaction log*.[77]

6.1.4 Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

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

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

(3) *test of CSP according to FPT_TEE.1 fails*[78].

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

Application note 12: The self-test according to FPT_TST.1 and test of external entities according to FPT_TEE.1 cause the secure state if the self-test or the tests fail. The exit of the secure state requires all conditions listed in the refinement being fulfilled.

FPT_TEE.1 Testing of external entities

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TEE.1.1 The TSF shall run a suite of tests *during start-up, periodically during normal operation, user initiated shutdown and before exiting the secure state according to FPT_FLS.1*[79] to check the fulfillment of

(1) ESR Identity [assignment: list of properties of the ESR] and

(2) CSP Identity [assignment: list of properties of the CSP][80].

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

FPT_TEE.1.2 If the test fails, the TSF shall *enter the secure state according to FPT_FLS.1 [selection: none additional action, [assignment: additional action(s)]*[81].

Application note 13: The Administrator may by able to define the actions in FPT_TEE.1 according to FMT_MOF.1.1 (5). E. g. the test of the ESR may include the interface used by the ESR for communication with the CTSS as reported by the CTSS interface component. The suite of tests determine whether the configured CSP is available for the TOE and Log messages can be signed. The TOE may use signature counter and time stamps received from CSP to test the CSP. The signature counter shall increase strong monotonically without gaps because any gap may indicate unauthorized signature-creation. The tests of the CSP should

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

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

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

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

81 [assignment: *action(s)*]

allow the CSP to identify the TOE as user of the CSP, cf. FIA_UID.1.1 clause (2) in [PP CSP]. Please refer for further explanations to the user notes and evaluator notes in CC part 2 [CCp2], chapter J.12.

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, at the request of the authorised user, periodically during normal operation and before exiting the secure state according to FPT_FLS.1*[82] to demonstrate the correct operation of *parts of TSF*[83].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of *TSF data*[84].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of *TSF **implementation***[85].

6.1.5 Code Update Package import

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

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/UCP The TSF shall enforce the *Update SFP*[86] on

(1) *subjects: Administrator;*

(2) *objects: Update Code Package*;

(3) *operations: import, decrypt*[87].

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

Hierarchical to: No other components.

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

FDP_ACF.1.1/UCP The TSF shall enforce the *Update SFP*[88] to objects based on the following:

(1) *subjects: Administrator;*

(2) *objects: Update Code Package with security attributes Issuer and Signature*[89].

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:

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

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

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

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

86 [assignment: *access control SFP*]

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

88 [assignment: *access control SFP*]

89 [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*]

(1) *Administrator is allowed to import and store received Update Code Package if*

(a) the digital signature of the UCP generated by the Issuer is successful verified by the CSP and

(b) the verified UCP is deciphered by means of CSP.[90]

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

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

(1) *Administrator is not allowed to import received Update Code Package if verification of digital signature by means of CSP fails*;

(2) [*assignment: other rules, based on security attributes, that explicitly deny access of subjects to objects*].[91]

Application note 14: The Administrator should be allowed to execute the stored *Update Code Package* if the version number of the *Update Code Package* is equal or higher than the version number of the TSF. The execution of UCP is outside the TSF-mediated functionality of the PP on hand.

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

Hierarchical to: No other components.

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

[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2.1/UCP The TSF shall enforce the *Update SFP*[92] when importing user data, controlled under the SFP, from outside of the TOE.

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

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

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

FDP_ITC.2.5/UCP The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

(1) *storing of encrypted Update Code Package only after successful verification by means of CSP,*

(2) *decrypts authentic Update Code Package by means of CSP*[93].

FDP_RIP.1/UCP Subset residual information protection

Hierarchical to: No other components

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

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

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

93 [assignment: *additional importation control rules*]

Dependencies: No dependencies.

FDP_RIP.1.1/UCP The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource* ***after unsuccessful verification of the digital signature of the issuer by means of CSP***[94] the following objects: *received Update Code Package* [95].

6.2 Security assurance requirements

The PP requires the TOE to be evaluated to EAL2.

6.3 Security requirements rationale

6.3.1 Dependency rationale

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

SFR	Dependencies of the SFR	SFR components
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_ITC.2/TD	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/LM Dependency on FTP_ITC.1 or FPT_TRP.1 is not fulfilled because secure import is ensured by OE.SecOEnv. FPT_TDC.1
FDP_ITC.2/TSS	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/LM Dependency on FTP_ITC.1 or FPT_TRP.1 is not fulfilled because secure import is ensured by OE.SecCommCSP in case of platform architecture. In case of client-server architecture FTP_ITC.1 is fulfilled, cf. chapter 7 (FTP_ITC.1/TC).

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

95 [assignment: *list of objects*]

SFR	Dependencies of the SFR	SFR components
FDP_ITC.2/UCP	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/UCP, 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 CSP uses the security attributes of UCP
FDP_RIP.1/UCP	No dependencies	
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_ATD.1	No dependencies	
FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.1
FIA_UAU.5	No dependencies	
FIA_UAU.6	No dependencies	
FIA_UID.1	No dependencies	
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1/LM, FDP_ACC.1/UCP FMT_SMR.1 FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FDP_ACC.1/LM, FDP_ACC.1/UCP, FMT_MSA.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1, FMT_SMR.1
FMT_MSA.4	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/LM
FMT_MTD.1/AD	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MTD.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
FPT_TDC.1	No dependencies	
FPT_FLS.1	No dependencies	

SFR	Dependencies of the SFR	SFR components
FPT_TEE.1	No dependencies	
FPT_TST.1	No dependencies	

Table 2: Dependency rationale

6.3.2 Security functional requirements rationale

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

	O.GenLM	O.ImpExp	O.IAA	O.SecMan	O.TEE	O.TST	O.SecUCP
FDP_ACC.1/LM	x	x					
FDP_ACC.1/UCP							x
FDP_ACF.1/LM	x	x					
FDP_ACF.1/UCP							x
FDP_ETC.2/DTBS	x						
FDP_ETC.2/LM		x					
FDP_ITC.2/TSS	x						
FDP_ITC.2/TD	x	x					
FDP_ITC.2/UCP							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			x
FMT_MSA.4	x	x		x			
FMT_MTD.1/AD			x	x			
FMT_MTD.3/PW			x	x			
FMT_SMF.1	x	x		x			
FMT_SMR.1	x	x	x	x			

	O.GenLM	O.ImpExp	O.IAA	O.SecMan	O.TEE	O.TST	O.SecUCP
FPT_TDC.1	x	x					
FPT_FLS.1					x	x	
FPT_TEE.1					x	x	
FPT_TST.1						x	

Table 3: Security functional requirements rationale

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

The security objective for the TOE O.GenLM “Generation of Log messages” is met by the following SFR:

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

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

– The SFR FDP_ETC.2/DTBS reuqires the TSF to export Data To Be Signed to CSP for time stamping and signature generation.

– The SFR FMT_MSA.1 clause (4) prevents the manipulation of the *Transaction Number*.

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

– The SFR FMT_MSA.3 ensures restrictive security attributes of *Log message* as defined and prevent alternative initial values of the security attributes of Log message.

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

– The SFR FMT_MOF.1 clause (2) , describes the behaviour of FMT_MSA.4 for *Serial Number* in the Log message.

– The SFR FMT_MOF.1, FMT_MTD.3/PW, FMT_MSA.3, FMT_MSA.4 defined for SFR FDP_ACC.1/LM and FDP_ACF.1/LM are listed in SFR FMT_SMF.1.

– The SFR FPT_TDC.1 ensures that the security attributes of the imported *Transaction Data* and of the exported *Log messages* are correctly interpreted.

The security objective for the TOE O.ImpExp “Import of *Transaction Data* from and Export of *Log message* to CTSS interface component” is met by the following SFR:

– The SFR FDP_ACC.1/LM and FDP_ACF.1/LM require access control on import of *Transaction Data*; and export of *Log messages* to CTSS interface component for roles defined by FMT_SMR.1.

– The SFR FDP_ITC.2/TD requires the TSF to import the *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 export of *Log messages* with security attributes defined by FMT_MSA.4 to CTSS interface component for generation of receipts and verification of *Log messages*.

– The SFR FPT_TDC.1 ensures that the security attributes imported with *Transaction Data* and exported with *Log messages* are correctly interpreted.

The security objective for the TOE O.IAA "Identification of external entities and authentication of Administrators" is met by the following SFR:

– The SFR FMT_SMR.1 lists the roles known to the TSF, where subject CTSS interface component is automatically started and identified only, and Administrator and CSP are requested to authenticated themselves according to FIA_UAU.5.

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

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

– The SFR FIA_UAU.5 defines the authentication mechanisms supported by the TSF.

– The SFR FMT_MOF.1.1 clause (1) defines the rule that additonal authentication (except for the Administrator itself) may be enabled and disabled by the Administrator.

– The SFR FIA_UAU.6 defines the condition for re-authentication.

– The SFR FIA_AFL.1 defines action if password authentication fails.

– The SFR FIA_ATD.1 defines the security attributes of users known to TSF and the SFR FIA_USB.1 require binding of these security attributes to successful authenticated users.

– The SFR FMT_MTD.1/AD and FMT_MTD.2/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 SFR:

– The SFR FMT_SMR.1 defines the roles known to TSF and requires the TSF to associate users with these roles.

– The SFR FMT_SMF.1 lists the management functions as management of functions FMT_MOF.1, management of TSF data FMT_MTD.1/AD and FMT_MTD.3/PW, and management of security attributes FMT_MSA.1, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4.

– The SFR FMT_MOF.1 restricts the ability to modify, enable, disable, determine the behaviour of and modify the behaviour of security functions to Administrator.

– The SFR FMT_MTD.1/AD and FMT_MTD.2/PW require 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 generation security attributes of TDS and TDSS including the security attributes time stamps.

– The SFR FMT_MSA.4 prevents management of the *Transaction Number*s.

The security objective for the TOE O.TEE "Test of external entities" is met directly by the SFR FPT_TEE.1. The SFR FMT_MOF.1, clause (5), restricts the definition and modification of the FPT_TEE.1 behaviour to the Administrator. The SFR FIA_ATD.1 defines the security attribute *Identity* for ESR and CSP tested by FPT_TEE.1. If any test fails the TSF enters a secure state according to FPT_FLS.1.

The security objective for the TOE O.TST "Self-test" is met by the following SFR:

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

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

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

The security objective for the TOE O.SecUCP “Secure download and authorized use of *Update Code Package*” is met by the following SFR:

– The SFR FDP_ACC.1/UCP and FDP_ACF.1/UCP requires the TSF to provide access control to enforce SFP *Update*. Note the verification of the authenticity of UCP and decryption of authentic UCP are performed by CSP under control of the TSF. The SFR FMT_MSA.1 prevents the modification of security attributes of UCP.

– The SFR FDP_ITC.2/UCP requires the TSF to import UCP as user data with security attributes if the authenticity of UCP is successful verified.

– The SFR FMT_MSA.3 requires to provide restrictive initial security attributes to enforce the SFP *Update*.

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

6.3.3 Security assurance requirements rationale

The 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.

7 Package Trusted Channel between TOE and CSP

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

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

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

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

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

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

Table 4: Elliptic curves, key sizes and standards

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*[96] 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*[97].

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 ICC role with establishment of trusted channel according to FTP_ITC.1/TC,*

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

(3) *message authentication by MAC verification of received messages*[98]

to support user authentication.

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

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

(2) *message authentication by MAC verification of received messages shall be used after initial authentication of remote entity according to clause (1) for trusted channel according to FTP_ITC.1/TC*[99].

Application note 15: The ST writer may assign another method of mutual authentication with key establishment in FIA_UAU.5.1/TC clause (2) if this method is supported by the certified CSP and therefore meets the OSP.SecCryM "Secure cryptographic mechanisms" in [PP CSP].

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a *PACE in PCD role*[100] to prove the identity of the *TOE*[101] to ~~an external entity~~ **CSP and establishing a trusted channel according to FTP_ITC.1/TC**.

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

Hierarchical to: No other components.

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys ***for FCS_COP.1*** in accordance with a specified cryptographic generation algorithm *PACE with [selection: elliptic curves in table 4] and*

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

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

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

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

100 [assignment: *authentication mechanism*]

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

Generic Mapping in PCD role[102] and specified cryptographic key sizes *256 bits*[103] that meet the following: *[ICAO], section 4.4*[104].

Application note 16: PACE is used to authenticate the TOE and the CSP. It establishes a trusted channel with MAC integrity protection of the following communication trough the trusted channel.

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

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

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

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

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

FCS_COP.1.1 The TSF shall perform *MAC calculation and MAC verification*[105] in accordance with a specified cryptographic algorithm *according to AES-256* [*FIPS197] in [selection: CMAC (NIST SP800-38B [NIST2005]), GMAC (NIST SP800-38D[NIST2007]), HMAC (FIPS PUB 198-1 [NIST2008])]*[106] and cryptographic key sizes *256 bits*[107] that meet the following: *the referenced standards above according to the chosen selection*[108].

The following extended components are defined in [PP CSP] and used here for key generation 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*][109] random number generator that implements: [assignment: *list of security capabilities*].

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

Application note 17: The TOE is defined as as software running on the CSP platform (referred as Platform architecture in [PP CSP]) or as device (referred as Client-server architecture in [PP CSP]). The TOE may use internal source or external source or more than one source of randomness providing seeds of at least 125

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

103 [assignment: *cryptographic key sizes*]

104 [assignment: *list of standards*]

105 [assignment: *list of cryptographic operations*]

106 [assignment: *cryptographic algorithm*]

107 [assignment: *cryptographic key sizes*]

108 [assignment: *list of standards*]

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

bits entropy. The deterministic part of the RNG shall meet BSI TR3116-5 [BSI CryASE] and therefore of class DRG.3 or higher according to [AIS20].

The dependencies are fulfilled:

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

Table 5: Dependency rationale for the functional package

The security objective for the TOE O.SecCommCSP “Trusted channel between TOE and CSP” is implemented by the SFR

– FTP_ITC.1/TC Inter-TSF trusted channel directly requiring the trusted channel between the TOE and the CSP protecting the integrity for their communication.

– FIA_UAU.5/TC requires the TSF to authentication the CSP as communication end point of the trusted channel.

– FIA_API.1 requires the TSF to authentication themselves as communication end point of the trusted channel to the CSP.

– FCS_CKM.1 requires the TSF to generate MAC keys for FCS_COP.1.

– FCS_CKM.4 requires secure key destruction in order to fulfill the dependency of FCS_CKM.1.

– FCS_COP.1 requires the TSF to calculate MAC for the own messages and to verify MAC for the CSP messages.

– FCS_RNG.1 requires the TSF to implement a random number generator used for key generation according to FCS_CKM.1.

8 Reference Documentation

[CCp1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1, Revision 5, April 2017

[CCp2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017

[CCp3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components;CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

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

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

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

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

[PPC-CSP-TS-Au] Common Criteria Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit

[TR ECC] BSI, Elliptic Curve Cryptography, BSI Technical Guideline TR-03111, Version 2.0, 2012, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_pdf.html

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

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

[TR TSEA] Technische Richtlinie BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, Version 1.0, 5. Juni 2018

[ASI20] BSI AIS 20/31, A proposal for: Functionality classes for random number generators, Version 2.0, 2011

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

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

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

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

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

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

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

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

Keywords and Abbreviations

Term	Description
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]
tax authorities	authority inspecting accounts and records in form of *Log messages*
certified technical security system (“zerti-fizierte technische Si-cherheitseinrichtung”)	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)

Table 6: Terminology

Abbreviations	Term
A.xxx	Assumption
CC	Common Criteria
CSP	cryptographic service provider, the TOE of [PP CSP]
CTSS	certified security device 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
T.xxx	Threat
TD	Transaction data
TDS	Transaction data set

Abbreviations	Term
TDSS	Transaction data set sequence
TOE	Target of Evaluation
TSF	TOE security functions
UCP	*Update Code Package*

Table 7: Abbreviations