A-Trust Gesellschaft für Sicherheitssysteme
im elektronischen Datenverkehr GmbH
Landstraßer Hauptstraße 1b, E02
A-1030 Wien

https://www.a-trust.at
E-Mail: office@a-trust.at

Tel: +43 (1) 713 21 51 - 0
Fax: +43 (1) 713 21 51 - 350

Security Target - SMAERS for a.sign TSE Online

Version: 1.0.3
Date: 26.07.2021

Contents

Date	Rev	Author	Changes
28.07.2021	1.0.3	RS	versioning
08.07.2021	1.0.2	DK	Update TOE Deliverables.
23.03.2021	1.0	RS	Evaluator Feedback, OS-Version, CSPL Version
03.03.2021	0.834	RS	Evaluator Feedback, FCS_RNG.1
18.02.2021	0.833	RS	Evaluator Feedback
02.02.2021	0.832	RS	Evaluator Feedback
16.12.2020	0.831	RS	Evaluator Feedback
12.12.2020	0.83	RS, DK	Evaluator Feedback
07.12.2020	0.82	RS, DK	References to required concepts
25.08.2020	0.81	RS	editorial corrections
25.08.2020	0.8	RS	editorial corrections
24.08.2020	0.78	RS, DK	clarifications
16.08.2020	0.77	RS	adaptation according to BSI-CC-PP-0105-V2-2020
31.07.2020	0.76	RS	implemented OR 0.3
21.07.2020	0.75	RS, DK, DR	implemented OR 0.2
02.07.2020	0.74	RS, DK, DR	changes in chapter 8 according to OR 0.1
26.06.2020	0.73	RS, DK, DR	Rewrite according to Protection Profile 0.93 Observation Report 0.1
20.05.2020	0.72	RS, DK, DR	Rewrite according to Protection Profile 0.91
17.01.2020	0.7	RS, DK	Application Notes 4, 15, 17 FSC_RNG TOE description (NON-TOE components) TOE Overview (customers view) Chapter 8 SF.SecCommCSP 6.3.2 Security functional requirements rationale
16.10.2019	0.6	RS, DK	feedback ITSEF
10.10.2019	0.5	RS, DK	Summary Specification
03.10.2019	0.4	RS, DK	feedback ITSEF
02.10.2019	0.3	RS, DK	rationale
27.09.2019	0.2	RS, DK	internal review
21.06.2019	0.1	RS	initial version

Table 1: Document history

List of Tables

List of Figures

1 ST Introduction

In order to combat tax-fraud, electronic record-keeping systems in Germany must be equipped with a Certified Technical Security System (CTSS; Zertifizierte Technische Sicherheitseinrichtung) that consists of a storage medium, a security module, and a unified digital interface. The security module is subject to common criteria security certifications. W.r.t. to security requirements for the security module defined by Bundesamt für Sicherheit in der Informationstechnik the module consists of two components:

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

This protection profile defines the security requirements of the SMAERS component. Depending on the overall architecture, different security requirements exist for a CSP. These are defined in two protection profiles and protection profile configurations. For details on allowed architectures and required protection profiles and configurations, cf. Chapter 1.3 below, in particular Section Non-TOE Hardware/Software/Firmware available to the TOE.

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

1.1 ST Reference

Title	Security Target - A-Trust SMAERS for a.sign TSE Online
Sponsor	A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH
ST Version	1.0.3
ST Date	26.07.2021
CC Identification	Common Criteria for Information Technology Security Evaluation Version 3.1,Revision 5 ([CCP1])
Assurance Level	EAL2 augmented with ALC_LCD.1 and ALC_CMS.3
Certification ID:	BSI-DSZ-CC-1140

Table 2: ST Reference

1.2 TOE Reference

Title	A-Trust SMAERS for a.sign TSE Online
Version	1.2.0

Table 3: TOE Reference

1.3 TOE Overview

The TOE is the A-Trust SMAERS for a.sign TSE Online which is a part of the ‘a.sign TSE Online‘ TSS. It implements the *client-server architecture* running on a platform supporting secure storage of assets and relies on an Utimaco CryptoServer CSPLight Version 1.0.0 as a Cryptographic Service Provider Light (CSPL) located in the A-Trust Datacenter secure environment for all cryptographic operations except for the implementation of the trusted channel which is implemented using the Password Authenticated Connection Establishment (PACE) protocol [TR 03110]. The TOE followes the following specifications:

1. Technische Richtlinie TR-03153 ([TR TSEA]): "Technische Sicherheitseinrichtung für Elektronische Aufzeichnungssysteme". This document describes the basic structure of a TSS andits functionality. The major components of the TSS are the secure element (SE), the SE-API andthe secure storage.
2. Technische Richtlinie TR-03151 ([TR SE]): "Secure Element API (SE-API)". This document defines treating the transactions and retrieving the signed data from the secure elementas well as the management functionality. It also defines the data formats for the messages that are created by the TSS.
3. Common Criteria Protection Profile ([PP-SMAERS]): Schutzprofil für die Anwendungskomponente des Sicherheitsmoduls ("Security Module Application for ElectronicRecord-keeping Systems", SMAERS). This PP defines the security and assurance requirementsfor the TOE described in this ST.
4. Common Criteria Protection Profile ([PP CSPLight]): Schutzprofil für einen einfachen kryptographischen Dienstanbieter ("Cryptographic Service Provider Light", CSP-L). This Protection Profile contains the requirements for the CSP that is used by the TOE.
5. Cryptographic services of the CSP have to be compliant with BSI Technical Guideline TR-03116-5 [TR CryAS].

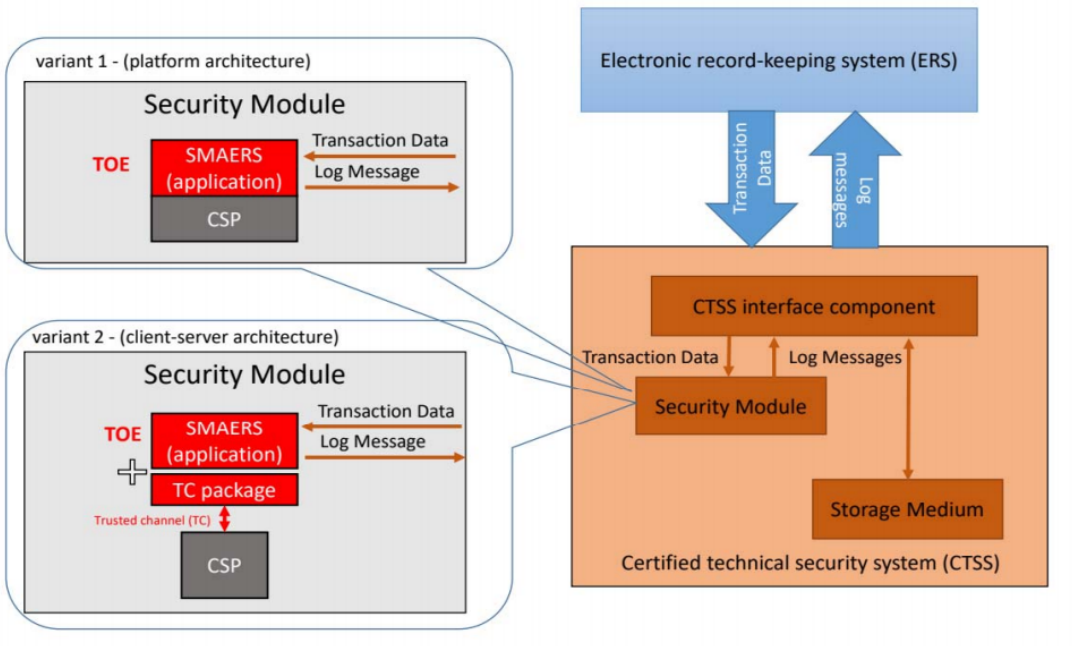

Figure 1: Description and interaction between TOE and the relevant non-TOE components

The TOE is a security module application as part of the security module of a certified technical security system (CTSS) for electronic record-keeping systems (ERS). Figure 1 describes the interaction between TOE and non-TOE components. The CTSS consists of a security module, a storage medium, and a CTSS interface component providing the standardized digital interface (cf. [FCG], section 146a, paragraph 1, sentence 3) for the electronic recordkeeping system and cash inspection (cf. [FCG], section 146b). The [FCG] section 2 requires the security module to provide

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

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

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

dency.

Transaction logs are created to protect the transaction data of the electronic record-keeping system as certified data. They are generated whenever a transaction is started, finished (i.e. completed or terminated), and may be generated when transaction data are updated. The protocol data of transaction logs contain the transaction number of the transaction and time stamps. All transaction logs with the same transaction number build together the required data of the fiscal transaction [KSV] Section 2, Sentence 2.

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

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

The TOE

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

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

protocol data.

1.3.1 TOE Type

The TOE is implemented as software running on a component that is physically separated from the CSP in a client-server architecture. Therefore the Security target at hands claims the package *trusted channel* between the TOE and the CSP in Chapter 7. A trusted channel is necessary because the TOE and the CSP are implemented as separated components and must interact through a trusted channel in order to protect the integrity of the communication data, and to prevent misuse of the CSP w.r.t. signing and time stamping services provided for the TOE.

Method of Use

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

The CTSS-Administrator needs to define the list of allowed `client_Ids`. Only these `client_Ids` are allowed to access the Target of Evaluation (TOE).

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

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

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

TOE Lifecycle

Since the TOE lifecycle is part of the CTSS life cycle, here only the TOE lifecycle is described, while the CTSS life cycle is described in the document [Umgebungskonzept]

detailing provisioning of CTSS. This document is connected to the documentation of the underlying public key infrastructure (PKI) [PKI-Konzept].

The update procedures to allow for recovery from security incidents including the procedures for creating, distributing, and enforcing installation of update code packages for the TOE and the CSP is described in the document [Updatekonzept].

In short the TOE is delivered from A-Trust either via download from the A-Trust Website. The TOE is delivered unpersonalized and has to be personalized by an integrator using a provisioning API of the TOE.

TOE Boundaries

Physical Scope Since TOE is a pure software component, there are no physical boundaries.

TOE is delivered in form of a library and the accompanying documentation as described in table 4.

TOE requires a secure platform as described in the document [Umgebungskonzept].

No	Type	Identifier	Release	Form of Delivery
1	SW	SMAERS	1.2.0	delivered as a software module (library)
2	DOC	Functional specification - SMAERS for a.sign TSE Online	1.0.2	PDF
3	DOC	Operational user guidance - SMAERS for a.sign TSE Online	1.0.3	PDF

Table 4: TOE deliverables

Logical Scope The logical scope of TOE is defined by the interface defined in [TR SE] allowing the user to

authenticate as admin to manage the TOE

manage the TOE allowing admin to

- changing the Admin-PIN
- setting the list of allowed ClientIds
- updating the TOE using Update Code Package (UCP)
- managing audit logs

- manange the life cycle of TOE

start, update and finish transactions in order to generate transaction logs.

export log messages which are exported archives according to [TR SE].

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

The TOE requires:

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

A-Trust SMAERS for a.sign TSE Online uses a CSP which meets Common Criteria Protection Profile Configuration Cryptographic Service Provider Light Time Stamp Service, Audit and Clustering [PPC-CSPLight-TS-Au-Cl] running on hardware that meets Appendix: Operational Requirements for CSPLight.

A-Trust SMAERS for a.sign TSE Online requires Utimaco CSPLightas described in [Utimaco-CSPLight].

The TOE requires as opeating system Windows 10.

A-Trust SMAERS for a.sign TSE Online relies on a platform with secure storage. The [ope] describes the assumptions the TOE has on this platform and the [Umgebungskonzept] specifies the secure storage in more detail.

The protection of the assets by the platform (see OE.SMAERSPlatform) as described in the document [Umgebungskonzept] depends on: a Trusted Platform Module (TPM) is used for remote attestation. Further measures as described in the document [Umgebungskonzept] enusre the requirements of OE.SMAERSPlatform.

2 Conformance Claims

2.1 CC Conformance Claims

The ST claims conformance to CC version 3.1 revision 5. Conformance of this ST with respect to CC Part 2 [CCP2] (security functional components) is CC part 2 extended. Conformance of this ST with respect to CC Part 3 [CCP3] (security assurance components) is CC part 3 conformant.

2.2 Package Claim

This ST claims to be conformant to the package Trusted Channel between TOE and CSP as defined in [PP-SMAERS]. This ST claims conformance to EAL2 augmented with ALC_LCD.1 and ALC_CMS.3.

2.3 ST Claim

This ST does not claim conformance to any other PP.

2.4 Conformance Rationale

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

2.5 Conformance Statement

This ST claims **strict** conformance to [PP-SMAERS].

3 Security Problem Definition

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, and modifications and gaps shall be detectable,
- the transaction number (as part of the transaction data) that enumerates transactions. The transaction number must be continuously increasing without gaps.
- the audit records imported from the CSP and exported to the CTSS interface component,
- the update code package (UCP) and the UCP version number
- the PACE password to setup the trusted channel to the CSP (only in case the package 'Trusted Channel' is claimed).

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

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

Table 5: Assets to be protected by the TOE

3.1.2 Users and Subjects

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

- electronic record-keeping system (ERS),

- CTSS interface component,
- CSP,
- (SMAERS-) administrator.

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

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

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

3.1.3 Roles

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

- role unidentified user: This role is associated with any user not (successfully) identified by the TOE. This role is assumed for subjects after start-up of the TOE and deactivated CTSS interface component. The TOE allows users in this role to run self-test of the TOE.
- role administrator: A user in this role is allowed to perform management functions. The administrator subject is acting on behalf of a human user after successful authentication as administrator until logout.
- role CTSS interface: A subject in this role is allowed to import Transaction Data from CTSS interface component, to generate transaction logs and system logs, and to export transaction logs and system logs to the CTSS interface component. A subject in this role is started automatically after start-up of the TOE if the CTSS interface role is activated and the CTSS interface component and the CSP are successfully tested according to FPT_TEE.1. The ERS uses the CTSS role.
- CSP role: A subject in this role is allowed to import audit records from CSP and to export Audit logs to the CTSS interface component. In addition the CSP role is allowed to start the update process. A subject in CSP role is started automatically after start-up of the TOE if the CSP is successfully tested according to FPT_TEE.1.

3.1.4 Objects

The TSF operates on the following types of user data objects

- transaction data (TD),
- audit records,
- data-to-be-signed (DTBS),
- protocolData with signature containing the time stamp, the signature counter, and the digital signature; all generated by the CSP (cf. [TR SE] and [TR TSEA]),
- log messages (LM) as transaction log, system log or audit log,
- update code package (UCP),
- commands (type of operation).

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

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

Audit records are data imported from the CSP.

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

- certified data i.e.
  - in case of a *transaction log*: the *transaction data* with the type of the certified data *transaction log*, object identifier (id-SE-API-transaction-log): bsi-de (0.4.0.127.0.7) applications (3) sE-API (7) sE-APIdataformats(1) 1 (cf. [TR SE], chapter 2.3.1)
  - in case of a *system log*: the security related events with the type of the certified data *system log*, object identifier (id-SE-API-audit-log): bsi-de (0.4.0.127.0.7) applications (3) sE-API (7) sE-API-dataformats(1) 2 (cf. [TR SE], chapter 2.3.2)
  - in case of an *audit log*: the *audit record* with the type of the certified data *audit log*, object identifier (idSE-API-audit-log): bsi-de (0.4.0.127.0.7) applications (3) sE-API (7) sE-API-dataformats(1) 3 (cf. [TR SE], chapter 2.3.3)
- protocol data generated by the TSF
  - the *transaction number*,
  - the *keyID* as a hash value of the signature-verification key
  - the type of the operation as name of the API function whose execution is recorded by the log message, i.e. *StartTransaction*, *UpdateTransaction* or *FinishTransaction*,

– the *optional protocol data* (may be empty).

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

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

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

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

3.1.5 Security Attributes

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

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

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

Passwords as *authentication reference data* have the security attributes

- *status*: the values initial password and operational password,
- *number of unsuccessful authentication attempts* (10).

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

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

The TOE accepts *transaction data* only if the clientID is known and mapped to a signa-

ture key in the CSP (*keyID*).

The TOE manages for each known *keyID* the last assigned transaction number and the transaction numbers of the ongoing transactions. If the type of the operation of imported *transaction data* is StartTransaction, then a new transaction is started and the TOE generates a new transaction number by addition of 1 to the last assigned transaction number, includes this value in the protocol data of the transaction log returned to the CTSS interface component, and adds 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 cf. [TR SE].

A UCP has the security attributes

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

3.1.6 Log messages

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

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

The following security attributes are conditional in log messages:

- Transaction logs contain the security attribute *transaction number* assigning the *log message* to the transaction of the electronic record-keeping system.
- System logs contain the security attribute *event* assigning the log message to the security related event of the TSF.
- Audit logs contain the security attribute *audit record* assigning the log message to security related events of the CSP.

3.2 Threats

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

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

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

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

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

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

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

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

3.3 Organisational Security Policies

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

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

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

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

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

Application note 2: The update is performed by the platform provided by the operational environment, c.f. OE.CSPPlatform for the platform architecture or OE.SMAERSPlatform for the client-server architecture.
A-Trust SMAERS for a.sign TSE Online updates are performed by OE.SMAERSPlatform.

3.4 Assumptions

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

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

A-Trust SMAERS for a.sign TSE Online is remotely accessible via a trusted channel to the TOE (client-server architecture) and certified as compliant to [PPC-CSPLight-TS-Au-Cl] running on hardware that meets Appendix: Operational Requirements for CSPLight as well as the requirements in chapter 1.2 section "TOE Life Cycle"

A.ProtComCSP Protection of Communication between TOE and CSP
The integrity of the communication data between TOE and CSP in the client-server architecture is protected via a trusted channel, and the security target must claim the package Trusted Channel, defined in Chapter 7.

In case of the platform architecture of the CSP, the CSP provides a secure execution environment for the TOE and protects the integrity of communication data with the TOE directly using the security services of the CSP.

A-Trust SMAERS for a.sign TSE Online claims the package Trusted Channel, defined in Chapter 7.

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

A-Trust SMAERS for a.sign TSE Online implents the client-server architecture,

hence options b and c of Figure 2 apply.

A.VerifLMS Verification of Log Message Sequences

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

A.Admin Trustworthy Administrator

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

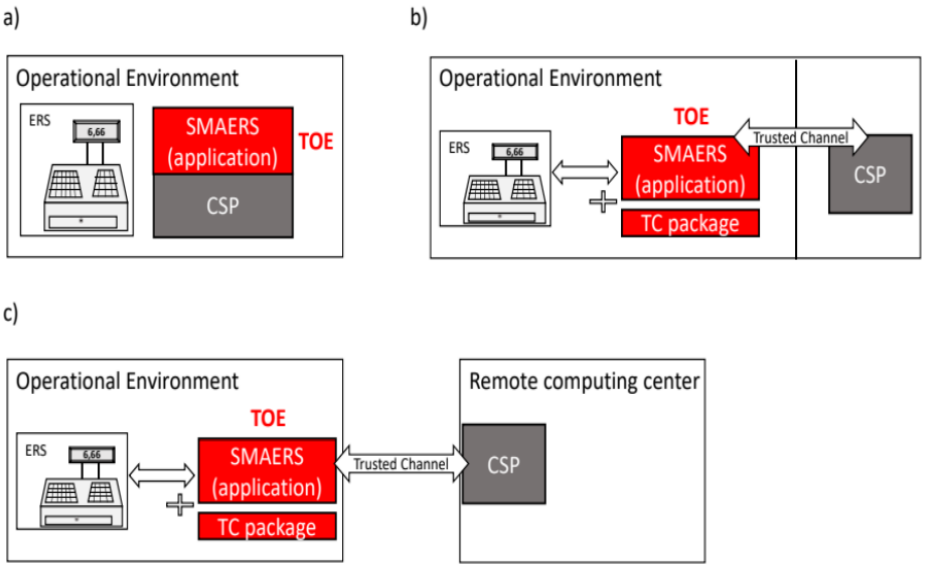

Figure 2: The TOE is always operated as a local component. a) platform architecture b) client-server architecture with local computing center c) client-server architecture with remote computing center

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

4 Security Objectives

4.1 Security Objectives for the TOE

O.GenLM Generation of *Log Messages*
The TSF generates transaction logs containing

- *transaction data*, *transaction number* created by the TSF, and
- time stamps and digital signatures created by the cryptographic service provider.

The TSF generates *system logs*.

O.ImpExp Import of *Transaction Data* from and Export of Log Messages to CTSS Interface Component
The TSF imports *transaction data* from the electronic record-keeping system through the CTSS interface component, import *audit records* from the CSP and export *log messages* to the CTSS interface component.

O.IAA Authentication of Administrators
The TOE verifies the claimed identity of the administrators by means of password.

O.SecMan Security Management
The TOE restricts the security management of TSF and TSF data to authenticated administrators. The TSF prevents management of the *transaction number* generation.

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

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

O.ImpExpUCP Secure Import and Export of User Data
The TSF securely exports the user data and TSF data to the secure storage of the platform and import the user data and TSF data after the successful update process.

4.2 Security Objectives for the Operational Environment

OE.ERS Trustworthy Electronic Record-Keeping System

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

OE.SMAERSPlatform Secure platform storage

The platform that executes the TOE has to ensure the integrity of the TOE itself and to provide secure storage which protects the integrity and confidentiality of stored security relevant objects as required (cf. Chapter 1.3.1 “TOE Type”). The platform verifies and installs the UCP.

OE.CSP Cryptographic Service Provider Component

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

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

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

OE.CSPPlatform CSP as a Secure Platform of the TOE

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

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

OE.Transaction Verification of Transaction

The operational environment shall verify the validity of *log message sequences* by verification of the corresponding digital signatures, shall verify the transaction numbers as being consecutive without gaps, and shall verify the points in time when

the transaction starts as being consecutively 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. The certificate shall be securely distributed to the tax inspector.

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

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

OE.SUCP Signed Update Code Packages
The manufacturer issues digitally signed *update code packages* together with its security attributes.

OE.SecUCP Secure download and authorized use of *Update Code Package*
The platform verifies the authenticity of received update code packages and installs only authentic update code packages.

4.3 Security Objective Rationale

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

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:

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

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

Table 6: Security Objective Rationale

and identity of the electronic record-keeping system connected to the TOE.

3. 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.

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

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

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

2. 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,

3. The security objective for the operational environment OE.SMAERSPlatform re-

quiring the operational environment to protect the TOE against manipulation and misuse.

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

1. The security objective for the TOE O.TEE requiring the TSF to test the presence and identity of the CSP connected to the TOE.
2. The client-server architecture requires OE.SMAERSPlatform.
3. The security objective for the operational environment O.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. The TOE and the CSP component are physically separated components. The integrity of the communication between the TOE and the CSP is protected by means of a trusted channel as provided by the CSP according to [PPC-CSP-TS-Au], [PPC-CSP-TS-Au-Cl], [PPC-CSPLight-TS-Au-Cl] and the TOE claims the package trusted channel between the TOE and the CSP, cf. Chapter 7.

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

1. The security objective for the TOE O.GenLM "Generation of Log messages" by means of digital signatures generated by the CSP, which allows to detect manipulation of transaction data sets according to OE.Transaction.
2. The security objective for the TOE O.IAA requiring the TSF to authenticate administrators by means of a password.
3. The security objective for the TOE O.TEE "Test of External Entities" requiring the TSF to test the presence and identity of the CSP connected to the TOE.
4. The security objective for the TOE O.TST "Self-Test and Secure State" detects failure and prevents generation of transaction data sets if time source is not available or the test of the CSP fails.
5. The security objectives for the operational environment OE.CSP "Cryptographic Service Provider Component" ensures the availability of a certified CSP for generation of time stamps and digital signatures, and the distribution of the certificate linked to the taxpayer for signature verification.
6. The security objective for the operational environment OE.SecOEnv "Secure Operational Environment" protecting the communication between ERS and TOE.

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

1. The security objective for the TOE O.GenLM "Generation of Log Messages" requiring the TSF to generate log messages containing *transaction data* imported from the electronic record-keeping system, requiring the TSF to generate time stamps

whenever a transaction starts, is completed or aborted, and requiring the TSF to create a *transaction number* and a digital signature of the *transaction data* using the digital signature-creation service of the cryptographic service provider.

2. The security objective for the TOE O.ImpExp "Import of *Transaction Data* from and Export of Log Message to CTSS Interface Component" requiring the TSF to import *transaction data* from the electronic record-keeping system through the CTSS interface component and to export log messages to the CTSS interface component.
3. The security objective for the TOE O.TEE "Test of External Entities" requiring the TSF to test the availability of the CTSS interface component and CSP connected to the TOE.
4. The security objective for the operational environment OE.SecOEnv "Secure Operational Environment" protecting the communication between ERS and TOE.

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

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

1. The security objectives for the TOE O.ImpExpUCP *"Secure Import and Export of User Data"* ensuring that user data are exported and imported after successful update process.
2. The security objective for the TOE O.TST "Self-Test and Secure State" ensuring a correctly increased version number after installation of an update code package.
3. The security objective for the operational environment OE.SUCP ensures that the authentic *update code packages* are signed and distributed with security attributes.
4. The OE.SecUCP "Secure download and authorized use of *Update Code Package*" ensures that only authentic UCPs are installed.
5. The OE.SMAERSPlatform ensures verifying the UCP.

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

1. The security objective for the TOE O.TEE requiring the TSF to test the presence and identity of the ERS as an external entity.
2. The security objective for the operational environment OE.ERS "Trustworthy Electronic Record-Keeping System".
3. The security objective for the operational environment OE.SecOEnv "Secure Operational Environment" protecting the communication of ERS and TOE.

The organizational security policy *OSP.CertSecDev Certified Security Device* is directly enforced by the security objectives for the operational environment OE.CSP "Crypto-

graphic Service Provider Component" and the certification conformant to this protection profile.

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

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

1. the security objective for the TOE O.GenLM "Generation of *Log messages*" requiring the TSF to generate *log messages* containing *transaction data* imported from the electronic record-keeping system, to generate time stamps whenever a transaction starts, is completed or aborted, and to generate a transaction number and a digital signature of the *transaction data* created using the digital signaturecreation service of the cryptographic service provider,
2. the security objectives for the TOE O.IAA "Authentication of Administrators" requiring the TSF to authenticate administrators by means of a password,
3. the security objective for the TOE O.ImpExp "Import of Transaction Data from and Export of *Log Message* to CTSS Interface Component" requiring the TSF to import *transaction data* from the electronic record-keeping system through the CTSS interface component and to export log messages to the CTSS interface component.
4. 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.
5. The security objective for the operational environment OE.Transaction "Verification of Transaction" ensures the condition for verification of the digital signature of the *transaction data* set.

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

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

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

The assumption *A.ProtComCSP Protection of Communication between TOE and CSP* is

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

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

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

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

5 Extended Component Definition

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

5.1 Authentication Proof of Identity (FIA_API)

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

Family Behaviour

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

Component Levelling:

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

Management: FIA_API.1

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

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

Audit: FIA_API.1

There are no auditable events foreseen.

FIA_API.1 Authentication Proof of Identity

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

5.2 Generation of Random Numbers (FCS_RNG)

Family Behaviour

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

Component Levelling:

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

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no auditable events foreseen.

FCS_RNG.1 Random number generation

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

6 Security Requirements

Selections that have been made by the ST Author are denoted by selection. Assignments that have been made by the ST Author are denoted by assignment.

6.1 Security Functional Requirements

6.1.1 Security Management

FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles: unidentified user, administrator, CTSS interface role and CSP role and no other roles.
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: 1. management of security functions behaviour (cf. FMT_MOF.1), 2. management of authentication reference data (cf. FMT_MTD.1/AD, FMT_MTD.3/PW), 3. management of security attributes (cf. FMT_MTD.3/PW, FMT_MSA.3, FMT_MSA.4), 4. None.

FMT_MOF.1 Management of security functions behaviour

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MOF.1.1	The TSF shall restrict the ability to

1. enable and disable 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,
6. determine the behaviour of and modify the behaviour of the functions select the auditable events according to FAU_GEN.1/SYS to administrator,
7. determine the behaviour of and modify the behaviour of the functions automatic export of audit trails according to FAU_STG.3.1/SYS clause (1) to administrator

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

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 attributes clientID to administrator,
2. define depending on the clientID the identity of the signature-creation key (keyID) to be used for the transaction log to administrator,
3. define the identity of the signature-creation key (keyID) to be used for the system log and audit logs to administrator,
4. increase by 1 the internally stored security attribute "transaction number" whenever a transaction is started to subjects in CTSS interface role,
5. modify the TD security attribute "transaction number" imported from the TD to none,
6. increase the security attributes "version number" of UCP after successful installation to CSP role.

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

FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components.
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

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 and no additional security attributes belonging to the ERS
(b) security attribute identity and no additional security attributes belonging to the CSP.

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

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/AD	The TSF shall restrict the ability to

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.

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 a user to a different secure operational password.

FIA_AFL.1 Authentication failure handling

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when 10 unsuccessful authentication attempts occur related to authenticateUser function call.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met, the TSF shall block the user until the account gets successfully unblocked.

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.

FIA_UID.1 Timing of identification

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow self test according to FPT_TST.1 on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1 Timing of authentication

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1	The TSF shall allow (1) self test according to FPT_TST.1, (2) testing of external entity ERS according to FPT_TEE.1 and starting the subject CTSS interface component if testing was successful and the role CTSS interface component is activated, (3) testing of external entity CSP according to FPT_TEE.1 and start the subject CSP if testing was successful, (4) 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.

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 an administrator, (2) None

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

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. subject:
   a) subject acting for CTSS interface component,
   b) subject acting for CSP;
2. objects:
   a) transaction data,
   b) audit record,
   c) data-to-be-signed,
   d) protocolData with signature,
   e) log message,
   f) commands;
3. operations:
   a) import,
   b) export.

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
   f) commands.

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

1. A subject in activated CTSS interface role is allowed to
   a) import the transaction data from the CTSS interface component according to FDP_ITC.2/TD,
   b) import commands from activated CTSS interface component,
   c) export the DTBS of transaction log and system log to the CSP according to FDP_ETC.2/DTBS,
   d) import the protocolData with signature from the CSP according to FDP_ITC.2/TSS,
   e) export the transaction log and system log to the CTSS interface component according to FDP_ETC.2/LM.
2. A subject in activated CTSS interface role is allowed to terminate the transaction after time limit defined according to FMT_MOF.1.1 clause (2) is reached.
3. A subject in CSP role is allowed to import audit records from the CSP according to FDP_ITC.2/TSS and to export audit logs to the CTSS interface component according to FDP_ETC.2/LM.

FDP_ACF.1.3/LM The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.

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

1. a user in other role than CTSS interface role is not allowed to perform actions listed in FDP_ACF.1.2/LM clause (1) and (2).
2. a user in other role than CSP role is not allowed to perform actions listed in FDP_ACF.1.2/LM clause (3).

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 transaction data controlled under the SFP from outside of the TOE:

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

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

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

4. The TSF shall import audit records from the CSP.

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 the CSP.
FDP_ETC.2.2/DTBS	The TSF shall export the user data with the security attributes associated with the data-to-be-signed.
FDP_ETC.2.3/DTBS	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported **data-to-be-signed**.
FDP_ETC.2.4/DTBS	The TSF shall enforce the following rules when user data is exported from the TOE: 1. Data-to-be-signed shall be exported for generation of a log message with a security attribute identifying the private signature key to be used by FDP_DAU.2/TS according to [PPC-CSP-TS-Au] [PPC-CSP-TS-Au-Cl] [PPC-CSPLight-TS-Au-Cl].

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 the CSP.
FDP_ITC.2.2/TSS	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/TSS	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the 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 the CSP: none.

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

For A-Trust SMAERS for a.sign TSE Online: The CSPL generates and returns to the TOE the signature counter, the time stamp and the signatures for the data-to-be-signed exported by the TOE according to FDP_ETC.2/DTBS. The CSPL generates time stamps according to FDP_DAU.2/TS using a time source according to FPT_STM.1, cf. [PPC-CSP-TS-Au-Cl]. The CSPL meets [TR SE], for the transaction logs, then the CSP returns a log message to the TOE.

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*

1. transaction logs:
   a) transaction number of the transaction identifying the log messages which belongs to the transaction,
   b) signature counter of the private signature key used by FDP_DAU.2/TS according to [PPC-CSP-TS-Au] [PPC-CSP-TS-Au-Cl] [PPC-CSPLight-TS-Au-Cl] enumerating all log messages,
   c) type of the operation,
   d) time stamp when the log message was signed,
   e) keyID as hash value of the public key for verification of the signature,
   f) signature for verification of the authenticity of the certified data and protocol data.
2. system logs:
   a) type of the operation or TSF security event
   b) signature counter of the private signature key used by FDP_DAU.2/TS according to [PPC-CSP-TS-Au] [PPC-CSP-TS-Au-Cl] [PPC-CSPLight-TS-Au-Cl] enumerating all log messages,
   c) time stamp when the log message was signed,
   d) keyID as hash value of the public key for verification of the signature,
   e) signature for verification of the authenticity of the certified data and protocol data.
3. audit records of the CSP shall be exported unchanged as audit logs to the CTSS interface component.

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

FPT_TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TDC.1.1	The TSF shall provide the capability to consistently interpret 1. clientID, 2. type of the operation, 3. transaction number, 4. signature counter, 5. time stamp, 6. keyID as hash value of the public key, 7. signature when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use [TR SE] and [TR TSEA] when interpreting the TSF data from another trusted IT product.

FMT_MSA.2 Secure security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for 1. transaction numbers building a strong increasing sequence without gaps, 2. Time stamps of the log messages building a non-decreasing sequence with consideration of adjustments of the CSP's time source.

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

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

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

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

6.1.4 Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to:	No other components.
Dependencies	No dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur:

1. self test according to FPT_TST.1 fails,

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

3. test of CSP according to FPT_TEE.1 fails. The TSF shall exit the secure state only if the self-test, the test of the ERS and the test of the CSP are passed.

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

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 and no other properties of the ERS and 2. CSP identity and no other properties of the CSP. The tests include the identification of the TOE to the tested device.
FPT_TEE.1.2	If the test fails, the TSF shall enter the secure state according to FPT_FLS.1 none.

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

For A-Trust SMAERS for a.sign TSE Online: The administrator is not able to define the actions in FPT_TEE.1 and the administrator is not able to define additional actions in case of a failure of the self tests.
The tests of the CSP allow the CSP to identify the TOE as user of the CSP, cf. FIA_UID.1.1 clause (2) in [PP CSPLight].

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.

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

6.1.5 Security Audit

FAU_GEN.1/SYS Audit data generation - System Log

Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps
FAU_GEN.1.1/SYS	The TSF shall be able to generate an audit record of the following auditable events:

1. start-up and shutdown of the audit functions;
2. all auditable events for the not specified level of audit; and
3. other auditable events

1. system operation commands as specified in [TR SE], Appendix A,
2. authentication failure handling (FIA_AFL.1): the reaching of the threshold for the unsuccessful authentication attempts with claimed Identity of the user,
3. failure with preservation of secure state (FPT_FLS.1): entering and exiting secure state,
4. setting of the version number of the UCP and upgrade of stored data,
5. None

FAU_GEN.1.2/SYS	The TSF shall record within each audit record at least the following information:

1. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
2. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, no other audit relevant information.

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

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/SYSCTSS	The TSF shall restrict the ability to 1. manual export, 2. clear after manual export, the system logs to CTSS Interface Component.

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/SYSAdmin	The TSF shall restrict the ability to 1. select audited events in FAU_GEN.1/SYS, 2. define the number of audit records causing automatic export and clearing of exported audit records according to FAU_STG.3.1/SYS clause (1), 3. define the percentage of storage capacity of audit records if actions are assigned in FAU_STG.3.1/SYS clause (2) the system logs to Administrator.

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

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.1.1/SYS	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2/SYS	The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.

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

Hierarchical to:	No other components.
Dependencies:	FAU_STG.1 Protected audit trail storage
FAU_STG.3.1/SYS	The TSF shall

1. automatically export audit trails and clear automatically exported audit records if the audit trail exceeds an Administrator defined number of audit records within 1024-2048

2. Enter secure state if the audit trail exceeds an Administrator *settable percentage of storage capacity*.

Application note 15: The ST writer shall perform the open operations in FAU_STG.3.1/SYS element. If the number of audit records in clause (1) is set to 1 then the TSF export each audit record automatically. If the number of audit records in clause (1) is set higher than maximum number of audit records in the audit trail then the TSF does not export audit records automatically. The assignment of clause (2) may be no actions if an appropriate number of audit records is assigned in clause (1). (applied)

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

6.1.6 Update Code Package

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

Hierarchical to:	FDP_ACC.1 Subset access control
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/UCP	The TSF shall enforce the update SFP on

1. subjects: CSP role;

2. objects: stored data;

3. operations: upgrade.

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

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/UCP	The TSF shall enforce the Update SFP to objects based on the following: 1. subjects: CSP role; 2. objects: update code package with security attributes version number.
FDP_ACF.1.2/UCP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: 1. CSP role is allowed to upgrade the stored data if a) the digital signature of the UCP generated by the issuer is successfully verified by the SMAERS platform.
FDP_ACF.1.3/UCP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: None.
FDP_ACF.1.4/UCP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: 1. a CSP role is not allowed to upgrade the stored data if the verification of digital signature of the UCP by means of the SMAERS platform fails; 2. None.

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

FDP_ETC.2/UCP_UD Export of user data with security attributes - User Data

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ETC.2.1/UCP_UD	The TSF shall enforce the log message SFP when exporting user data, controlled under the SFP(s), to the storage of the platform.
FDP_ETC.2.2/ UCP_UD	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3/ UCP_UD	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4/ UCP_UD	The TSF shall enforce the following rules when user data is exported from the TOE: None.

FDP_ITC.2/UCP_UD Import of user data with security attributes - User Data

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITC.2.1/UCP_UD	The TSF shall enforce the update SFP when importing user data, controlled under the SFP, from the storage of the platform.
FDP_ITC.2.2/UCP_UD	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/UCP_UD	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4/UCP_UD	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5/UCP_UD	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: security attribute version number associated with the imported user data is strictly smaller than the TOE's version number.

FDP_RIP.1/UCP Subset residual information protection

Hierarchical to:	No other components
Dependencies:	No dependencies.
FDP_RIP.1.1/UCP	The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource after successful upgrade of the stored data the following objects: previous code and data.

6.2 Security Assurance Requirements

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

6.2.1 Assurance Refinements

Refinement on ALC_CMS.3.1C:

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

Refinement on ADV_ARC.1.3D:

The security guidance documentation of each platform (hardware and software platform and operating system) on which the TOE is designed to run shall be provided in addition.

Refinement on ADV_ARC.1.1C to 1.5C:

The security architecture description shall include an assessment how each single security requirement imposed by the platform documentation (guidance documentation and if available evaluation or certification results) has been followed in the TOE design and implementation concept.

Examples for such security requirements could include but are not limited to:

- **Dedicated library calls: Dedicated calls protecting against attacks may be provided by the platform for cryptographic operation. For example, dedicated calls implement operations that are hardened against timing side channel attacks, while others execute faster, but are not hardened. The platform guidance may require such library calls to be used.**

- **Key usage limitations: Key usage above a certain limit may reveal side channel information which can then be exploited. The implementation must ensure that the key usage limit is adhered to.**
- **Dedicated calls to ensure a correct program flow are provided (i.e. for boolean verification calls) to ensure protection against attacks that disturb the execution flow. Such library calls must be made use of in critical operations.**
- **Dedicated library calls are provided for the secure generation of cryptographic random numbers. Other random number generation functionality is present, but is not suitable to generate cryptographic random numbers. It must be ensured that correct random number generation library calls are used.**

Refinement on ADV_ARC.1.1E:

The evaluators task includes to check consistency of the requirements considered in the architectural description against those outlined in the platform documentation.

Refinement on ATE_IND.2.1D:

Providing the TOE for testing shall include in addition the implementation representation of the TOE as defined by ALC_CMS.3.

Refinement of ATE_IND.2.2C:

The resources provided shall include additionally appropriate tools or access to the TOE development environment in order to enable the evaluator to perform source code review most efficiently.

Refinement of ATE_IND.2.3E:

The evaluators test activities shall include a verification of the TOE implementation representation provided in order to confirm code compliance of the TOE implementation representation to the security guidance of the hardware platform and operating system and libraries which the TOE/TSF is intended to be run on. Therefore, the evaluator shall assess and verify that all platform guidance requirements are met and indicate possible vulnerabilities to the AVA evaluation activity for the TOE for further consideration.

6.3 Security Requirements Rationale

6.3.1 Dependency Rationale

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

SFR	Dependencies of the SFR	SFR components
FAU_GEN.1/SYS	FPT_STM.1 Reliable time stamps	FPT_STM.1 provided by the CSP PP Module Time Stamp Service and Audit
FAU_STG.1/SYS	FAU_GEN.1 Audit data generation	FAU_GEN.1/SYS
FAU_STG.3/SYS	FAU_STG.1 Protected audit trail storage	FAU_STG.1/SYS
FDP_ACC.1/LM	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/LM
FDP_ACC.1/UCP	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/UCP
FDP_ACF.1/LM	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/LM, FMT_MSA.3
FDP_ACF.1/UCP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/UCP, FMT_MSA.3
FDP_ETC.2/DTBS	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/LM
FDP_ETC.2/LM	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/LM
FDP_ETC.2/ UCP_UD	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/UCP
FDP_ITC.2/TD	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/LM Dependency on FTP_ITC.1 or FPT_TRP.1 is not fulfilled because secure import is ensured by OE.SecOEnv. FPT_TDC.1
FDP_ITC.2/TSS	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/LM In the client-server architecture FTP_ITC.1 is fulfilled, cf. Chapter 7 (FTP_ITC.1/TC).
FDP_ITC.2/ UCP_UD	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/UCP, FTP_ITC.1 is not included for UCP transfer but FDP_ACC.1/UCP ensure integrity and confidentiality of UCP, FPT_TDC.1 is not included because the CSP uses the security attributes of UCP
FDP_RIP.1/UCP	No dependencies	
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_ATD.1	No dependencies	

FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.1
FIA_UAU.5	No dependencies	
FIA_UAU.6	No dependencies	
FIA_UID.1	No dependencies	
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
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/LM, FMT_SMR.1 FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FDP_ACC.1/LM, FDP_ACC.1/UCP, FMT_MSA.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1, FMT_SMR.1
FMT_MSA.4	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/LM
FMT_MTD.1/AD	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/ SYSCTSS	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/ SYSAdmin	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MTD.3/PW	FMT_MTD.1 Management of TSF data	FMT_MTD.1/AD
FMT_SMF.1	No dependencies	
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.1
FPT_TDC.1	No dependencies	
FPT_FLS.1	No dependencies	
FPT_TEE.1	No dependencies	
FPT_TST.1	No dependencies	

6.3.2 Security Functional Requirements Rationale

	O.GenLM	O.ImpExp	O.IAA	O.SecMan	O.TEE	O.TST	O.ImpExpUCP
FAU_GEN.1/SYS	x						
FAU_STG.1/SYS	x						
FAU_STG.3/SYS	x						
FDP_ACC.1/LM	x	x					
FDP_ACC.1/UCP						x	
FDP_ACF.1/LM	x	x					
FDP_ACF.1/UCP						x	
FDP_ETC.2/DTBS	x						
FDP_ETC.2/LM		x					
FDP_ITC.2/TSS	x						
FDP_ITC.2/TD	x	x					
FDP_ITC.2/UCP_UD						x	x
FDP_ETC.2/UCP_UD						x	x
FDP_RIP.1/UCP						x	
FIA_AFL.1			x				
FIA_ATD.1			x		x		
FIA_UAU.1					x		
FIA_UAU.5			x				
FIA_UAU.6			x				
FIA_UID.1					x		
FIA_USB.1			x				
FMT_MOF.1	x		x	x	x		
FMT_MSA.1	x			x	x		
FMT_MSA.2	x			x			
FMT_MSA.3	x			x			
FMT_MSA.4	x	x		x			
FMT_MTD.1/AD			x	x			
FMT_MTD.1/SYSCTSS	x						
FMT_MTD.1/SYSAdmin	x						
FMT_MTD.3/PW			x	x			
FMT_SMF.1	x	x		x			
FMT_SMR.1	x	x		x	x		
FPT_TDC.1	x	x					
FPT_FLS.1					x	x	
FPT_TEE.1					x	x	
FPT_TST.1						x	

	O.GenLM	O.ImpExp	O.IAA	O.SecMan	O.TEE	O.TST	O.ImpExpUCP

Table 10: Security Functional Requirements Rationale

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

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

- The SFR FDP_ACC.1/LM and FDP_ACF.1/LM require access control of import of TD and signatures, export of DTBS and log messages for roles defined by FMT_SMR.1.
- The SFR FDP_ITC.2/TD and FDP_ITC.2/TSS requires the TSF to import transaction data from CTSS interface component, audit records, time stamps, signature counter and signatures from CSP to generate log messages.
- The SFR FDP_ETC.2/DTBS requires the TSF to export data-to-be-signed to the CSP for time stamping and signature generation.
- The SFR FMT_MSA.1, clause (3) prevents the manipulation of the transaction number.
- The SFR FMT_MSA.2 ensures that the security attributes of a log message are generated in a way that the log message builds a valid transaction.
- The SFR FMT_MSA.3 ensures restrictive security attributes of a log message as defined, and prevents alternative initial values of the security attributes of a log message.
- The SFR FMT_MSA.4 describes the generation of security attributes which are included in a log message.
- The SFR FMT_MOF.1 clause (2), describes the behaviour of FMT_MSA.4 for keyID in a log message.
- The SFR FMT_MOF.1, FMT_MTD.3/PW, FMT_MSA.3, FMT_MSA.4 defined for SFR FDP_ACC.1/LM and FDP_ACF.1/LM are listed in SFR FMT_SMF.1.
- The SFR FPT_TDC.1 ensures that the security attributes of the imported transaction data and of the exported log messages are correctly interpreted.
- The SFR FAU_GEN.1/SYS, FMT_MTD.1/SYSCTSS, FMT_MTD.1/SYSAdmin, FAU_STG.1/SYS, FAU_STG.3/ SYS decribes the generation and management of system logs.

- The security objective for the TOE O.ImpExp Import of Transaction Data from and Export of Log message to CTSS Interface Component is met by the following SFR:
- The SFR FDP_ACC.1/LM and FDP_ACF.1/LM require access control on the import of transaction data; and export of log messages to the CTSS interface component for roles defined by FMT_SMR.1.
- The SFR FDP_ITC.2/TD requires the TSF to import transaction data with security attributes in order to determine the security attributes of log messages according to FMT_MSA.4.
- The SFR FDP_ETC.2/LM requires the export of log messages with security attributes defined by FMT_MSA.4 to the CTSS interface component for generation of receipts and verification of log messages.
- The SFR FPT_TDC.1 ensures that the security attributes imported with transaction data and exported with log messages are correctly interpreted.

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

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

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

- The SFR FMT_SMR.1 defines the roles known to TSF and requires the TSF to associate users with these roles.
- The SFR FMT_SMF.1 lists the management functions as management of functions FMT_MOF.1, management of TSF data FMT_MTD.1/AD and FMT_MTD.3/PW, and management of security attributes FMT_MSA.1, FMT_MSA.2, FMT_MSA.3

and FMT_MSA.4.

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

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

- The SFR FMT_SMR.1 lists the roles known to the TSF, where subject CTSS interface component is automatically started and identified only.
- The SFR FIA_UID.1 defines the self-test as the only TSF mediated action allowed before users and subjects are identified.
- The SFR FIA_UAU.1 defines the TSF mediated action allowed before users and subjects are authenticated. The subject CTSS interface component is allowed to perform automatically TSF mediated actions according to FPT_TST.1 and FPT_TEE.1 before users are authenticated.
- The SFR FIA_ATD.1 defines the security attribute identity for the ERS and the CSP tested by FPT_TEE.1. If any test fails, the TSF enters a secure state according to FPT_FLS.1.

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

- The SFR FPT_TST.1 requires the TSF to perform self-tests and FPT_FLS.1 requires the TSF to enter a secure state if one of the self-tests fails.
- The SFR FPT_FLS.1 requires the TSF to enter a secure state if the self-test fails, or the test of the electronic record-keeping system fails, or the test of cryptographic service provider fails.
- The SFR FPT_TEE.1 requires the TSF to enter the secure state according to FPT_FLS.1 if the test of the CTSS interface component or the CSP fails.
- The SFR FDP_ACC.1/UCP and FDP_ACF.1/UCP requires the TSF to provide

access control to enforce the update SFP. The SFR FMT_MSA.1 prevents the modification of security attributes "version number" of the UCP.

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

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

6.3.3 Security Assurance Requirements Rationale

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

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

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

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

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

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

the TOE.

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

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

7 Package Trusted Channel between TOE and CSP

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

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

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

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

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

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

Table 11: Elliptic Curves, Key sizes and Standards

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

Asset	Protection
PACE Password	integrity, confidentiality

Table 12: Additional assets in package Trusted Channel to be protected by the TOE

FTP_ITC.1/TC Inter-TSF trusted channel

Hierarchical to:	No other components
Dependencies:	No dependencies
FTP_ITC.1.1/TC	The TSF shall provide a communication channel between itself and **the CSP** that is logically distinct from other communication channels and provides assured identification of its end points **TOE and CSP** and protection of the channel data from modification .
FTP_ITC.1.2/TC	The TSF shall permit the TSF to initiate communication via the trusted channel.
FTP_ITC.1.3/TC	The TSF shall initiate communication via the trusted channel for communication with the CSP.

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

For A-Trust SMAERS for a.sign TSE Online: No sensitive data is transferred over the trusted channel.

FIA_UAU.5/TC Multiple authentication mechanisms

Hierarchical to:	No other components
Dependencies:	No dependencies
FIA_UAU.5.1/TC	The TSF shall provide

1. PACE with Generic Mapping with user in PCD role with establishment of a trusted channel according to FTP_ITC.1/TC,
2. no other method of authentication
3. message authentication by MAC verification of received messages to support user authentication.

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

1. PACE may be used for authentication of a CSP with establishment of a trusted channel according to FTP_ITC.1/TC,
2. message authentication by MAC verification of received messages shall be used after initial authentication of a remote entity according to clause (1) for a trusted channel according to FTP_ITC.1/TC.

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

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

Hierarchical to:	No other components
Dependencies:	No dependencies
FIA_API.1.1/TC	The TSF shall provide a PACE PIN in PCD role to prove the identity of the TOE to **a CSP and establishing a trusted channel according to FTP_ITC.1/TC**.

FCS_CKM.1 Cryptographic Key Generation - Key Agreement for Trusted Channel PACE

Hierarchical to:	No other components
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys for FCS_COP.1 in accordance with a specified cryptographic generation algorithm PACE with brainpoolP256r1 and Generic Mapping in PCD role and specified cryptographic key sizes 256 bits that meet the following: [ICAO], Section 4.4

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

FCS_CKM.4 Cryptographic Key Destruction

Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwrite with all zeroes that meets the following: NIST SP800-88 Rev.1.

FCS_COP.1 Cryptographic Operation

Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1	The TSF shall perform MAC calculation and MAC verification in accordance with a specified cryptographic algorithm according to AES-256 [FIPS197] in CMAC (NIST SP800-38B) [NIST2005] and cryptographic key sizes 256 bits that meet the following: the referenced standards above according to the chosen selection

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

to FCS_CKM.1.

FCS_RNG.1 Random Number Generation

Hierarchical to:	No other components
Dependencies:	No dependencies
FCS_RNG.1.1	The TSF shall provide a deterministic random number generator that implements:

(DRG.3.1) If initialized with a random seed [utilizing user input], the internal state of the RNG shall have 125 bits of entropy.

(DRG.3.2) The RNG provides forward secrecy.

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

FCS_RNG.1.2 The TSF shall provide random numbers that meet

(DRG.3.4) The RNG, initialized with a random seed [utilizing user input], generates output for which 2^{34} strings of bit length 128 are mutually different with probability $1-2^{-16}$.

(DRG.3.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A.

Note: Since the TOE is a pure software TOE, it is only possible to get sufficient random input from its environment. The developer decided to make use of a combination of an OS RNG output and additional user input. Because of missing reliable information for the entropy output of the OS RNG the additional user input is necessary and claimed as the seed input in this SFR only. The user is clearly informed via guidance documentation and the output of the tool in the provisioning phase how the seed has to be provided in order to get finally sufficient entropy input.

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

The dependencies are fulfilled:

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

Table 13: Dependency Rationale for the Functional Package

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

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

8 TOE Summary Specification

8.1 SF.GenLM Generation of Log messages

If the TOE is in the CTSS role (which is only activated when all self-tests have successfully passed), importing of Transaction Data is allowed. It then creates the DTBS incrementing the transaction counter retrieved from the secure storage of the platform and signs a request using the TC signature key and sends it to the CSPL.

CSPL generates the signed log message.

(FDP_ACC.1/LM, FDP_ACF.1/LM, FDP_ITC.2/TD, FDP_ETC.2/DTBS, FDP_ITC.2/TSS)

The TOE provides management functions with regard to the

- definition of the lifetime of ongoing transactions,
- behavior of functions testing external entities,
- behavior of functions testing external entities in case of failure of tests,
- selection of audited events,
- behavior of functions regarding automatic export of audit trails,
- management of authentication data records,
- changing initial passwords,
- registration of allowed `client_Ids` and associated signature creation keys,
- definition of the number of audit records causing automatic export and clearing of exported audit records,
- definition of the percentage of storage capacity of audit records.

(FMT_SMF.1 , FMT_SMR.1)

The TOE interprets all input data from trusted IT products with regard to [TR SE] and [TR TSEA]. (FPT_TDC.1)

TOE generates audit records for the following auditable events:

- startup and shutdown
- system operation commands as specified in [TR SE]
- reaching of the threshold of unsuccessful authentication
- failure with preservation of secure state
- setting of the version number of the UCP and upgrade of stored data

(FAU_GEN.1/SYS)

TOE allows manual export of audit trail by the CSP role using the function exportAuditTrail retreiving the audit log messages from CSPL and exports them. Upon successful export the messages are cleared using the function clearAuditTrail.

TOE protects the audit trail against unauthorised modification and deletion by storing them on the CSPL until audit trail export get cleared (FAU_STG.1/SYS).

TOE periodically checks the number of audit messages on the CSPL which need to be exported and in case this number exceeds the configurable range, TOE enters secure state (FAU_STG.3/SYS).

Only administrators are allowed to determine and modify the behavior of the function FPT_TEE.1 (FMT_MOF.1, FMT_SMF.1).

As required by FMT_MTD.1/SYSAdmin only administrators are allowed to

- select audited events
- define the number of audit records causing automatic export and clearing of exported audit records
- define the percentage of storage capacity of audit records

Only the CTSS interface role is allowed to export and clear system logs (FMT_MTD.1/SYSCTSS).

Only the CTSS interface role is allowed to set the accepted set of clientIDs and select the corresponding keyId used for signing the transaction logs.

Only the CTSS interface role is allowed to set the keyId for signing system logs and audit logs respectively.

The CTSS interface role ensures that the internally stored transaction number is increased by one whenever a transaction is started using the secure platform.

TOE does not allow to modify the imported transaction number.

The security attribute version number is only increased when the TOE is in CSP role. (FMT_MSA.1)

The TOE ensures that the transaction numbers are building a strong increasing sequence without gaps and the time stamps of log messages are in a non decreasing sequence by only increasing the transaction in case of StartTransaction. In case of Update and FinishTransaction the TOE ensures that the transaction number belongs to an ongoing transaction. (FMT_MSA.2, FMT_MSA.4)

`no one` is allowed to overwrite the provided initial values of the security attributes due

to the secure platforms authentication mechanism. (FMT_MSA.3)

8.2 SF.ImpExp Import of Transaction Data from and Export of Log message to CTSS interface component

The TOE imports Transaction Data (only if the TOE is in CTSS and CSP role) from the ERS and establishes a trusted channel with the CSPL using the PACE protocol. The TC uses only the signature key. TOE is responsible for the import of audit records. Import and export of data is performed according to TR SE and TR TSEA. (FDP_ACC.1/LM, FDP_ACF.1/LM, FDP_ETC.2/LM, FDP_ITC.2/TD, FMT_MSA.4, FMT_SMF.1, FMT_SMR.1, FPT_TDC.1)

8.3 SF.IAA Identification of external entities and authentication of Administrators

TOE is delivered in an uninitialized state, the administrator has to set a new password (FIA_ATD.1). This password is used to authenticate the Administrator when the TOE acts on behalf of Administrator. Authentication reference data is verified using the secure platform mechanism. (FMT_SMR.1, FIA_UAU.5).

The administrator is able to reset this Authentication Data Record using unblockUser (FMT_MTD.1/AD).

There is an Authentication Time-Out enforced by the TOE. Users get re-authenticated under the conditions power on or reset (FIA_UAU.6).

Configuration regarding the security functions behaviour (cf. FMT_MOF.1) and security attributes (FMT_MTD.3/PW) is stored in the secure platform environment.

The CTSS-Administrator has to specify accepted values of “Serial number of ERS” by calling the registerERS function. The administrator has to map serial numbers of ERS to signature creation keys used for transaction logs and system logs by calling mapERSToKey. The list of accepted serials, and mappings is maintained by the secure platform.

The TOE starts in the Unidentified User role. The TOE tests the ERS and CSP Identity. Only if all tests of external entities and self tests are successfull, the TOE enables the CTSS interface and CSP role. A user is only associated with the Administrator role after successful authentication. After 10 unsuccessful attempts, the Administrator role gets blocked until it gets successfully unblocked using a valid PUK (FIA_USB.1,

FIA_AFL.1).

8.4 SF.SecMan Security management

The TOE maintains the following roles which are associated to users: unidentified user, administrator, CTSS interface role and CSP role (FMT_SMR.1). The TOE restricts the security management of TSF and TSF data to authenticated Administrators. The TSF prevents management of the Transaction Number generation.

Security Management functions can only be used after successful authentication of an administrator.

The administrator has to specify accepted values of "Serial number of ERS" by calling the registerERS function.

The administrator has to map serial numbers of ERS to signature creation keys used for transaction logs and system logs by calling mapERSToKey. The list of accepted key serial numbers, and the respective mappings are protected by the secure platform. (FMT_MSA.1).

Only administrators are allowed to determine and modify the behavior of the function FPT_TEE.1 (FMT_MOF.1, FMT_SMF.1).

The last transaction number is incremented by TOE and is stored on the secure platform. (FMT_MSA.2, FMT_MSA.4) `no one` is allowed to specify alternative initial values for the transaction number (FMT_MSA.3).

Only administrator is able to delete and reset this Authentication Data Record (FMT_MTD.1/AD). The TOE enforces strong passwords and changing the initial password (FMT_MTD.3/PW).

8.5 SF.TEE Test of external entities

After ERS loads the TOE, it is in the secure state with the Unidentified User role. The TOE tests the ERS and CSP Identity. Only if all tests of external entities and self tests are successfull, the TOE leaves the secure state and enables the CTSS interface and CSP role (FIA_ATD.1, FPT_FLS.1, FPT_TEE.1, FIA_UAU.1, FIA_UID.1).

At startup and during operation the TOE ensures that the transaction number is strictly monotonically increasing and only registered `client_Ids` are allowed to use the according signing key and that the version number is only increasing after a successful update (FMT_MSA.1).

Only the role administrator is allowed to use the function password authentication, define a transaction timeout, use the management functions and modify their behaviour in case of failure regarding testing of external entities and select the auditable events and the

automatic export of audit trails according to FMT_MOF.1.

8.6 SF.TST Self-test and secure state

A-Trust provides cryptographic checksums of the TOE, user MAY verify the integrity. Furthermore the client component is signed which can be verified by platforms supporting code signing.

The TOE performs self-tests on startup, shutdown and periodically during operation. If one of the self-tests fails, it enters a secure state. The TOE also enters the secure state if the test of the electronic record-keeping systems fails, or the test of cryptographic service provider fails. (FPT_FLS.1, FPT_TST.1, FPT_TEE.1)

User data is stored on the secure platform including a version number, hence illegal modification can be detected. The digital signature of the UCP is verified by the SMAERS platform during the platforms native installation process (FDP_ACF.1/UCP). After an update and on every startup the TOE verifies that the version number of the user data is not modified and no unauthorized downgrade attempt was made. (FDP_ITC.2.2/UCP_UD)

Security attributes are unambiguously associated with the exported user data, because they are stored in the secure platform including a version number.

When exporting or importing user data their values must not be modified. (FDP_ETC.2.1/UCP_UD)

Security data is interpreted acccording to the included version number. (FDP_ITC.2.4/UCP_UD, FDP_ACC.1/UCP, FDP_ETC.2.1/UCP_UD, FDP_ITC.2.1/UCP_UD)

8.7 SF.SecUCP Secure download and authorized use of Update Code Package

The TOE is updated using Update Code Packages which are signed by an authorized entity.

Only Administrator is allowed to import received UCP if the digital signature of the UCP is successfully verified by the platform. Furthermore the version number of the UCP has to be equal or greater than the current version.

User data is stored with its associated version number, which is validated after a successful update. In case of an unsuccessful update a log message is generated.

(FDP_ACC.1/UCP, FDP_ACF.1/UCP, FDP_ETC.2/UCP_UD, FDP_ITC.2/UCP, FDP_RIP.1/UCP, FMT_MSA.1, FMT_MSA.2).

The TOE ensures that any previous information content of a resource is made unavailable

upon the deallocation of the resource after successful upgrade previous code and data is deleted (FDP_RIP.1/UCP)

8.8 SF.ImpExpUCP Secure Import and Export of User Data

During every export of user data, the version number of user data is included. On every import the TOE verifies that the version number of the user data is not modified and no unauthorized downgrade attempt was made. (FDP_ITC.2.2/UCP_UD, FDP_ETC.2.2/UCP_UD)

8.9 SF.SecCommCSP Secure communication between TOE and CSP

The TOE and the CSPL are physically separated components and thus there is a trusted channel between the TOE and the CSPL. The protocol used for the trusted channel is PACE according to [ICAO] (FIA_ITC.1/TC). CSPL is authenticated using this PACE channel (FIA_UAU.5/TC). Keys for the key agreement are generated according to (FCS_CKM.1). A PACE PIN is used by TOE to establish the trusted channel to CSPL (FIA_API.1/TC). Random numbers are generated according to FCS_RNG.1. Transmitted data in the secure channel is authenticated using a MAC according to (FCS_COP.1, FIA_UAU.5/TC, FIA_ITC.1/TC). As soon as keys are not needed any more, they are deleted according to (FCS_CKM.4).

9 References

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

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

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

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

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

[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

[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)

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

[PP CSPLight] Common Criteria Protection Profile Cryptographic Service Provider Light, BSI-CC-PP0111-2019

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

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

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

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

[PP-SMAERS] Common Criteria Protection Profile Security Module Application for Electronic Recordkeeping Systems (SMAERS), BSI-CC-PP-0105-V2-2020

[TR03153] Technische Richtlinie BSI TR-03153Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme Version 1.0.0, 6. Juni 2018 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03153/TR-03153.pdf?__blob=publicationFile

[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.

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

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

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

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

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

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

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

[TR 03110] BSI: Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.20, Feb 2015.

[PKI-Konzept] PKI-Konzept für CSPLight 1.0, 30.07.2020

[Umgebungskonzept] A-Trust SMAERS Umgebungskonzept 0.5, 15.03.2021

[Updatekonzept] A-Trust SMAERS Updatekonzept 0.3, 09.03.2021

[ope] Operational user guidance - SMAERS for a.sign TSE Online v1.0.3,

26.07.2021

[Utimaco-CSPLight] Utimaco CryptoServer Core-API 1.6.0, 19.02.2021

[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.