cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems

Security Target

BSI-DSZ-CC-1120

Common Criteria / ISO 15408

EAL 2

Document Version 1.4 • 2020-04-06

cv cryptovision GmbH • Munscheidstr. 14 • 45886 Gelsenkirchen • Germany
www.cryptovision.com • info@cryptovision.com • +49-209-167-2450

Content

Version Control

Version	Date	Author	Changes to Previous Version
0.1	2019-12-14	Thomas Zeggel	Initial version
0.2	2019-01-14	Thomas Zeggel	New version based on preliminary version 0.71 of the protection profile.
0.3	2019-04-10	Thomas Zeggel	First version for certification start based on final (certified) protection profile (version 0.7.5). Still missing: Details of the lifecycle (chapter 1), description of the TSF_group to SFR mapping in chapter 8.
0.4	2019-06-24	Thomas Zeggel	Version after observation report v1.
0.5	2019-07-31	Thomas Zeggel	Version after observation report v3.
0.6	2019-09-10	Thomas Zeggel	Version after observation report v5. Life-cycle definition adjusted in section 1.3.8.
0.7	2019-10-30	Thomas Zeggel	Version after observation report 1120_OR_ADV_SMAERS_v3 with changes based on ADV document evaluation.
0.8	2019-11-29	Thomas Zeggel	Version after comments from certification body: comments regarding lifecycle added, notes regarding usage of CSP functionality added. Third party applet in figure 2 deleted. “BSI-CC-PP-0107-2019” added in reference [PPC-CSP-TS-Au].
0.9	2019-11-29	Thomas Zeggel	TOE identification modified (direct reference to SMAERS preparational Guidance).
1.0	2020-02-14	Thomas Zeggel	Small modifications regarding basic architecture and life cyle.
1.1	2020-02-27	Thomas Zeggel	Typos and details of TOE production corrected.
1.2	2020-03-04	Thomas Zeggel	Developer note added, minor modifications.
1.3	2020-03-11	Thomas Zeggel	Minor modifications after TÜVIT and BSI comments in section 1.4.2, 1.5 and references.
1.4	2020-04-06	Thomas Zeggel	Details regarding delivery added (section 1.5).

1 Introduction

1.1 ST/TOE Identification

Title:	cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems– Security Target
Document Version:	v1.4
Origin:	cv cryptovision GmbH
Compliant to:	Common Criteria Protection Profile – Security Module Application for Electronic Record-keeping Systems, BSI-CC-PP-0105-2019 [PP0105]
TOE identification:	cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems, version 1.0
Short TOE name:	cryptovision SMAERS
CSP platform:	cryptovision CSP
Javacard OS platform:	NXP SE050 JCOP 4, [Zert_OS]
TOE documentation:	Administration and user guide [Guidance], [Guidance_OPE]

1.2 ST overview

This document contains the security target for the product cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems – for a Common Criteria certification according to EAL2. It is designed to be used exclusively on the cryptovision CSP, which is certified according to CC EAL 4+ ([PP CSP] with PP-module [PPC-CSP-TS-Au]) and itself is a composite product based on the NXP SE050 JCOP 4 Javacard OS platform, which is certified according to CC EAL 6+ [ZertOS].

This security target defines the security objectives and requirements for the cryptovision SMAERS.

This security target claims strict conformance to the Protection Profile *Common Criteria Protection Profile – Security Module Application for Electronic Record-keeping Systems*, BSI-CC-PP-0105-2019 [PP0105]. The main objectives of this ST are:

- to introduce the TOE (SMAERS application),
- to define the scope of the TOE and its security features,
- to describe the security environment of the TOE, including the assets to be protected and the threats to be countered by the TOE and its environment during the product development, production and usage,
- to describe the security objectives of the TOE and its environment supporting in terms of integrity and confidentiality of application data and programs and of protection of the TOE,
- to specify the security requirements which includes the TOE security functional requirements, the TOE assurance requirements and TOE security functionalities.

The assurance level for the TOE is CC EAL2.

1.3 TOE overview

The TOE overview follows the description in the protection profile [PP0105].

1.3.1 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]).

1.3.2 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.

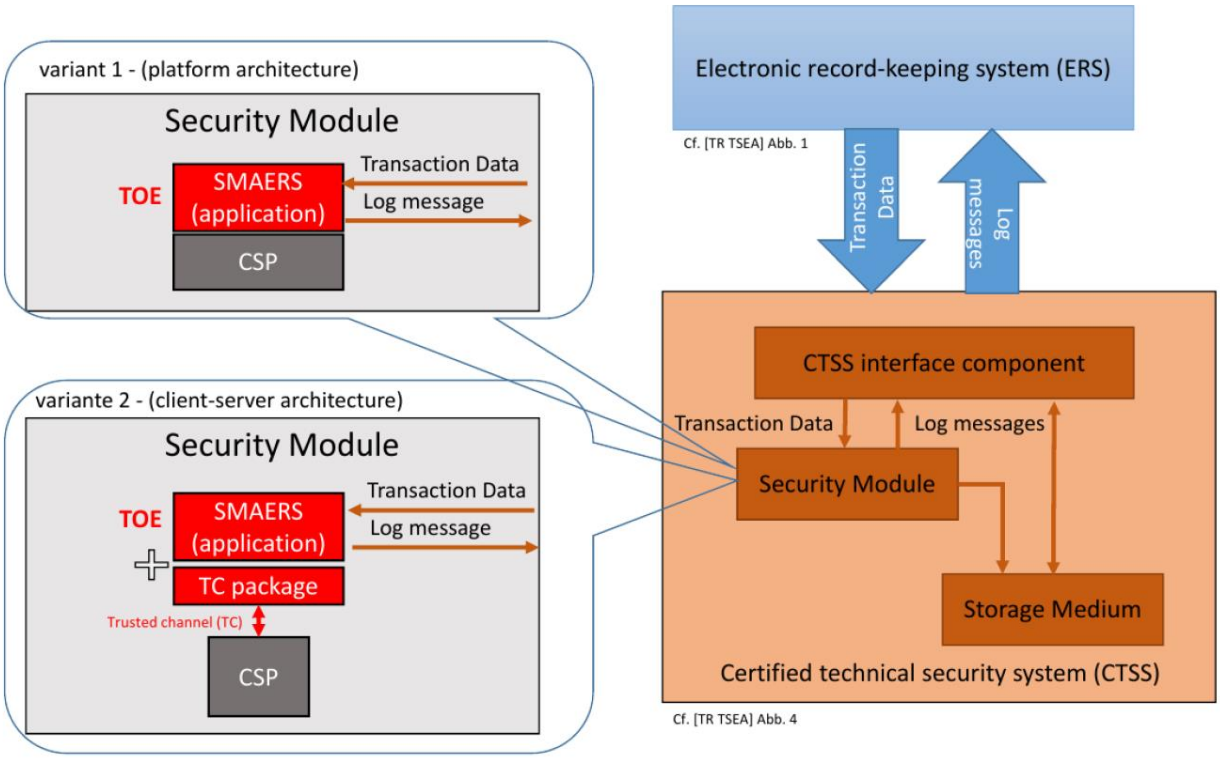

Figure 1: Description and interaction between the TOE and the relevant non-TOE components

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.

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 Systems 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,
- 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 implemented in 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].

The TOE is a software application running on a defined combination of hardware and software (cryptovision CSP), thus the TOE is implemented as software running on the CSP as secure execution platform (cf. Platform architecture [PP CSP]). The TOE is implemented as two Javacard applets.

1.3.3 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] section 146b).

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

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

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[2] 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.

1.3.4 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].

1.3.5 TOE and TOE platform

The specific The Target of Evaluation (TOE) of this ST (Cryptovision SMAERS) is an application to be used on the Cryptovision CSP, which is certified according to [PP CSP] with PP-module [PPC-CSP-TS-Au]. The TOE is a security module application implemented as software running on the CSP platform (referred as Platform architecture in [PP0104]).

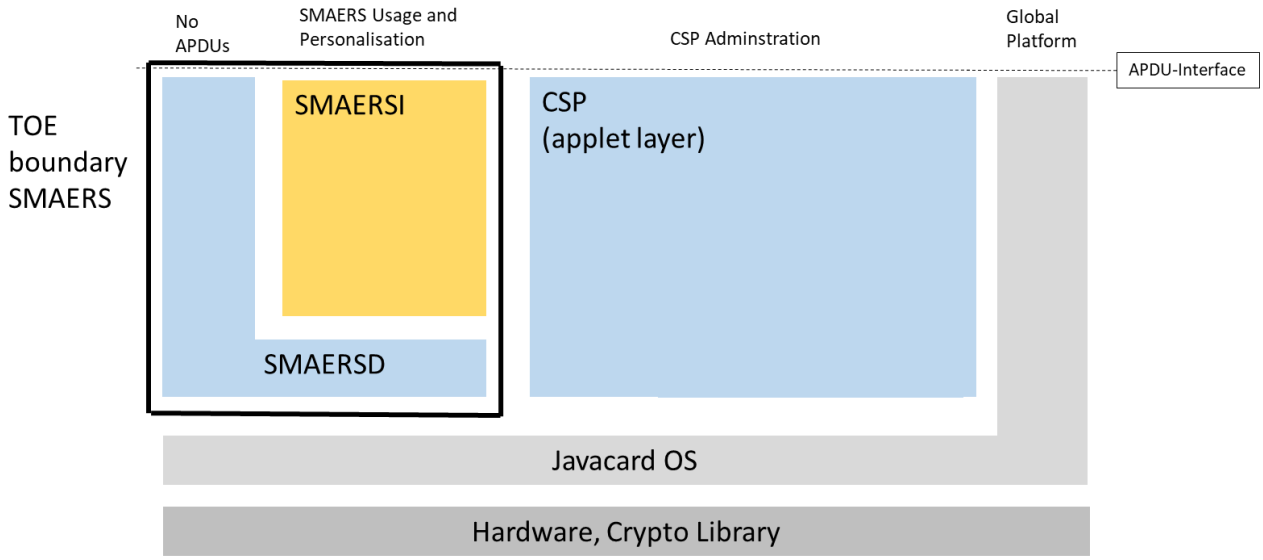

Figure 3: Structure of the TOE (SMAERS) and TOE boundary.

The SMAERS application consists of a data storage applet (SMAERSD) and a separate applet implementing the logic functionality and the APDU interface. Security functionality is provided by the CSP platform.

[2] This is the case for the TOE, which comprises the interface for an „time admin“ to set the internal time of the CSP.

When updating the SMAERS application, data reside in the SMAERSD applet, while the SMAERSI applet can be updated. Thus, all internal data are unchanged by the update process.

1.3.6 Major security features of the TOE

The TOE provides the security functionality as described in section 1.3.3. The specific cryptographic functionality is completely provided by the CSP platform and described in detail in [ST_CSP].

1.3.7 TOE identification

Identification of the TOE is performed by a GET DATA command according to the procedure described in [AGD_PRE], section 3.2.4.

1.4 TOE life cycle

The TOE lifecycle is not defined in the protection profile [PP0105].

1.4.1 Development and delivery of the TOE

The target platform of the TOE (cryptovision SMAERS) is the cryptovision CSP. The cryptovision CSP comprises of the NXP SE050 product, which itself is a composite product based on the certified hardware, certified crypto library and the certified Java card operating system layer. The development and certification of the NXP SE050 product is in the hands of NXP. The CSP package of cryptovision adds the necessary functionality to this Java Card platform to build a CSP according to [PP0104] and [PPC-CSP-TS-Au].

The cryptovision SMAERS was developed at cryptovision to add the functionality necessary to be used in a TSE technical device[3] according to the technical guidelines [TR-03151] and [TR-03153].

After completion of the development, the CSP application layer and the SMAERS application are delivered from cryptovision to D-Trust in a secure way (encrypted and digitally signed).

This delivery is the delivery of the TOE (SMAERS) according to Common Criteria.

1.4.2 Production of the TOE

Please note that the following steps are outside of the scope of the Common Criteria certification.

The TOE (the SMAERS application) is loaded on the CSP in the D-Trust high security Certificate Authority (CA) environment (encrypted and digitally signed) using standard Global platform mechanisms with delegated management. The CSP has been produced at D-Trust previously based on the CSP application and encrypted keys delivered by cryptovision and JCOP4 Java Card OS chips delivered by NXP.[4]

The main signature key of each SMAERS/CSP combination (embedded in the TSE) is generated on-card in the premises of D-Trust, the public key is exported and a certificate is generated using certified standard procedures at D-Trust (certified according to BSI TR-03145 [TR03145]). This certificate is stored in the SMAERS application.

During these initialization and personalization steps, D-Trust follows the TOE Preparation Guidance [Guidance] to provide the TOE in certified configuration. These steps are described in [PKIkonzept].

Afterwards, the TOE is delivered to the end-customer (embedded in the TSE).

[3] Technische Sicherheitseinrichtung

[4] The SE050 chips have been produced at NXP and integrated in an MicroSD card at a third party. Nonetheless, during this step the SE050 chips remain in a secured state.

1.5 TOE deliverables

The TOE is delivered to D-Trust in an PGP encrypted and signed email. The delivery constitutes the following items:

- SMAERSI applet, Version 0x0105 (Revision 0x3D15) embedded in APDUs with encrypted load files and digitally signed using DAP.
- SMAERSD applet, Version 0x0105, embedded in APDUs with encrypted load files and digitally signed using DAP.
- Preparation Guidance (AGD_PRE) as PDF file [Guidance], Version 1.0.14, Date 2020-04-02.
- Operational Guidance (AGD_OPE) as PDF file [Guidance-OPE], Version 1.0.14, Date 2020-04-01.

2 Conformance claims

2.1 CC conformance claims

The security target claims conformance to CC version 3.1 revision 5.

Conformance of this security target with respect to CC Part 2 [CC_2] (security functional components) is CC Part 2.

Conformance of this security target with respect to CC Part 3 [CC_3] (security assurance components) is CC Part 3 conformant.

2.2 Package claim

This security target claims conformance to EAL2.

2.3 PP claim

This security target claims strict conformance to

- Common Criteria Protection Profile – Security Module Application for Electronic Record-keeping Systems, BSI-CC-PP-0105-2019 [PP0105].

2.4 Conformance rationale

The ST requires exactly the components of EAL2 defined in CC part 3 [CC_3].

2.5 Dedicated platform

The TOE is dedicated to be used on the platform cryptovision CSP, which is certified according to [PP CSP] with PP-module [PPC-CSP-TS-Au].

The identification of the platform is described in [Guidance], section 3.2.4.

3 Security problem definition

This chapter has been taken from [PP0105].

3.1 Introduction

3.1.1 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.

3.1.2 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 and Time 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.

3.1.3 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 the 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-05351 [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 Serial 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.

3.1.4 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 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.
- Time Administrator role: User in this role is allowed to set the time of the CSP platform.
- 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 rolle.
- 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 ERS.

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 ERS a list of the last assigned transaction number and the transaction numbers of the ongoing transactions of this ERS. 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 FinishTransaction 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 the Log messages 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

3.2.1 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.

3.2.2 T.ManipTD Manipulation of Transaction Data

The attacker manipulates Transaction Data sent by the electronic record-keeping system through the CTSS interface component to the TOE, or generates forged Transaction Data and sends them to the TOE in order to generate wrong Transaction logs.

3.2.3 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.

3.2.4 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.

3.2.5 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.

3.2.6 T.ManipTN Manipulation of Transaction Number

The attacker manipulates the TOE internal Transaction Number used in Log messages.

3.2.7 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

3.3.1 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).

3.3.2 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.

3.3.3 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).

3.3.4 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.

3.3.5 OSP.Update Authorized Update Code Packages

Update Code Packages 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

3.4.1 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].

3.4.2 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.

PP application note 1: <applied>

3.4.3 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.

3.4.4 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

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment. The content has been taken from [PP0105].

4.1 Security Objectives for the TOE

This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organizational security policies to be met by the TOE.

4.1.1 O.GenLM Generation of Log messages

The TSF shall generate Transaction logs containing

- Transaction Data, Transaction Number generated by the TSF, and
- time stamps and digital signatures created by the cryptographic service provider.

4.1.2 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.

4.1.3 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.

4.1.4 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.

4.1.5 O.TEE Test of external entities

The TSF shall test on electronic record-keeping system and cryptographic service provider connected to the TOE, allows generation of Log messages only if both pass the tests, and enters a secure state if any test fails.

4.1.6 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.

4.1.7 O.SecUCP Secure download and authorized use of Update Code Package

The TSF shall verify the authenticity of received encrypted Update Code Package and decrypt 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

4.2.1 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.

4.2.2 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].

PP 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 Packages, decryption of Update Code Packages, 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.[5]

4.2.3 OE.CSPPlatform CSP as secure platform of the TOE

In case of the platform architecture[6] the CSP provides a secure execution environment and security services for the TOE running on top.

PP application note 3: <applied>

4.2.4 OE.Transaction Verification of Transaction

The operational environment shall verify the validity of Log message Sequences by verification of the digital signatures, the Transaction Numbers as being consecutive without gaps, the points in time when the transaction starts as being consecutive increasing with increasing Transaction Numbers 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.

[5] The TOE of this ST is provided together with a cryptographic service provider (cryptovision CSP).

[6] This is the case for the TOE.

4.2.5 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.

4.2.6 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.

PP application note 4: <applied>

4.2.7 OE.SUCP Signed Update Code Packages

The issuer shall issue encrypted and digital signed secure Update Code Packages 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.

The rationale has been taken from the protection profile [PP0105].

	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				

	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
OE.Transaction											x					x

Table 1: Overview of the security objectives coverage

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[7] 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 [PP CSP] 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.TDSVerif.
- 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 Packages are stored and installed by authorized Administrators only.

[7] Not relevant for the TOE, since it uses a secure platform architecture.

- The security objective for the operational environment OE.SUCP ensures that the authentic Update Code Packages 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 security target 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 Numbers 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 Packages” is implemented by the security objective for the operational environment OE.SUCP “Signed Update Code Packages” ensuring digital signature of secure Update Code Packages 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[8] 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”.

[8] Not relevant for the TOE, since it uses a secure platform architecture.

5 Extended Component Definition

The extended components defined in [PP0105] (FIA_API.1 and FCS_RNG.1) are used only in the package Package Trusted Channel between TOE and CSP, cf. chapter 7 of [PP0105], and thus are not relevant for this security target. No extended components are defined for this security target.

6 IT Security Requirements

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph 8.1 of Part 1 [CC_1] of the CC. Each of these operations is used in this ST and the underlying PP.

Operations already performed in the underlying Protection Profiles ([PP CSP], [PPC-CSP-TS-Au]) are uniformly marked by ***bold italic*** font style; for further information on details of the operation, please refer to the protection profile.

Operations performed within this Security Target are marked by **bold underlined** font style; further information on details of the operation is provided in foot notes.

6.1 Security functional requirements

6.1.1 Security Management

6.1.1.1 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,*** **Time Administrator**[9]***.***
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Developer note: The Time Administrator is directly connected to the according role in the CSP platform.

6.1.1.2 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)*** **None**[10]***.***

Developer note: Please note that the necessary security functionality for the SFR above is provided by the CSP platform.

6.1.1.3 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

[9] [assignment: other roles]

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

(1) enable and disable the function ***password authentication according to FIA_UAU.5.2, clause (2) if defined*** to ***Administrator,***

(2) determine the behaviour of and modify the behaviour of 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 to Administrator,

(3) determine the behaviour of the function FPT_TEE.1 by definition of the identity and features to be tested of ERS to Administrator,

(4) determine the behaviour of the function FPT_TEE.1 by definition of the identity and features to be tested of CSP to Administrator,

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

PP 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.

6.1.1.4 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*** to restrict the ability to
	(1) define the set of accepted values of the security attribute ***"Serial number of ERS"*** to ***Administrator,***
	(2) define depending on the Serial number of ERS the identity of the signature-creation key to be used for the Transaction log to Administrator,
	(3) define depending on the Serial number of ERS the Serial number in the protocol data of Transaction log to Administrator,
	(4) define 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 to Administrator,
	(5) increase by 1 the internally stored security attribute "Transaction Number" when transaction is started to subjects in CTSS interface role,
	(6) modify the TD security attribute "Transaction Number" imported from the TD to none,
	(7) modify the security attributes of UCP to none.

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

6.1.1.5 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes
	FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce ***the Log message SFP and Update SFP*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

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

6.1.2 User identification and authentication

6.1.2.1 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 ***Administrator:***

(1) Identity,

(2) Authentication Reference Data,

(3) Role

and

(a) security attribute Identity, **none**[11] ***belonging to the ERS***

(b) security attribute Identity, **none**[12] ***belonging to the CSP.***

PP 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.

6.1.2.2 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*** the ***Authentication Data Record of all authorized users*** to ***Administrator***.

(2) ***modify the Authentication Reference Data to the corresponding authorized user***.

6.1.2.3 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 and enforce changing initial passwords after first successful authentication of the user to a different secure operational password.***

6.1.2.4 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

[11] [assignment: additional security attributes]

[12] [assignment: additional security attributes]

FIA_AFL.1.1	The TSF shall detect when **an administrator configurable positive integer within 1-15**[13] [14] unsuccessful authentication attempts occur related to **PIN-based authentication** [15].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been **met**[16], the TSF shall **delay the next authentication attempt or block the authentication, configurable by the administrator**[17].

6.1.2.5 FIA_USB.1 User-subject binding

Hierarchical to:	No other components.
Dependencies:	FIA_ATD.1 User attribute definition
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: ***(1) Identity,*** ***(2) Role.***
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: ***the initial role of the user is Unidentified user***.
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: ***(1) 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.*** ***(4) The Administrator is allowed to activate and deactivate the CTSS interface role.***

6.1.2.6 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.

6.1.2.7 FIA_UAU.1 Timing of authentication

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification

[13] [assignment: range of acceptable values]

[14] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

[15] [assignment: list of authentication events]

[16] [selection: met, surpassed]

[17] [assignment: list of actions]

FIA_UAU.1.1	The TSF shall allow ***(1) self test according to FPT_TST.1,*** ***(2) testing of external entity ERS according to FPT_TEE.1 and 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) none,***[18] 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.

6.1.2.8 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1	The TSF shall provide ***password authentication*** 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) none***[19]***.***

6.1.2.9 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***.

6.1.3 User data protection

6.1.3.1 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*** 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,***

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

[19] [assignment: additional rules describing how the multiple authentication mechanisms provide authentication]

(e) Log message;

(3) operations:

(a) import,

(b) export.

6.1.3.2 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*** 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.

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.

FDP_ACF.1.3/LM The TSF shall explicitly authorise access of subjects to objects based on the following additional rules***:*** **None.**[20]

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).

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

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

6.1.3.3 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*** when importing ***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 ***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 ***Transaction Data*** received.
FDP_ITC.2.4/TD	The TSF shall ensure that interpretation of the security attributes of the imported ***Transaction Data*** is as intended by the source of the user data.
FDP_ITC.2.5/TD	The TSF shall enforce the following rules when importing user data ***Transaction Data*** controlled under the SFP from outside of the TOE: ***(1) The TSF shall import the Transaction Data with the security attribute 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.***

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

6.1.3.4 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 when exporting ***Data To Be Signed,*** controlled under the SFP(s), ***to CSP.***
FDP_ETC.2.2/DTBS	The TSF shall export the user data with the 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 ***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].

6.1.3.5 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*** when importing ***protocolData with Signature and audit records***, controlled under the SFP, from ***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 ***protocolData with Signature and audit records*** received.
FDP_ITC.2.4/TSS	The TSF shall ensure that interpretation of the security attributes of the imported ***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 ***protocolData with Signature and audit records*** controlled under the SFP from ***CSP***: **None.**[21]

PP 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 security target in hand uses CSP providing time stamps by administrator settable internal clock (sf. Selection clause (4) in FPT_STM.1.1). The CSP meets TR-03151 [TR SE] for the Transaction logs and returns a Log message to the TOE. The CSP generates the time stamp and signatures with signature counter; the TOE shall compile the Log message according to TR-03153 [TR TSEA]. The signature counter and the time stamp of Transaction logs and of audit data received as system logs are used to test the CSP according to FPT_TEE.1.

6.1.3.6 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*** when exporting user data ***Log message***, controlled under the SFP(s), ***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***

[21] [assignment: additional importation control rules]

(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.

PP application note 10: The CTSS interface component does not implement any security functionality addressed in this ST 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.

6.1.3.7 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*** 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]*** when interpreting the TSF data from another trusted IT product.

6.1.3.8 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.***

PP application note 11: The rules are enforced by iusing certified functionality of the CSP.

6.1.3.9 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) The 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.

(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.

6.1.4 Protection of the TSF

6.1.4.1 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

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

(3) test of CSP according to FPT_TEE.1 fails.

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

PP 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.

6.1.4.2 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*** to check the fulfillment of

(1) ERS Identity, **none**[22] ***and***

(2) CSP Identity, **none**[23]***.***

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

[22] [assignment: list of properties of the ERS]

[23] [assignment: list of properties of the CSP]

FPT_TEE.1.2 If the test fails, the TSF shall ***enter the secure state according to FPT_FLS.1,*** **none additional action.**[24]

PP application note 13: The Administrator may be able to define the actions in FPT_TEE.1 according to FMT_MOF.1.1 (5). E. g. the test of the ERS may include the interface used by the ERS 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 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 [CC_2], chapter J.12.

6.1.4.3 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*** to demonstrate the correct operation of **parts of TSF.**

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

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

6.1.5 Code Update Package import

6.1.5.1 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*** on

(1) subjects: Administrator;

(2) objects: Update Code Package;

(3) operations: import, decrypt.

6.1.5.2 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*** to objects based on the following:

(1) subjects: Administrator;

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

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:

[24] [selection: none additional action, [assignment: additional action(s)]

(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.

FDP_ACF.1.3/UCP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**[25]

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) **None.**[26]

PP 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.

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

Hierarchical to: No other components.

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

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

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

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

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

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

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

(2) decrypts authentic Update Code Package by means of CSP.

6.1.5.4 FDP_RIP.1/UCP Subset residual information protection

Hierarchical to: No other components

Dependencies: No dependencies.

FDP_RIP.1.1/UCP The TSF shall ensure that any previous information content of a resource is made unavailable upon ***the deallocation of the resource after unsuccessful verification***

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

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

of the digital signature of the issuer by means of CSP the following objects: ***received Update Code Package.***

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 FTP_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 FTP_TRP.1 is not fulfilled because secure import is ensured by OE.SecCommCSP in case of platform architecture.

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	

SFR	Dependencies of the SFR	SFR components
FPT_FLS.1	No dependencies	
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			

	O.GenLM	O.ImpExp	O.IAA	O.SecMan	O.TEE	O.TST	O.SecUCP
FMT_MTD.3/PW			x	x			
FMT_SMF.1	x	x		x			
FMT_SMR.1	x	x	x	x			
FPT_TDC.1	x	x					
FPT_FLS.1					x	x	
FPT_TEE.1					x	x	
FPT_TST.1						x	

Table 3: Security functional requirements rationale

The following part of the chapter demonstrates that the SFRs meet all security objectives for the TOE. This section has been taken from the protection profile [PP0105].

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 signaure generation.
- The SFR FMT_MSA.1 clauses (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 behavior of FMT_MSA.4 for Serial Number in the Log message.
- The SFR FMT_MOF.1, FMT_MDT.2, 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 imported with Transaction Data and of exported with 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 claus (1) defines the rule that additonal authentication (except for the Administrator itself) may be enabled and disabled by the Administartor .
- 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 SFR FMT_MTD.3/PW require the TSF to manage authentication data of users.

The security objective for the TOE O.SecMan “Security management” is met by the following 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 SFR FMT_MTD.3/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 TSF 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 Numbers.

The security objective for the TOE O.TEE “Test of external entities” is met directly by the SFR FPT_TEE.1. The SFR FMT_MOF.1, clause (5), restricts the definition and modification of the FPT_TEE.1 behavior to the Administrator. The SFR FIA_ATD.1 defines the security attribute Identity for ERS 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 chapter of the protection profile has been omitted, since the TOE of this security target are not physically separated components and the operational environment can ensure the integrity of the communication between the TOE and the CSP.

8 TOE summary specification (ASE_TSS)

8.1 TOE Security Functionality

8.1.1 TSF_Management: Management of the security functionality

This security functionality manages the configuration of the TOE and its security functions. During personalization, it manages instantiation and initial creation of objects. It provides default values and handles dynamic configuration data. This security functionality ensures that all security relevant data is stored in a secure way by using certified functions of the dedicated platform.

In operational life cycle state this TSF manages the configuration functions of the Administrator and Time Administrator, e.g., setting the system time and mapping ERS to Key.

8.1.2 TSF_Log: Handling of log data and signature functionality

This Security Functionality manages the signature functionality and the according system and transaction logging. It ensures that the needed types of data to be signed are present and passes them in the expected form to the CSP for signature creation. Furthermore, it guarantees that the received signature and further security attributes are correctly exported.

8.1.3 TSF_Auth: Authentication protocols

This security functionality uses different authentication mechanisms to differentiate identities and roles. This includes, e.g., password authentication for users as well as CSP and CTSS role authentication after a successful self test. Additionally it manages reauthentication of these roles. Within the TOE, TSF_Auth is implemented using the authentication mechanisms provided by TSF_CSP.

8.1.4 TSF_CSP: Cryptographic service provider

The cryptography-based security functionality of the TOE is provided by the cryptographic service provider. This includes authentication methods TSF_Auth relies on, as well as signature creation needed by TSF_Log. This TSF represents the dedicated platform cryptovision CSP and implement all cryptographic functions needed by the TOE. Please note that this functionality is dsignated as “TSF” although the CSP is not a part of the TOE.

8.1.5 TSF_Update: Update functionality and according management

TSF_Update comprises the functionality that is used to provide updates of the TOE. It is based on the Global Platform mechanisms of the CSP platform [GP_CIC].

8.2 TOE summary specification rationale

This summary specification shows that the TSF and assurance measures are appropriateto fulfill the TOE security requirements.

Each TOE security functional requirement is implemented by at least one security functionality. The mapping of TOE Security Requirements and TOE Security Functionalities isgiven in the following table. If iterations of a TOE security requirement are covered by the same TOE security functionality the mapping will appear only once. The description of the TSF is given in section 8.1.

	TSF_Management	TSF_Log	TSF_Auth	TSF_CSP	TSF_Update
FMT_SMR.1	x		x		
FMT_SMF.1	x	x	x	x	
FMT_MOF.1	x	x	x	x	
FMT_MSA.1	x	x	x	x	
FMT_MSA.3	x				
FIA_ATD.1	x		x	x	
FMT_MTD.1/AD	x		x	x	
FMT_MTD.3/PW	x		x	x	
FIA_AFL.1	x		x	x	
FIA_USB.1	x	x	x	x	
FIA_UID.1			x	x	
FIA_UAU.1	x		x	x	
FIA_UAU.5	x		x	x	
FIA_UAU.6	x		x	x	
FDP_ACC.1/LM	x	x	x	x	
FDP_ACF.1/LM	x	x	x	x	
FDP_ITC.2/TD		x	x	x	
FDP_ETC.2/DTBS		x	x	x	
FDP_ITC.2/TSS		x	x	x	
FDP_ETC.2/LM		x	x	x	
FPT_TDC.1		x	x	x	
FMT_MSA.2		x		x	
FMT_MSA.4		x	x	x	
FPT_FLS.1			x	x	
FPT_TEE.1			x	x	
FPT_TST.1			x	x	
FDP_ACC.1/UCP				x	x
FDP_ACF.1/UCP				x	x
FDP_ITC.2/UCP				x	x
FDP_RIP.1/UCP				x	x

Table 4: SFR and TSF mapping

- FMT_SMR.1 claims that the TSF shall shall maintain the roles Unidentified User, Administrator, Time Administrator, CTSS interface role and CSP role. This is realized by TSF_Management and TSF_Auth.
- FMT_SMF.1 requires that the TSF shall be capable of performing the following management functions: (1) management of security functions behavior, (2) management of Authentication Reference Data, (3) management of security attributes, (4) none. This is realized by TSF_Management, TSF_Log, TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).
- FMT_MOF.1 requires that the TSF shall restrict the ability to (1) enable and disable the functions password authentication according to FIA_UAU.5.2, clause (2) if defined to Administrator, (2) determine the behaviour of and modify the behaviour of 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 to Administrator, (3) determine the behaviour of the function FPT_TEE.1 by definition of the identity and features to be tested of ERS to Administrator, (4) determine the behaviour of the function FPT_TEE.1 by definition of the identity and features to be tested of CSP to Administrator, (5) determine the behaviour of and modify the behaviour of the function FPT_TEE.1 in case the test of CTSS interface component or CSP fails to Administrator. This is realized by TSF_Management, TSF_Log, TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).
- FMT_MSA.1 requires that the TSF shall enforce the Log message SFP and Update SFP to restrict the ability to (1) define the set of accepted values of the security attribute “Serial number of ERS” to Administrator, (2) define depending on the Serial number of ERS the identity of the signature-creation key to be used for the Transaction log to Administrator, (3) define depending on the Serial number of ERS the Serial number in the protocol data of Transaction log to Administrator, (4) define 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 to Administrator, (5) increase by 1 the internally stored security attribute “Transaction Number” when transaction is started to subjects in CTSS interface role, (6) modify the TD security attribute “Transaction Number” imported from the TD to none, (7) modify the security attributes of UCP to none. This is realized by TSF_Management, TSF_Log, TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).
- FMT_MSA.3 requires that the TSF shall enforce the Log message SFP and Update SFP to provide restrictive default values for security attributes that are used to enforce the SFP and that the TSF shall allow the none to specify alternative initial values to override the default values when an object or information is created. This is realized by TSF_Management.
- FIA_ATD.1 requires the TSF shall maintain the following list of security attributes belonging to Administrator: (1) Identity, (2) Authentication Reference Data, (3) Role and (a) security attribute Identity, none belonging to the ERS (b) security attribute Identity, none belonging to the CSP. This is realized by TSF_Management and TSF_Auth based on TSF_CSP.
- FMT_MTD.1/AD requires that the TSF shall restrict the ability to (1) delete and create the Authentication Data Record of all authorized users to Administrator (2) modify the Authentication Reference Data to the corresponding authorized user. This is realized by TSF_Management and TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).
- FMT_MTD.3/PW requires that the TSF shall ensure that only secure values are accepted for passwords and enforce changing initial passwords after first successful authentication of the user to a different secure operational password. This is realized by TSF_Management and TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).
- FIA_AFL.1 requires that the TSF shall detect when an administrator configurable positive integer within 1 – 15 unsuccessful authentication attempts occur related to PIN-based authentication, and

that when the defined number of unsuccessful authentication attempts has been met, the TSF shall delay the next authentication attempt or block the authentication, configurable by the administrator. This is realized by TSF_Management and TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).

- FIA_USB.1.1: FIA_USB.1.1 requires that the TSF shall associate the following user security attributes with subjects acting on the behalf of that user (1) Identity, (2) Role. FIA_USB.1.2 requires that the TSF shall enforce the following rules on the initial association of user security attributeswith subjects acting on the behalf of users: the initial role of the user is Unidentified user. FIA_USB.1.3 requires that the TSF shall enforce the following rules governing changes to the user security attributesassociated 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. (4) The Administrator is allowed to activate and deactivate the CTSS interface role. This is realized by TSF_Management, TSF_Log, TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).
- FIA_UID.1 requires that the TSF shall allow self test according to FPT_TST.1 on behalf of the user to be performed before the user is identified, and that the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. This is realized by TSF_Auth based on TSF_CSP.
- FIA_UAU.1: FIA_UAU.1.1 requires that the TSF shall allow (1) self 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) none, 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. This is realized by TSF_Management and TSF_Auth based on TSF_CSP.
- FIA_UAU.5 requires that the TSF requires that the TSF shall provide password authentication to support user authentication, and that the TSF shall authenticate any user's claimed identity according to the rule that (1) password authentication shall be used for Administrator, (2) none. This is realized by TSF_Management and TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).
- FIA_UAU.6 requires that the TSF shall re-authenticate the user under the conditions power on or reset. This is realized by TSF_Management and TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).
- FDP_ACC.1/LM requires that the TSF shall enforce the Log Message SFP 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. This is realized by TSF_Management, TSF_Log, TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).
- FDP_ACF.1/LM: FDP_ACF.1.1/LM requires that the TSF shall enforce the Log Message SFP 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. This is realized by

TSF_Management, TSF_Log, TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).

- FDP_ITC.2/TD: FDP_ITC.2.1/TD requires that the TSF shall enforce the Log message SFP when importing Transaction Data controlled under the SFP, from outside of the TOE. FDP_ITC.2.2/TD requires that the TSF shall use the security attributes associated with the imported Transaction Data. FDP_ITC.2.3/TD requires that the TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the Transaction Data received. FDP_ITC.2.4/TD requires that the TSF shall ensure that interpretation of the security attributes of the imported Transaction Data is as intended by the source of the user data. FDP_ITC.2.5/TD requires that the TSF shall enforce the following rules when importing user data Transaction Data controlled under the SFP from outside of the TOE: (1) The TSF shall import the Transaction Data with the security attribute 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. This is realized by TSF_Log, TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).
- FDP_ETC.2/DTBS: FDP_ETC.2.1/DTBS requires that the TSF shall enforce the Log message SFP when exporting Data To Be Signed, controlled under the SFP(s), to CSP. FDP_ETC.2.2/DTBS requires that the TSF shall export the user data with the security attributes associated with Data To Be Signed. FDP_ETC.2.3/DTBS requires that the TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported Data To Be Signed. FDP_ETC.2.4/DTBS requires that 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]. This is realized by TSF_Log, TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).
- FDP_ITC.2/TSS: FDP_ITC.2.1/TSS requires that the TSF shall enforce the Log message SFP when importing protocolData with Signature and audit records, controlled under the SFP, from CSP. FDP_ITC.2.2/TSS requires that the TSF shall use the security attributes associated with the imported user data. FDP_ITC.2.3/TSS requires that the TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the protocolData with Signature and audit records received. FDP_ITC.2.4/TSS requires that the TSF shall ensure that interpretation of the security attributes of the imported protocolData with Signature and audit records is as intended by the source of the user data. FDP_ITC.2.5/TSS requires that the TSF shall enforce the following rules when importing protocolData with Signature and audit records controlled under the SFP from CSP: None. This is realized by TSF_Log, TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).
- FDP_ETC.2/LM: FDP_ETC.2.1/LM requires that the TSF shall enforce the Log message SFP when exporting user data Log message, controlled under the SFP(s), to CTSS interface component. FDP_ETC.2.2/LM requires that the TSF shall export the user data with the user data's associated security attributes. FDP_ETC.2.3/LM requires that 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 requires that 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. This is realized by TSF_Log, TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).

- FPT_TDC.1: FPT_TDC.1.1 requires that 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 when shared between the TSF and another trusted IT product. FPT_TDC.1.2 requires that the TSF shall use BSI TR-03151 [TR SE] and BSI TR-03153 [TR TSEA] when interpreting the TSF data from another trusted IT product. This is realized by TSF_Log, TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).
- FMT_MSA.2 requires that 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. This is realized by TSF_Log based on security fuctionality provided by the CSP platform (TSF_CSP).
- FMT_MSA.4 requires that the TSF shall use the following rules to set the value of security attributes: (1) The 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. (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. This is realized by TSF_Log, TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).
- FPT_FLS.1 requires that 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. 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. This is realized by TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).
- FPT_TEE.1: FPT_TEE.1.1 requires that 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 to check the fulfillment of (1) ESR Identity, none and (2) CSP Identity, none. The tests include the identification of the TOE to the tested device. FPT_TEE.1.2 requires that the TSF shall enter the secure state according to FPT_FLS.1 none additional action if the test fails. This is realized by TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).

- FPT_TST.1: FPT_TST.1.1 requires that 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 to demonstrate the correct operation of parts of TSF. FPT_TST.1.2 requires that the TSF shall provide authorised users with the capability to verify the integrity of TSF data. FPT_TST.1.3 requires that the TSF shall provide authorised users with the capability to verify the integrity of TSF implementation. This is realized by TSF_Auth based on security fuctionality provided by the CSP platform (TSF_CSP).
- FDP_ACC.1/UCP requires that the TSF shall enforce the Update SFP on (1) subjects: Administrator; (2) objects: Update Code Package; (3) operations: import, decrypt. This is realized by TSF_Update based on security fuctionality provided by the CSP platform (TSF_CSP).
- FDP_ACF.1/UCP: FDP_ACF.1.1/UCP requires that the TSF shall enforce the Update SFP to objects based on the following: (1) subjects: Administrator; (2) objects: Update Code Package with security attributes Issuer and Signature. FDP_ACF.1.2/UCP requires that the TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: (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. FDP_ACF.1.3/UCP requires that the TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none. FDP_ACF.1.4/UCP requires that 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) None. This is realized by TSF_Update based on security fuctionality provided by the CSP platform (TSF_CSP).
- FDP_ITC.2/UCP: FDP_ITC.2.1/UCP requires that the TSF shall enforce the Update SFP when importing user data, controlled under the SFP, from outside of the TOE. FDP_ITC.2.2/UCP requires that the TSF shall use the security attributes associated with the imported user data. FDP_ITC.2.3/UCP requires that 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 requires that 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 requires that 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. This is realized by TSF_Update based on security fuctionality provided by the CSP platform (TSF_CSP).
- FDP_RIP.1/UCP requires that 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 the following objects: received Update Code Package. This is realized by TSF_Update based on security fuctionality provided by the CSP platform (TSF_CSP).

9 References

In the following tables, the references used in this document are summarized.

Common Criteria

[CC_1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017; CCMB-2017-04-001.
[CC_2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 5, April 2017; CCMB-2017-04-002.
[CC_3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017; CCMB-2017-04-003.
[CC_4]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5, April 2017; CCMB-2017-04-004.

Protection Profiles

[PP CSP]	Common Criteria Protection Profile “Cryptographic Service Provider”, BSI-CC-PP-0104-2019, Version 0.9.8, Bundesamt für Sicherheit in der Informationstechnik.
[PPC-CSP-TS-Au]	Common Criteria Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au) Protection Profile-Module CSP Time Stamp Service and Audit (PPM-TS-Au), BSI-CC-PP-0107-2019, Version 0.9.5, Bundesamt für Sicherheit in der Informationstechnik.
[PP0105]	Common Criteria Protection Profile – Security Module Application for Electronic Record-keeping Systems, BSI-CC-PP-0105-2019, Version 0.7.5.
[PP_Javacard]	Java Card Protection Profile - Open Configuration, Version 3.0 (May 2012), Published by Oracle, Inc.

TOE and Platform References

[ST_CSP]	cryptovision CSP – Java Card applet providing Cryptographic Service Provider, Security Target, BSI-DSZ-CC-1119.
[ST_Javacard]	NXP JCOP 4 P71 Security Target Lite for JCOP 4 P71 / SE050Rev. 3.4 – 2019-06-06 ; Evaluation documentation, Final, NSCIB-CC-180212
[Zert_Javacard]	Certification Report JCOP 4 P71, Report number: NSCIB-CC-180212-CR, TÜV Rheinland Nederland B.V., 23 July 2019.
[ST_IC]	NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library - Security Target Lite - Rev. 1.1 — 31 May 2019, DSZ-CC-1040
[Zert_IC]	Certification Report BSI-DSZ-CC-1040-2019 for NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library from NXP Semiconductors Germany GmbH; 2019-06-14.
[Guidance]	cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems - Preparation Guidance (AGD_PRE).
[Guidance_OPE]	cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems - Operational Guidance (AGD_OPE).

[GP_CIC]	GlobalPlatform Card Common Implementation Configuration Version 1.0, February 2014
[AGD_PRE]	JCOP 4 P71 - User manual for JCOP 4 P71 (User Guidance and Administrator Manual), Rev. 3.3 – 20181213, NXP doc. no. 469533.
[TR03145]	BSI TR-03145-1, Secure CA operation, Part 1 - Generic requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level 'high', Version 1.1, 27.03.2017
[PKIkonzept]	PKI-KONZEPT FÜR TSE-TOKENS für die TSE-Produktion bei der D-Trust GmbJ, Version 1, D-Trust GmbH, 2020.

References from the protection profile

[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
[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
[AIS20]	BSI AIS 20/31, A proposal for: Functionality classes for random number generators, Version 2.0, 2011
[RFC5639]	M. Lochter, J. Merkle. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation (RFC5639), 2010. Available at http://www.ietf.org/rfc/rfc5639.txt.
[ICAO]	ICAO, Machine Readable Travel Documents, ICAO Doc9303, Part 11: Security Mechanisms for MRTDSs, seventh edition, 2015
[NIST2005]	NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication May 2005
[NIST2007]	NIST Special Publication 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November, 2007
[NIST2008]	FIPS PUB 198-1 The Keyed-Hash Message Authentication Code (HMAC), July 2008
[NIST 2013]	National Institute of Standards and Technology. FIPS PUB 186-4: Digital Signature Standard (DSS). 2013
[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 7498-2:1989)
cryptographic service provider	Component in the operational environment of the TOE providing cryptographic service for the TOE as defined in [PP CSP] with PP-module [PPC-CSP-TS-Au]
tax authorities	authority inspecting accounts and records in form of Log messages
certified technical security system (“zertifizierte technische Sicherheitseinrichtung”)	device dedicated to protect the electronic record-keeping system and digital records (cf. [FCG] section 146a sentence 2). It consists of a security module and a storage medium and providing the unified digital interface (cf. [FCG] section 146a sentence 3)
unified digital interface (“einheitliche digitale Schnittstelle”)	Interface for transmission or output of records or accounts for cash inspection according to [FCG] section 146b paragraph 2 sentence 2.
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 5: Terminology

Acronym	Term
A.xxx	Assumption
CC	Common Criteria
CSP	cryptographic service provider, the TOE of [PP CSP] with PP-module [PPC-CSP-TS-Au]
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

Acronym	Term
SFR	Security functional requirement
T.xxx	Threat
TD	Transaction data
TDS	Transaction data set
TDSS	Transaction data set sequence
TOE	Target of Evaluation
TSF	TOE security functions
UCP	Update Code Package

Table 6: Abbreviations