D-TRUST | Ein Unternehmen der Bundesdruckerei

D-TRUST Web-Dienst TSE-SMAERS Security Target

Version 2.1.20, 2021-11-16

Table of Contents

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:

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

This Security Target defines the security requirements of the SMAERS component. This Security Target document covers D-TRUST Web-Dienst TSE-SMAERS.

The requirements and descriptions in this document apply to both TOE if not explicitly limited to one TOE.

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

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

1.1. ST Reference

- ST Reference: D-TRUST Web-Dienst TSE-SMAERS Security Target
- Sponsor: D-TRUST GmbH, Kommandantenstr. 15, 10969 Berlin
- Developer: Bundesdruckerei GmbH, Kommandantenstr. 18, 10969 Berlin
- ST Version: 2.1.20
- ST Date: 2021-11-16
- CC Version: 3.1 Revision 5
- Certification ID: BSI-DSZ-CC-1137-V3

- Assurance Level: EAL 2 augmented with ALC_LCD.1 and ALC_CMS.3

1.2. TOE Reference

- TOE Name: D-TRUST Web-Dienst TSE-SMAERS
- TOE Version: 1.3.3

1.3. TOE Overview

D-TRUST Web-Dienst TSE-SMAERS is part of the D-Trust TSS. D-Trust develops a webservice as a remote form of a "Technical Security System", (TSS, "Technische Sicherheitseinrichtung") in a client/server architecture.

This webservice follows the following specifications

- Technische Richtlinie TR-03153 (**[BSI-TR-03153]**): "Technische Sicherheitseinrichtung für Elektronische Aufzeichnungssysteme". This document describes the basic structure of a TSS and its functionality. The major components of the TSS are the secure element (SE), the SE-API and the secure storage.
- Technische Richtlinie TR-03151 (**[BSI-TR-03151]**): "Secure Element API (SE-API)". This document defines treating the transactions and retrieving the signed data from the secure element as well as the management functionality. Also, it defines the data formats for the messages that are created by the TSS.
- Common Criteria Protection Profile BSI-CC-PP-0105 (**[PP-SMAERS]**): Schutzprofil für die Anwendungskomponente des Sicherheitsmoduls ("Security Module Application for Electronic Record-keeping Systems", SMAERS). This PP defines the security and assurance requirements for the TOE described in this ST.
- Common Criteria Protection Profile BSI-CC-PP-0111 (**[PP-CSP-LIGHT]**): 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.

The following picture shows the TOE as part of the TSS client :

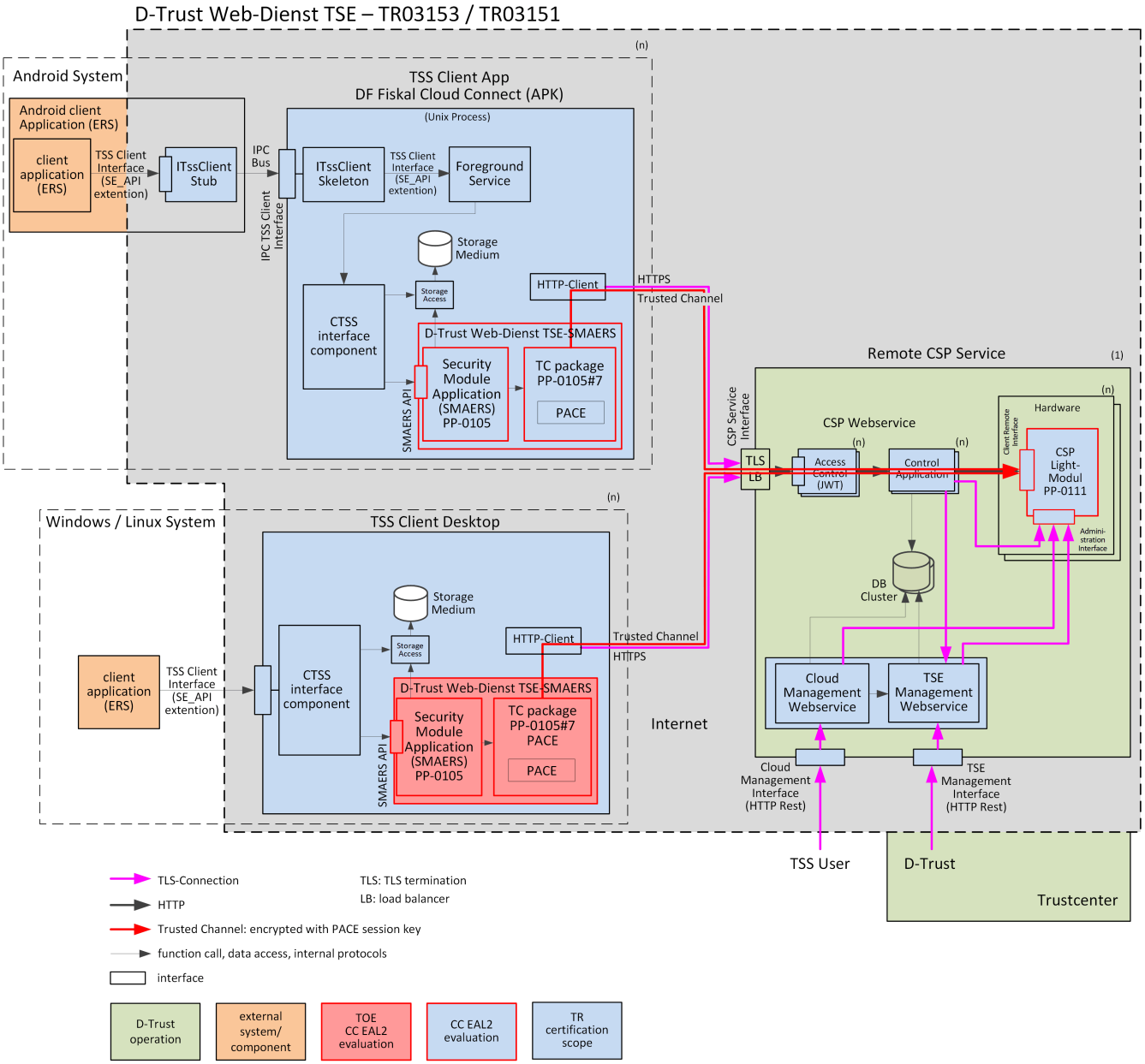

Figure 1. Architecture of the webservice

1.3.1. Integration of the TOE in the Environment

The webservice as to see in **Figure 1** comprises several specific applications that work together to form a TSS and to address the challenges of a remote operation of a TSS.

TSS Client Desktop exposes the functionality of the SE-API. The TSS Client is intended to be installed on a ERS or at the operational environment under the physical control of the taxpayer (see figure 2c **[PP-SMAERS]** and represents the primary interface to the end user (being the ERS). The TSS Client comprises the following components:

- The **CTSS interface component** implements the user interface "TSS client interface". The functionality of the TSS client interface is implemented according to **[BSI-TR-03151]** even though it is not completely compliant.
- The **Secure Storage** is provided by the ERS as the TOE is a pure software TOE.
- The **D-TRUST Web-Dienst TSE-SMAERS** as described in this Security Target

The **Remote CSP Service** is operated by D-Trust in their Trustcenter. It is used by multiple TSS clients in order to sign data. It specifically comprises the following components:

- The **CSP Webservice** is responsible for the authentication of the incoming request of a TSS client and for processing the request. It comprises the modules Access Control Module that is responsible for the verification of the token that is transmitted along with the http request and the Control Application that checks for existence and status of the account of the TSS based on the transmitted key reference.
- The **CSP Light Module** is responsible for a certain amount of signature keys (and therewith taxpayers). This module is involved in the negotiation of the trusted channel with the TSS clients and creates the signatures for the ERS.
- The **Cloud Management Web Service** implements the management of the data of the TSS account. This module implements the life cycle of the TSE from the perspective of a TSS user (start operation, decommission, etc.).
- The **TSE Management Web Service** implements the TSE Management interface and allows the trust center to perform the required administrative operations.

1.3.2. Usage and major security features

The TOE provides the following major security features:

- The TOE receives transaction data from the ERS
- The TOE generates time stamped and signed Transaction Log messages using the CSP cryptographic services in order to generate verifiable sequences of transaction data and Log messages for cash inspection (cf. **[KassenSichV]** section146b).
- The TOE imports audit records from the CSP-light and exports them as Audit LogMessages
- The TOE securely maintains the transaction counter
- The TOE restricts the access of ERS to the services of the TOE based on their IDs
- The TOE receives signed data from the CSP and stores them on the secure storage.
- The TOE implements a trusted channel to the CSP light,

- The TOE implements a self test including tests of the CSP light and the ERS,
- The TOE offers function for administration of its security functions, the TOE also offers the authentication of a TR-administrator for further administrative functions outside the TOE,
- The TOE offers functionality in the context of a secure software update.

1.3.3. TOE type

The TOE is a pure software component that provides the functionality of SMAERS according to **[PP-SMAERS]**. In terms of **[SMAERS-PP]** 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). The TOE does not provide any kind of interface for direct user interaction. Instead, the TOE provides its services via a programming interface to be consumed by other applications.

The TOE has been developed as a Java application and its source code does not differ amongst the various Operating Systems.

1.3.4. Required non TOE-Hardware/software/firmware

The TOE is developed as part of the D-Trust TSS Client and requires

- the availability of the D-Trust TSS Client component that provides the functions for SE-API,
- a network connection to a certified CSP as part of the D-Trust backend
- an underlying platform with a secure storage (see OE.SMAERSPlatform),

Also, the TOE has been developed as a Java application and requires one of the following runtime environments in its environment.

1. AdoptOpenJDK OpenJ9 (jdk8u292-b10_openj9-0.26.0)
2. Azul Zulu Community Java 8 (8u292b10 Zulu: 8.54.0.21)

If the TOE is operated under OS-X based on the M1 CPU, the Azul Zulu Community Java 8 8u302b08, Zulu: 8.56.0.23 shall be used.

The D-TRUST Web-Dienst TSE-SMAERS is agnostic of the underlying OS and only relies on the services provided by the Java Virtual Machine. Please note however that the TOE is only intended for use on platforms with CPUs of the x86, x64 or ARMv8 architecture and the following classes of Operating Systems.

- Windows Embedded POSReady 7

- Windows 10 and Windows Server 2016/2019
- Windows 8.1 and Windows Server 2012
- Linux distributions RHEL/CENTOS/Oracle Linux
    - RHEL 6-8
    - CentOS 6 -8
    - Oracle Linux 6-7
- von Suse
    - Suse Linux (Enterprise and OpenSuse) 11-15
- Linux Distributions based on Debian incl. Ubuntu
    - Debian 8-9
    - Ubuntu 12.04-21.04
    - Raspbian OS based on Debian 8-9
- Flatcar OS (Stable Version 2905)
- OS-X
    - 10.15 (Catalina)
    - 11 (Big Sur)

The TOE has been developed for use with D-TRUST Web-Dienst TSE-CSP Security CSP-light which is undergoing certification according to **[PP-CSP-LIGHT]**, **[PPC-CSP-TS-Au-Cl]** and **[PPC-CSPLight-TS-Au-Cl]**. The API of the CSP is described in **[CSP-FSP]**. The TOE requires the platform to provide secure storage; specific requirements on this topic are defined in **[SMAERS-INT]**. In the course of this evaluation, the TOE has been tested in combination with version 1.3.1 of the D-TRUST Web-Dienst TSE-CSP Security CSP-light. While the TOE is cabable of operating on any of the aforementioned Operating Systems, it has specifically been tested under Red Hat Enterprise Linux 8, 64 bit in the course of the evaluation.

1.3.5. TOE Life Cycle

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

According to **[SMAERS-PP]**, the additional documentation must address, but is not limited to the

following documents:

1. The provisioning of the CSP within the life cylce of the CTSS describing the initial personalization and subsequent renewal of keying material used in the context of the TOE, the assignment and separation of users and roles contained in the CSP, and the audit configuration of the CSP.This concept is provided in form of **[PKI-Konzept]**.
2. 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. This information is provided in form of **[SMAERS-update-concept]**,
3. The PKI concept of the underlying public key infrastructure (PKI) and the audit reports of the involved trust centers to ensure the correct identification of the taxpayer, the binding of the CTSS and keying material to the taxpayer, and the verifiability of generated signatures by third parties. This concept is provided in form of **[PKI-Konzept]**.

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

Additional documentation must be provided in the following cases:

1. If the client-server model is used, the personalization and management of the password used to protect the trusted channel between the TOE and the CSP must be described. As this ST bases on a client-server model, this information is also in form of **[PKI-Konzept]**.
2. If a CSPLight is used instead of a CSP, it must be securely operated in an environment certified according to ISO/IEC 27001. The operator must implement and continuously maintain an information security management system (ISMS) with security level high according to Appendix: Operational Requirements for CSPLight. As this ST bases on the use of a CSP-light, this information is also provided as part of **[PKI-Konzept]**.

1.4. TOE Description

1.4.1. Introduction

The TOE is the main part of the D-Trust TSS client for Desktop and is comprised of a software library that supports a ERS following the requirements of the **[KassenSichV]**

1.4.2. TOE boundaries

physical boundaries

The TOE is a software library that does (strictly speaking) have no physical boundaries. The complete TOE in terms of the Common Criteria comprises:

- The software library implementing the SMAERS functionality on all systems.
  - smaers-1.3.3-400793-hotfix_3.0.0.jar (Hash value: 9aeefb774dcc956c8800233d2c1d1e1e3d5981890f764699d489e6c7cb5050de)
- An integration-, configuration and operations manual formatted as a PDF document (**[SMAERS-INT]**) which is augmented by information on the secure environment of the TOE (**[SMAERS-UMGEBUNG]**, **[SMAERS-UMGEBUNG-CLOUD]**),
- An interface definition for application developer (smaers-api.zip, SHA-256 value: 8501b8e9011d2f4acce7efbbcb17ab71cf2d59865d331a892d85068caf45ff74 (**[SMAERS-API]**))

As desired, the guidance documents and the TOE are delivered to the customer (the integrator) via a personal delivery, encrypted and signed email or a secure download portal. The PDF documents and the JAR files that make up the TOE are signed in order to allow a verification of their authenticity at any time.

logical boundaries

The TOE is responsible to receive transaction data, process it and retrieve the corresponding signatures by the CSP. For this purpose, the TOE will add a transaction counter to the transaction data that is maintained on the secure storage. The TOE ensures that the transaction counter is incremented before a new transaction is started. In addition, the TOE imports audit records from the CSP-light and exports them as Audit LogMessages to the ERS.

The TOE utilizes the PACE algorithm to derive a temporary cryptographic key from a pre shared secret and uses the temporary key to secure the communication channel between itself and the CSP. Via this channel, the processed transaction data will be sent to the CSP and signatures and log messages are returned back. The TOE maintains a list of clientIDs of approved ERS. This list can be maintained using the role *CTSS interface*. The TOE will not accept any transaction data by a ERS whose ID is not on this list.

The administrator (SMAERS administrator as well as TR administrator) authenticates against the TOE by the use of a PIN. The PIN is secured by the use of a retry counter and the Administrator account will be blocked after a wrong PIN has been entered 5 times. A blocked Administrator account can only be recovered by use of a PUK.

The TOE provides mechanisms for management and self tests (which includes tests of the ERS and the

CSP light). More details about this can be found in the TOE Summary Specification.

The TOE generates a system log consisting of commands and TSF security events as certified data and Transaction Log Messages for transactions. The logical boundaries of the D-TRUST Web-Dienst TSE-SMAERS are represented by the functionality outlined in the previous paragraphs. As the TOE is implemented in Java, it primarily exposes its services via a Java programming interface. As outlined later in this chapter, the TOE has not been developed to be directly used by end users. Instead, customers will install and use the complete TSS client that the TOE is part of.

The following listing shows an examples, of how the TOE can be invoked by another component.

Cryptographic primitives

The following table summarizes the cryptographic primitives that are exposed via the interfaces of the TOE.

Table 1. Cryptographic primitives

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application
Authenticity (of exported *Log Messages*)	SHA384withPLAIN-ECDSA	**[FIPS_186-4]** B.4 and D.1.2.4, **[BSI-TR-03111]**	Curve: 1.3.132.0.34 (secp384r1)	**[PP-CSP-LIGHT]**, **[PP-SMAERS]**
Communication with CSP	PACE with AES CMAC CBC mode with PKCS5 padding	TR-03110-2, **[NIST800-90A]** , **[NIST800-38B]**,<<[NIST800-38A>>, **[PKCS5]**	256 bit, brainpoolP256r1	**[PP-SMAERS]**, **[PP-CSP-LIGHT]**

It should be noted that while these cryptographic primitives are exposed via the interface of the TOE, some are implemented by the CSP.

In addition, the TOE provides a functionality for a secure update.

For the operation of the corresponding CSP-light, a certified ISMS (see **[ISMS-Zert-CSP]**) and a dedicated PKI concept (see **[PKI-Konzept]**) are available. For the audit configuration of the CSP-light that is required by the Protection Profile, it should be mentioned that the TOE uses the CSP-light with all available audit events enabled.

2. Conformance Claims

2.1. CC Conformance Claim

As defined by the references [CC1], [CC2] and [CC3], this Security Target:

- conforms to the requirements of Common Criteria v3.1, Revision 5 and
- is Part 2 extended,
- is Part 3 conformant.

2.2. PP Claim

This Security Target claims strict conformance to [PP-SMAERS].

2.3. 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 to be conformant to the assurance package as defined by EAL2 augmented with ALC_LCD.1 and ALC_CMS.3.

2.4. Conformance Rationale

The TOE as described in this ST is a product that allows to protect transaction data of Electronic Record Keeping Systems by using a certified cryptographic service provider (CSP).

It therewith falls directly into the classes of TOEs that are defined by [PP-SMAERS]. In chapter 1.2 [PP-SMAERS] states:

> 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.

[PP-SMAERS] requires strict conformance which is claimed by this Security Target. By claiming the strict conformance it is also ensured that this ST is conformant with respect to the

- Security Problem Definition,
- Security Objectives and
- Security Requirements

from [PP-SMAERS].

3. Security Problem Definition

3.1. Introduction

The Security Problem Definition is identical to the one of **[PP-SMAERS]**. The changes as required due to the use of the functional package for the PACE channel as described in chapter 7 of **[PP-SMAERS]** have been made. No further changes were made by the authors of this Security Target.

Assets

The assets of the TOE are

- the transaction data provided by the CTSS interface component, where authenticity and integrity including completeness of the transaction data shall be protected, i.e. verification of the transaction log messages shall determine whether the transaction data was received from the CTSS interface component, and modifications and gaps shall be detectable,
- the transaction number (as part of the transaction data) that enumerates transactions. The transaction number must be continuously increasing without gaps.
- the audit records imported from the CSP and exported as audit logs to the CTSS interface component, the system logs and transaction logs
- the update code package (UCP) and the UCP version number
- the PACE password to setup the trusted channel to the CSP (only in case the package 'Trusted Channel' is claimed).

The following table summarizes the assets and their need for protection

Table 2. Assets to be protected by the TOE

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

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

Users and subjects

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

- electronic record-keeping system (ERS),
- CTSS interface component,
- CSP,
- administrator (comprising SMAERS-administrator and TR-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 for the TOE is D-Trust or an integrator acting on behalf of D-Trust. Due to the implemented concept for administration, no administration in the field is foreseen. This way, the end user does not need any administrative privileges. The TR-administrator on the other hand is able to perform certain administrative tasks that require administrative permissions according to **[BSI-TR-03151]**. It should be noted that these functions are not implemented by the TOE itself but rather by the CTSS interface component in the direct environment of the TOE. To be more precise: the CTSS interface component utilizes the authentication functionality of the TOE for the authentication of the TR-administrator. The actual access control for functionality that is only accessible for the TR-administrator is then implemented by the CTSS component. In contrast to the SMAERS-administrator, the TR administrator does not have to be independent of the tax payer.

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

Roles

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

role unidentified user

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

role SMAERS-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 TR-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. In contrast to the SMAERS-administrator, the TR administrator does not have to be independent of the tax payer.

role CTSS interface

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

CSP role

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

Objects

The TSF operates on the following types of user data objects

- transaction data (TD),
- audit records,
- data-to-be-signed (DTBS),
- protocolData with signature containing the time stamp, the signature counter, and the digital signature; all generated by the CSP (cf. **[BSI-TR-03153]** and **[ICAO-Doc9303]**),
- 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 **[BSI-TR-03151]**.

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. **[BSI-TR-03151]**, chapter 2.3.1)
  - in case of a system log: the security related events with the type of the certified data system log, object identifier (id-SE-API-system-log): bsi-de (0.4.0.127.0.7) applications (3) sE-API (7) sE-APIdataformats(1) 2 (cf. **[BSI-TR-03151]**, chapter 2.3.2)
  - in case of an audit log: the audit record with the type of the certified data audit log, object identifier (id-SE-API-audit-log): bsi-de (0.4.0.127.0.7) applications (3) sE-API (7) sE-API-dataformats(1) 3 (cf. **[BSI-TR-03151]**, 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 **[BSI-TR-03151]** for details of the log messages format.

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

Security attributes

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

- user identity (User-ID),

- authentication reference data,
- role with detailed access rights gained after successful authentication.

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

Passwords as authentication reference data have the security attributes

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

The transaction data (TD) have the security attributes

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

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

The TOE manages for each known keyID the last assigned transaction number and the transaction numbers of the ongoing transactions. If the type of the operation of imported transaction data is StartTransaction, then a new transaction is started and the TOE generates a new transaction number by addition of 1 to the last assigned transaction number, includes this value in the protocol data of the transaction log returned to the CTSS interface component, and add this value to the list of ongoing transaction. If the type of the operation is UpdateTransaction or 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. **[BSI-TR-03151]**.

A UCP has the security attributes

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

Log messages

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

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

The following security attributes are conditional in log messages:

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

3.2. Threats

T.EvadTD: Evading Transaction Data

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

T.ManipTD: Manipulation of Transaction Data

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

T.ManipDTBS: Manipulation of Data To Be Signed and time stamped

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

T.ManipLM: Manipulation of a Log message

The attacker manipulates without detection a log message exported to the CTSS interface

component. This log message is then used for cash inspection.

T.ManipLMS: Manipulation of a Log message sequence

The attacker manipulates without detection the log message sequence exported to the CTSS interface component. This log message sequence is then used for cash inspection.

T.ManipTN: Manipulation of Transaction Number

The attacker manipulates the TOE's internal transaction number used in log messages.

T.FaUpD: Faulty Update Code Package

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

PP 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.

Consideration of Application Note 1: The aforementioned Application Note has been considered. It lead to an administrative concept in which the administrator (D-Trust or an integrator on behalf of D-Trust) will perform all required administration before the TOE is initialized at the taxpayers site. No administrative functionality by the SMAERS-administrator is planned during operation.

3.3. Organizational 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 device

The taxpayer shall correctly operate the electronic record-keeping system (cf. **[FCG]**, Section 379 (1), Sentence 1, Number 4), and correctly protect the electronic record-keeping system and the certified security device; cf. [FCG], Section 379 (1), Sentence 1, Numbers 5.

OSP.ValidTrans: Validation of transactions

A sequence of transactions is valid if

1. all Log messages meet the requirements for content defined in **[KSV]** section 2,
2. their check values according to [KSV] section 2 sentence 2 number 7 are valid digital signatures,
3. the transaction numbers are consecutive increasing without gaps (cf. **[KSV]** section 2 sentence 4), and
4. the points in time when the transaction starts are monotonic increasing.

The sequence of Log messages support detection of incomplete transactions and manipulations.

OSP.Update: Authorized Update Code 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.

PP Application Note 2: 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.

Consideration of Application Note 2: The aforementioned Application Note has been considered during the design of the update mechanisms. Please refer to the descriptions in the **Section 8** for more details.

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 conformant 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 conformant to **[PPC-CSP-TS-Au]** or **[PPC-CSP-TS-Au-Cl]** (platform architecture). The CSP exports audit records in form of audit logs meeting **[BSI-TR-03151]**.. Also, the CSP must provide a fully defined API description.

A.ProtComCSP: Protection of communication between TOE and CSP

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

A.ProtComERS: Protection of communication between TOE and electronic record-keeping system

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

A.VerifLMS: Verification of Log message Sequences

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

A.Admin: Trustworthy Administrator

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

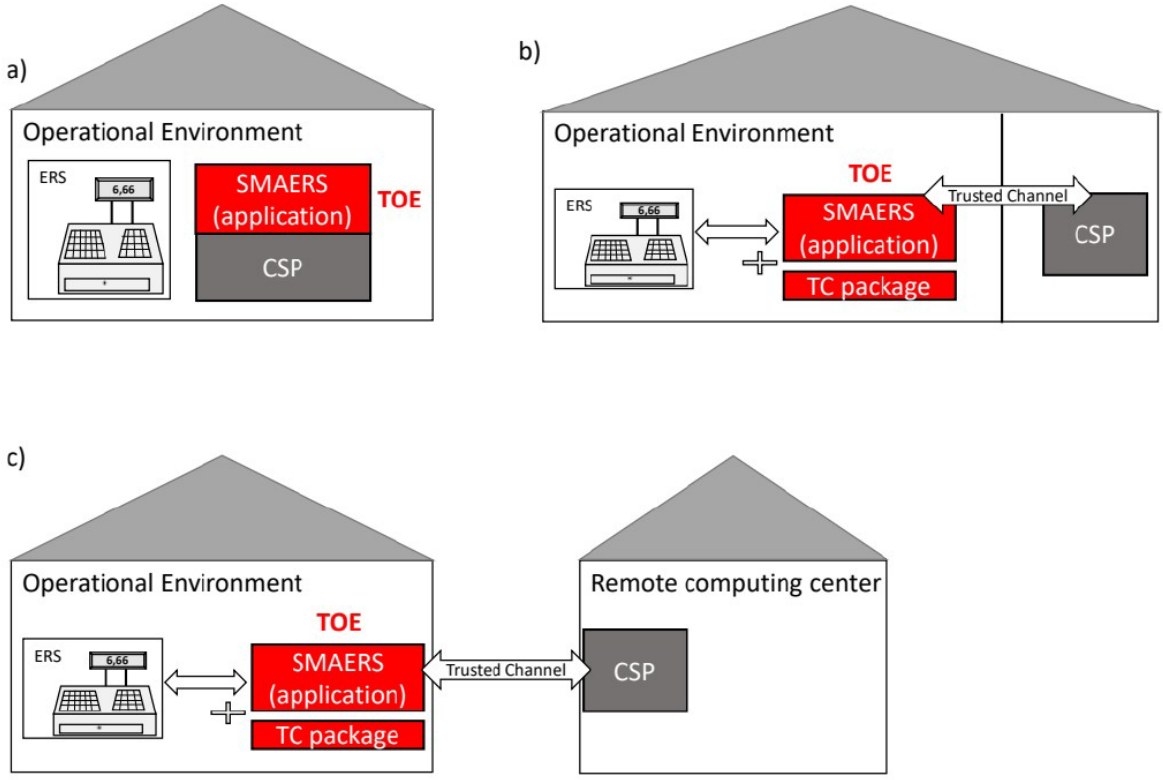

Figure 2. The TOE is always operated as local component. a) Platform architecture b) client-server architecture with local computing center c) client-server architecture with remote computing center

ST Application Note 1: Please note that A.Admin only applies to the SMAERS-administrator.

4. Security objectives

4.1. Security Objectives for the TOE

O.GenLM: Generation of Log messages

The TSF shall generate transaction logs containing

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

The TSF shall generate system logs.

O.ImpExp: Import of Transaction Data from and Export of Log message to CTSS interface component

The TSF shall import transaction data from the electronic record-keeping system through the

CTSS interface component, import audit records from the CSP and export log messages to the CTSS interface component.

O.IAA: Identification of external entities and authentication of Administrators

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

O.SecMan: Security management

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

O.TEE: Test of external entities

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

O.TST: Self-test and secure state

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

O.ImpExpUCP Secure Import and Export of User Data

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

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.

ST Application Note 2: This TOE implements the client-server architecture. Thus, this ST uses the functional package for the PACE channel in chapter 7 of **[PP-SMAERS]**, which adds **O.SecCommCSP** to the list of Security Objectives of **[PP-SMAERS]**, as required by chapter 7.

4.2. Security objectives for the operational environment

OE.ERS: Trustworthy electronic record-keeping system

The taxpayer shall correctly use an electronic record-keeping system that provides separately, correctly, completely and in real time all transaction data that are legally required for the generation of log messages to the TOE (cf. Application Note 1). The electronic record-keeping system shall support testing its presence and identity as an external entity by the TOE. The

electronic record-keeping system shall produce receipts including not only the transaction data, but also the points in time whenever a transaction is started, completed or terminated, as well as the transaction number provided by the certified security device.

OE.SMAERSPlatform Secure platform storage

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

OE.CSP: Cryptographic service provider component

A CSP must be either remotely accessible via a trusted channel to the TOE (client-server architecture) and certified as conformant to **[PPC-CSP-TS-Au]**, **[PPC-CSP-TS-Au-Cl]**, or **[PPC-CSPLight-TS-Au-Cl]** running on hardware that meets Appendix: Operational Requirements for CSPLight. Or, the operational environment shall provide a cryptographic service provider for the TOE that is certified as conformant to [PPC-CSP-TS-Au] or [PPC-CSP-TS-Au-Cl], i.e. using the platform architecture. The CSP shall export audit records in form of audit logs meeting **[BSI-TR-03151]**.

PP Application Note 3: The Common Criteria Protection Profile Configurations **[PPC-CSP-TS-Au]**, **[PPC-CSP-TS-Au-Cl]**, and **[PPC-CSPLight-TS-Au-Cl]** require the cryptographic service provider to provide security services to digitally sign transaction data, to verify a signature of an update code package, and for time services. The CSP audit records shall be exported meeting **[BSI-TR-03153]** in order to avoid a transformation of an audit record into a log message. The vendor of the TOE may provide the TOE together with a certified cryptographic service provider.

Consideration of Application Note 3: The Application Note has been considered. The developer deploys a CSP-light conformant to **[PP-CSP-LIGHT]** and the TOE is intended for use with this CSP only.

OE.CSPPlatform: CSP as secure platform of the TOE

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

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

Consideration of Application Note 4: The Application Note has been considered. The package for the trusted channel is claimed by this ST.

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.

ST Application Note 3: Please note that the requirement of an administrator that shall be independent of the tax payer is only applicable to the SMAERS-administrator. The TR-administrator does not have to be independent of the tax payer.

OE.SecCommCSP Secure communication between TOE and CSP

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

OE.SUCP: Signed Update Code Packages

The manufacturer shall issue digitally signed update code packages together with its security attributes.

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

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

4.3. Security Objectives rationale

Please refer to chapter 4.3 and 7 of **[PP-SMAERS]**.

5. Extended Component definition

Please refer to chapter 5 of **[PP-SMAERS]**.

6. Security Requirements

The CC allows several operations to be performed on functional requirements: *refinement*, *selection*, *assignment*, and *iteration*. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by the word "refinement" in **bold** text and the added/changed words are in **bold** text, or directly included in the requirement text as **bold** text. In cases where words from a CC requirement component were deleted, these words are ~~crossed out~~. Refinements made by the ST author are additionally introduced by the string "refinement:"

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as *italic* text. Selections to be filled in by the ST author appear in square brackets and are underlined.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as *italic* text. Assignments to be filled in by the ST author appear in square brackets and are *italicized*.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/" and the iteration indicator after the component identifier.

6.1. Security Functional Requirements

6.1.1. Security Management

FMT_SMR.1: Security roles

Hierarchical to

No other components

Dependencies

FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the roles:

- *unidentified user*,
- ***SMAERS**- administrator*,

- *CTSS interface role*, and
- *CSP role*,
- [*TR-administrator*].

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 behavior (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. *[management of acceptable ERS Serial Numbers]*

FMT_MOF.1: Management of security functions behavior

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. ~~– refinement: enable and disable the functions password authentication according to **FIA_UAU.5.2**, clause (2) if defined to administrator,–~~
2. ***determine the behavior of and modify the behavior 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 behavior of* the function *FPT_TEE.1* *by definition of the identity and features to be tested of ERS* to *administrator*,**
4. ***determine the behavior of* the function *FPT_TEE.1* *by definition of the identity and features to be tested of CSP* to *administrator*,**
5. ~~strike**refinement: determine the behavior of and modify the behavior 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 20 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) 23to administrator***

ST Application Note 4: It should be noted that the TOE does not provide the administration due to the number 1 of **FMT_MOF.1.1**. The developer assesses this as a more strict implementation of the SFR and refined the text from **[PP-SMAERS]** accordingly. While the SFR restricts management to the role of Administrator, the current TOE does not allow an administration at all. As the TOE does maintain the role of an administrator but simply does not allow the management of this information, it is considered a more strict implementation than required by the SFR.

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.

Consideration of Application Note 5: The application note has no implications to this Security Target.

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 ~~s~~ "clientID"* to CTSS interface role,_
2. ***define depending on the clientID the identity of the signature-creation key (keyID) to be used for the transaction log to CTSS interface role,***
3. ***define the identity of the signature-creation key (keyID) to be used for the system log and audit logs to CTSS interface role,***
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 attribute "version number" of UCP after successful installation to CSP role.***

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

Consideration of Application Note 6: The application note has no implications to this Security Target.

FMT_MSA.3: Static attribute initialization

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 ~~individual users~~ **administrator**:

1. *identity,*
2. *authentication reference data,*
3. *role*

and

a. **security attribute *identity [and none]* belonging to the ERS**
b. **security attribute *identity [and password for PACE]* belonging to the CSP.**

ST Application Note 5: Please note that the requirement in FIA_ATD.1.1 applies to the role SMAERS administrator as well as the TR-administrator.

ST Application Note 6: The Identity of the ERS is represented by its clientID/serial number

PP Application Note 7: The refinements distinguish between the sets of security attributes maintained for authenticated user administrator, and the tested user ERS and CSP according to **FPT_TEE.1**. The security attributes are defined by user by administrator according to **FMT_MSA.1**.

Consideration of Application Note 7: This Security Target separates the security attributes accordingly.

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.***

ST Application Note 7: Please note that FMT_MTD.1.1/AD refers to the SMAERS-administrator.

FMT_MTD.3/PW Secure TSF data - Password

Hierarchical to

No other components.

Dependencies

FMT_MTD.1_AD 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.**

ST Application Note 8: In accordance with **[BSI-TR-03153]**, the TOE does initially not have any PIN for the Administrator. It is enforced that the Administrator has to set the PIN to an initial value upon first use while being authenticated by the use of the PUK.

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 [5] unsuccessful authentication attempts occur related to [*Administrator authentication*].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [met], the TSF shall *[block the Administrator role from further logins]*.

ST Application Note 9: After the TOE has been blocked, the Administrator role can only be unblocked by the use of a PUK. This applies to TR-administrator as well as to SMAERS-administrator

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.*

ST Application Note 10: Please note that the requirement from FIA_USB.1.3 (third bullet) applies to the role SMAERS administrator as well as TR-administrator

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

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*]

ST Application Note 11: Please note that the requirement from FIA_UAU.5.2 applies to the role SMAERS-administrator as well as TR-administrator

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 or after 24 hours*

ST Application Note 12: The TOE functionality **power on or reset** refers to the restart or initial start of the JVM in the environment of the D-TRUST Web-Dienst TSE-SMAERS.

6.1.3. User data protection

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

Hierarchical to

No other components.

Dependencies

FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/LM

The TSF shall enforce the *Log Message SFP* on

1. *subjects:*

a. *subject acting for CTSS interface component,*

b. *subject acting for CSP;*

2. *objects:*

a. *transaction data,*

b. *audit record,*

c. *data to be signed,*

d. *protocolData with signature,*

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 initialization

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 authorize 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]
[FDP_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 ~~user data~~ **transaction data** controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/TD

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

FDP_ITC.2.3/TD

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

FDP_ITC.2.4/TD

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

FDP_ITC.2.5/TD

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

1. *The TSF shall import the transaction data with the security attribute clientID of the ERS 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 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 ~~user data~~ **data to be signed**, controlled under the SFP(s), ~~outside of the TOE~~ **to CSP**.

FDP_ETC.2.2/DTBS

The TSF shall export the user data with the ~~user data's associated~~ **security attributes associated with data to be signed**.

FDP_ETC.2.3/DTBS

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

FDP_ETC.2.4/DTBS

The TSF shall enforce the following rules when user data is exported from the TOE:

1. *data to be signed shall be exported for generation of a Log message with security attribute identifying the private signature key to be used by FDP_DAU.2/TS according to **[PPC-CSP-TS-Au]**, **[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 ~~user data~~ **protocolData with signature and audit records**, controlled under the SFP, from ~~outside of the TOE~~ **the CSP**.

FDP_ITC.2.2/TSS

The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/TSS

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

FDP_ITC.2.4/TSS

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

FDP_ITC.2.5/TSS

The TSF shall enforce the following rules when importing ~~user data~~ **protocolData with signature and audit records** controlled under the SFP from ~~outside of the TOE~~ **CSP** : [*none*]

PP 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 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 CSP providing time stamps by administrator settable internal clock (sf. Selection clause (4) in FPT_STM.1.1). If the CSP meets TR-03151 **[BSI-TR-03151]** for the Transaction logs then the CSP returns a Log message to the TOE. If the CSP generates the time stamp and signatures with signature counter then the TOE shall compile the Log message according to TR-03153 **[BSI-TR-03153]**. The signature counter and the time stamp oftTransaction logs and of audit data received as Audit logs may be used to test the CSP according to **FPT_TEE.1**.

Consideration of Application Note 8: The Application Note has been considered.

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), ~~outside of the TOE~~ **to CTSS interface component**.

FDP_ETC.2.2/LM

The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3/LM

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

FDP_ETC.2.4/LM

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

1. *transaction logs:*
    a. *transaction number of the ERS transaction and identifying the log messages which belongs to the transaction,*
    b. *signature counter of the private signature key used by FDP_DAU.2/TS according to **[PPC-CSP-TS-Au]**, **[PPC-CSP-TS-Au-Cl]**, **[PPC-CSPLight-TS-Au-Cl]**,*
    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 protocolData.*
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 protocolData.*
3. *audit records of the CSP shall be exported unchanged as audit logs to the CTSS interface component.*

PP 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.

Consideration of Application Note 9: This application note does not have any impact on the ST.

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. *clientID as hash value of the public key,*
7. *signature*

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2

The TSF shall use **[BSI-TR-03151]** and **[BSI-TR-03153]** 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.

PP 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.

Consideration of Application Note 10: This application note has been considered

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 of the ERS 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.

PP 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.

Consideration of Application Note 11: The TOE only exists the secure state, if the test suite of **FPT_TST.1** and **FPT_TEE.1** was executed successfully.

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 [ERS Serial Number] and*
2. *CSP identity [PACE PIN, signature counter, and time stamp].*

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** [no additional action]*.

PP Application Note 12: The SMAERS-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 signature counter and time stamps received from CSP to test the CSP. The signature counter shall increase strong monotonically without gaps because any gap may indicate unauthorized signature-creation. The tests of the CSP should allow the CSP to identify the TOE as user of the CSP, cf. **FIA_UID.1.1** clause (2) in **[PP-CSP]**, **[PP-CSP-LIGHT]**. Please refer for further explanations to the user notes and evaluator notes in **[CC2]**, chapter J.12.

Consideration of Application Note 12: The Application Note has been considerd.

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***. **PP 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.

Consideration of Application Note 13: The Application Note has been considered.

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*
    a. *system operation commands as specified in **[BSI-TR-03153]**, Appendix A,*
    b. *authentication failure handling (FIA_AFL.1): the reaching of the threshold for the unsuccessful authentication attempts with claimed Identity of the user,*
    c. *failure with preservation of secure state (FPT_FLS.1): entering and exiting secure state,*
    d. *setting of the version number of the UCP and upgrade of stored data,*
    e. *[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, [*none*].

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

Consideration of Application Note 14: The previous application note has been considered during development. All SystemLogs will be created in ASN.1 format according to **[BSI-TR-03151]**, App E. Additional information required in **[SMAERS-PP]** that is not required by **[BSI-TR-03151]** will be defined in proprietary extensions that will be documented in **[SMAERS-INT]**.

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].*

ST Application Note 13: Please note that FMT_MTD.1.1/SYSAdmin refers to the SMAERS-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 [1]*
2. ***[no actions] if the audit trail exceeds an Administrator settable percentage of storage capacity .***

PP 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).

Consideration of Application Note 15: The developer decided to set the threshold for automatic export in clause 1 to 1. For this reason, the TOE does not provide any automatic export and the assignment in clause 2 has been set to "no actions".

PP 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.

Consideration of Application Note 16: The developer has decided to implement an automatic export after each creation of an audit record.

6.1.6. Code Update Package import

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

Hierarchical to

FDP_ACC.1 Subset access control

Dependencies

FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/UCP

The TSF shall enforce the *update SFP* on

1. subjects: *CSP role*;
2. objects: *stored data*;
3. operations: *upgrade*

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

Hierarchical to

No other components.

Dependencies

FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization

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:

1. [*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].*

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

Consideration of Application Note 17: The previous application note has been considered during development.

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), ~~outside of the TOE~~ **to the storage of the platform.**

FDP_ETC.2.2/UCP_UD

The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3/UCP_UD

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

FDP_ETC.2.4/UCP_UD

The TSF shall enforce the following rules when user data is exported from the TOE: [assignment: *none*]

ST Application Note 14: In conformance with the descriptions in the previous chapters of **[SMAERS-PP]**, the TOE realizes the upgrade of stored information completely during after an update. For this reason, the SFR FDP_ETC.2/UCP_UD is not implemented.

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, ~~outside of the TOE~~ **the storage of the platform.**

FDP_ITC.2.2/UCP_UD

The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/UCP_UD

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

FDP_ITC.2.4/UCP_UD

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

FDP_ITC.2.5/UCP_UD

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*none*].

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:

1. 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.
2. 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.
3. 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.

4. 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

This chapter is equivalent to the corresponding chapter in **[PP-SMAERS]**, because no additional SFRs were introduced in this Security Target, which were not already present in the Protection Profile.

6.3.1. Dependency rationale

This chapter is equivalent to the corresponding chapter in **[PP-SMAERS]** (under consideration of its chapter 7), because no additional SFRs were introduced in this Security Target, which were not already present in the Protection Profile.

6.3.2. Security functional requirements rationale

This chapter is equivalent to the corresponding chapter in **[PP-SMAERS]** (under consideration of its chapter 7), because no additional SFRs were introduced in this Security Target, which were not already present in the Protection Profile.

6.3.3. Security assurance requirements rationale

This chapter is equivalent to the corresponding chapter in **[PP-SMAERS]**.

7. Package Trusted Channel between TOE and CSP

The functional package for a trusted channel support between the TOE and the CSP is used by this Security Target as mandated by **[PP-SMAERS]**. The trusted channel is a specific means to meet the assumption **A.ProtComCSP** Protection of Communication between TOE and CSP. The CSP provides one end point of the trusted channel according to **[PP-CSP-LIGHT]**>>, 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).

This chapter contains the Security Functional Requirements that belong to this functional package. The SFRs for cryptographic mechanisms based on elliptic curves refer to the following table for selection of curves, key sizes and standards.

Table 3. Elliptic curves, key sizes and standards

elliptic curve	key size	standard
brainpoolP256r1	256 bits	**[RFC5639]**, **[BSI-TR-03111]**, section 4.1.3
brainpoolP384r1	384 bits	**[RFC5639]**, **[BSI-TR-03111]**, section 4.1.3
brainpoolP512r1	512 bits	**[RFC5639]**, **[BSI-TR-03111]**, section 4.1.3
Curve P-256	256 bits	**[FIPS_186-4]** B.4 and D.1.2.3
Curve P-384	384 bits	**[FIPS_186-4]** B.4 and D.1.2.4
Curve P-521	521 bits	**[FIPS_186-4]** B.4 and D.1.2.5

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.

7.1. Security Functional Requirements

7.1.1. Trusted Channel between TOE and CSP

FTP_ITC.1/TC Inter-TSF trusted channel

Hierarchical to

No other components.

Dependencies

No dependencies.

FTP_ITC.1.1/TC

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

FTP_ITC.1.2/TC

The TSF shall permit *the TSF* 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*.

PP 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.

Consideration of Application Note 18: Due to the architecture of the TOE, the developer decided to also provide protection against disclosure by the means of 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 trusted channel according to **FTP_ITC.1/TC***,
2. *[none]*
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 the

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

PP 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-CSP-LIGHT]**.

Consideration of Application Note 19: This ST does not contain another method of mutual authentication. The channel between TOE and CSP is secured using PACE as specified in clause (1). For this reason, the author assigned "none" to the open assignment in **FIA_UAU.5.1/TC** (2).

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

Hierarchical to

No other components.

Dependencies

No dependencies.

FIA_API.1.1

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

FCS_CKM.1 Cryptographic key generation – Key agreement for Trusted Channel PACE

Hierarchical to

No other components.

Dependencies

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

FCS_CKM.1.1

The TSF shall generate cryptographic keys ***for FCS_COP.1*** in accordance with a specified cryptographic generation algorithm *PACE with [brainpoolP256r1] and Generic Mapping in PCD role* and specified cryptographic key sizes *256 bits* that meet the following: ***[ICAO-Doc9303]***, *section 4.4*

PP 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.

Consideration of Application Note 20: The application note does not require any action in this ST.

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]
FMT_MSA.2 Secure security attributes]

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *[zeroization]* that meets the following: *[none]*.

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 **refinement: encryption and decryption including** *MAC calculation and MAC verification* in accordance with a specified cryptographic algorithm *according to AES-256 [FIPS-197]* **refinement: in CBC mode with PKCS5 padding according to [NIST800-38A] and [PKCS5]** in [*CMAC (NIST SP800-38B [NIST 2005]))*] and cryptographic key sizes *256 bits* that meet the following: *the referenced standards above according to the chosen selection.*

ST Application Note 15: Please note that the scope of FCS_COP.1 has been extended compared to **[PP-SMAERS]** as the TOE encrypts the PACE channel in addition to the MAC calculation and verification.

The following extended components are defined in **[PP-CSP]**, **[PP-CSP-LIGHT]** 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:

1. [*(DRG.3.1) If initialized with a random seed [based on user input], the internal state of the RNG shall [have [125 bit]].*
2. *(DRG.3.2) The RNG provides forward secrecy.*
3. *(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

1. [*(DRG.3.4) The RNG initialized with a random seed [based on user input] generates output for which [2^19] strings of bit length 128 are mutually different with probability [2^(-10)].*
2. *(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 [**[BSI-TEST-***

SUITE]].

PP 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 **[BSI-TR-03116]** and must therefore be of class DRG.3 or higher according to **[AIS20]**

Consideration of Application Note 21: As the TOE is a pure software TOE is has to rely on its environment to provide real random input as a seed for the random number generator. Due to the various environments and different hardware situations in the environment, the developer decided to obtain the seed by user input. The guidance documentation of the TOE will provide more information to the user on how to provide the seed.

Please refer to **[PP-SMAERS]** for the fulfillment of dependencies.

8. TOE Summary Specification

The TOE is a software library that is meant to be integrated by other components and that is not meant to have any direct user interaction. As such, a summary of its functionality in this chapter is given in form of an abstract overview. The design documentation for the ADV class will provide a more technical view to this functionality.

8.1. Startup and State

The D-TRUST Web-Dienst TSE-SMAERS is a software library that exposes its functionality via a programming interface (API). It does - by design - not run as a service or process. It rather can be used to execute certain functionality. When a function of the D-TRUST Web-Dienst TSE-SMAERS is invoked by another software component, the Java Virtual Machine (JVM) will load the TOE into memory, execute the called function and return the result. The TOE stores information in persistent memory by utilizing a SQLite database or uses java static variables to keep state information in volatile memory amongst function invocations. The latter one is lost as soon as the JVM shuts down the D-TRUST Web-Dienst TSE-SMAERS. Certain state information is stored by design only in volatile memory, e.g. the authentication state of the Administrator, the state of the Trusted Channel connection (PACE session), the last execution of the self test of the TOE and the test of the CSP. This means this state data is reset after startup of the JVM/app, the Administrator needs to log on again (**FIA_UAU.6**), the Trusted Channel needs to be established again and the self tests will run at first function invocation after JVM/app startup. Also, the authentication state of the admin is disregarded after an administrator configurable time (with a maximum of 1 hour) has passed.

The following paragraphs describe the security functionality of the TOE in more detail.

8.2. Self Testing and testing of external entities

The TOE implements self testing and testing functionality as required by [PP-SMAERS] for the following three areas:

Testing the ERS The functionality of the ERS is tested by comparing the clientID that is provided by the ERS to the list of known clientIDs. If the clientID is amongst the list of known clientIDs, the test passes and the status *CTSS_interface* is set to true. Otherwise the status is set to false (which is also its default value). The test is started at the beginning of every function call using the clientID provided as an argument to the function. If no clientID is provided, the test fails (FPT_TEE.1). In accordance with FMT_MOF.1 the TOE provides the administrator with the possibility to query the last result of the test of the ERS and to overwrite the result of the test of the ERS. This is the decision about the features that shall be tested according to FMT_MOF.1. The definition of the identity that is defined in FMT_MOF.1 is realized by the functionality to add and remove clientIDs. As the functionality to add and remove clients is only accessible once the test of the ERS has been succesfully performed, the test knows a special condition: If no client has been registered yet, the test will always succeed.

Testing the CSP The functionality of the CSP is tested by establishing a PACE channel. In addition, if audit records are available, they will be retrieved and a consistency check will be performed with the signature counter and time stamp of the last audit record. If these tests are successful, the status *CSP_role* is set to true. The test of the CSP will be executed at the start of each function of the TOE unless it had already been executed successfully within the last 24 hours since the last start of the JVM/app (FPT_TEE.1). In accordance with FMT_MOF.1 the TOE provides the administrator with the possibility to query the last result of the test of the CSP and to overwrite the result of the test of the CSP. This is the decision about the features that shall be tested according to FMT_MOF.1. The definition of the identity that is defined in FMT_MOF.1 is realized by the functionality to configure the CSP that is used by the TOE.

Self testing During its self test, the TOE will

- execute a basic test of its security functionality,
- verify the integrity of its TSF data and
- verify the integrity of its executables.

If the self test fails, the TOE will enter a secure state. This means that only functions required to restore the state of the TOE (FPT_FLS.1, FPT_TST.1) are accessible. All other functions will return an error. The self test will be executed at the start of each function of the TOE unless it had already been executed successfully within the last 24 hours since the last start of the JVM (in case of the D-TRUST Web-Dienst TSE-SMAERS). In addition, the TOE provides a function that allows to call this self test functionality.

8.3. Authentication

The TOE provides functions for user authentication as outlined by **[BSI-TR-03151]**. By means of the function *AuthenticateUser* the administrator is able to log in and can use the restricted functions afterwards. For this purpose the TOE securely maintains the authentication reference data for the administrator role (i.e. the PIN and PUK) **FIA_ATD.1**. The administrator logs out by means of the function *LogOut*. An authenticated user is also considered logged out after a certain (configurable) period of time of inactivity or a restart of the JVM (**FIA_UAU.6.1**). The authentication for an administrator is offered for the SMAERS-administrator as well as for the TR-administrator. It should be noted however that in the case of the TR-administrator the actual enforcing of the access to certain functions is enforced by the CTSS interface component.

The function *AuthenticateUser* maintains a retry counter and will block the Administrator role if a wrong PIN has been entered 5 times (**FIA_AFL.1**, **FIA_UAU.5**). To unblock a blocked user, the *UnblockUser* function is provided (**FMT_MTD.1/AD**). When the administrator sets a new PIN, the TOE will enforce a policy to make sure that the PIN is secure (**FMT_MTD.3.1/PW**)

8.4. Access Control

The TOE enforces the access control policy as required by **[PP-SMAERS]** in **FDP_ACC.1/LM**. This means that every function of the API that is provided by the TOE requires a set of access rights and these access rights are enforced by each function. The access control policy bases on the states *CTSS_interface*, *CSP_role* and *SMAERS-administrator*.

The TOE will allow access to its functions only for authorised users (based on the currently active states). The only function that is accessible at all times, is the function to start the self test (**FIA_UID.1**, **FIA_UAU.1**). This way, the access control functionality also covers all objects (and subjects) required by FDP_ACF.1/LM, namely Transaction Data, Audit Records, DTBS, protocol data with signature and Log messages. The TOE access control policy also ensures that the functionality to export the DTBS to the CSP light is performed along with the key reference that shall be used by the CSP light to perform the signature (**FDP_ETC.2.1/DTBS**). The access control policy ensure that no role is allowed to modify the transaction number (**FMT_MSA.1**).

8.5. TOE lifecycle and signature key binding

[BSI-TR-03151] requires the Secure Element to be initialized in order to be used for operation. This is realized for the TOE by means of the *initializeLocal* function at the TOE-API; this function (amongst others) controls the key reference for the key that shall be used by the CSP(**FMT_MSA.1**). This key is used by the CSP to sign audit logs as well as transaction and system logs. At this time the TOE is tied to a signature key at the CSP by means of the so-called key reference. For this to work, the signature key

needs to be created at the CSP by means of management operations at the Remote CSP Service before. The binding of an initialized TOE instance to a key reference (referencing the signature key at the CSP) is unchangeable during the lifetime of the TOE instance. In order to decommission the TOE the *disableLocal* function needs to be used. Among others this requests the deletion of the related signing key at the CSP. After this the operational use of the TOE (e.g. transaction operations) and the use of the referenced signature key, is not possible anymore.

8.6. Management

The TOE provides functions for management. As part of these management functions, the SMAERS-administrator can set the maximum lifetime of a transaction as required by **FMT_MOF.1**. As outlined before, these functions will change settings of the TOE that are stored in the local database. The use of some of these functions is restricted.

Client Management The TOE manages a set of ERS clients known to the TOE. An ERS is identified by means of the clientId of the ERS. This is the serial number of the respective ERS. The API of the TOE provides functions for adding and removing clientIds known to the TOE (*addClients* and *removeClients*) (**FMT_SMF.1**, **FMT_MSA.1**). After the initialization of the TOE, no clientId is known to the TOE. When a transaction starts, the *clientId* provided is verified against the list of known clientIds. Therefore, the user (in *CTSS_interface role*) needs to add a *clientId* before a transaction for that client can be started. The maximum number of clients that may be active (added and not removed) on the TOE at a time is 500. The TOE responds with an error at the addClient function if this number will exceed. The TOE is tested and the manufacturer ensures operation for up to this number of active clients.

Other Management Functions The TOE uses the role Administrator (controlled by authentication) as well as the CSP_role and the CTSS_role (**FMT_SMR.1**). The latter two are controlled by the results of tests that are implemented by the TOE. This way, each user is associated with these roles (**FIA_USB.1**)

The TOE provides configuration management by a function named *setConfiguration*. It allows setting and changing at least the following configuration parameters: The PACE-Password (**FIA_ATD.1**) used for the Trusted Channel connection to the CSP, the URL of the Remote CSP Service, the duration of time after the authenticated administrator is automatically logged out when inactive (**FMT_SMF.1**, **FMT_MOF.1**, **FMT_MSA.1**) and the audit events that should be recorded (**FMT_MTD.1/SYSAdmin**). The TOE enforces an overall policy to use restrictive default values for all attributes and does not allow anybody to specify alternative default values (**FMT_MSA.3**).

8.7. Transaction Handling

The TOE offers functionality for transaction handling as its central functionality. Transactions are only accepted from registered ERS (**FDP_ITC.2.5/TD**) To this end the API of the TOE provides functions for start, update and finish a transaction, namely *startTransaction*, *updateTransaction*, *finishTransaction*. These API-functions provide input parameter based on the interface outlined in **[BSI-TR-03151]** (**FDP_ITC.2.5/TD**,**FDP_ITC.2/TSS**, **FDP_ITC.2/TD**, **FPT_TDC.1**). For convenience of the API-user, an externally used transaction identification may be provided in order to associate a transaction to a business identifier (e.g. order number). The TOE retrieves the Audit records from the CSP light and stores them into the local storage under consideration of the rules as given in **FDP_ETC.2.4/LM** (**[FDP_ITC.2/TD)]**, **FDP_ITC.2/TSS**).

Based on the description of the transaction function in **[BSI-TR-03151]**, the API of the TOE provides functions to retrieve log messages for transactions (as a return value for the functions *startTransaction*, *updateTransaction* and *finishTransaction*) and to retrieve AuditLog messages from the CSP-light (*getRemoteLogMessages*). (**FDP_ETC.2/DTBS**, **FDP_ETC.2/LM**)

In order to implement the transaction operations, the TOE securely maintains a transaction counter. This counter is increased when starting a new transaction (**FMT_MSA.1**). Every started transaction is managed by the TOE persistently, as long it is ongoing, until it is finished. In addition, the TOE ensures that the time stamps of log messages build a non decreasing sequence (under consideration of potential adjustments of the time) (**FMT_MSA.2.1**, **FMT_MSA.4**) The maximum number of open transactions (started and not finished) on the TOE at a time is 500. The TOE responds with an error at the startTransaction function if this number will exceed. The TOE is tested and the manufacturer ensures operation for up to this number of open transactions.

The TOE supports the Transaction Update Variant *unsigned* only (see **[BSI-TR-03151]**). This means process data provided at an updateTransaction invocation is accumulated persistently by the TOE for the ongoing transaction. A LogMessage is created at latest at the respective finishTransaction operation or when the amount of accumulated process data exceeds a certain limit for this transaction.

8.8. Cryptographic support

The TOE implements the cryptographic primitives that are required for its operation. This specifically includes

- negotiating a PACE channel with the CSP (**FTP_ITC.1/TC**, **FIA_UAU.5.1/TC**, **FIA_API.1**), the channel bases on PACE with generic mapping with TOE in PCD role, using brainpoolP256r1 in accordance to **[ICAO-Doc9303]**,
- Encryption and decryption for the PACE tunnel (**FCS_CKM.1**, **FCS_COP.1**) including MAC

generation and verification (AES-256, CBC mode with PKCS5 padding according to **[FIPS_197]**, **[PKCS5]** and CMAC **[NIST800-38B]**),

- provision of random numbers based on a SHA-256 generator as defined in chapter 10.1.1 of **[NIST800-90A]** (**FCS_RNG.1**) to be used while establishing the PACE channel and for key generation.

The TOE will overwrite all cryptographic keys with zeros as soon as they are not longer needed (**FCS_CKM.4**).

8.9. Secure update

It falls into the responsibility of the environment to securely update the TOE (cf. OE.SecUCP). Guidance, on how such an update can be performed is provided in **[SMAERS-INT]**. The TOE stores its current version number in its software binary and also in its database. If an update is performed by the environment, these two version numbers deviate and the TOE realizes (during the self test) that an update has occurred. The TOE will then

1. Update the version information in the database (**FDP_ACC.1/UCP**, **FDP_ACF.1/UCP**) and
2. Update schema information in the database if required (**FDP_ITC.2/UCP_UD**)

These actions are performed as part of the first self test after an update has been performed but only if the test of the CSP has passed (as the CSP role is required).

Please note that the TOE does not require the user to call any function of the TOE before an update is performed. For this reason, **FDP_ETC.2/UCP_UD** is implicitly fulfilled.

The TOE only supports one database and relies on the environment that the previous version of the TOE software binary is securely overwritten. This complies with **FDP_RIP.1.1/UCP**

8.10. Logging

The TOE knows three different types of log message:

1. Transaction logs that are produced with the support of the CSP-Light and that secure the imported transaction data,
2. Audit log entries that are written by the CSP-Light
3. System logs that produced by the TOE itself and signed with the help of the CSP-Light.

The system logs that are produced by the TOE comprise the following audit events (audit records):

1. start-up and shutdown of the audit functions;
2. system operation commands as specified in **[BSI-TR-03153]**, Appendix A,
3. every use of the authentication function (including the claimed identity of the user)
4. failure with preservation of secure state (FPT_FLS.1): entering and exiting secure state,
5. setting of the version number after an upgrade happened

For each system log message the TOE records the Date and time of the event (which is assumed to be the time of the signature), type of event, subject identity (if applicable), and the outcome (success or failure) of the event; This complies with **FAU_GEN.1/SYS**.

The TOE will export each System Log message (caused by an audit event) into the database directly after it has retrieved the signed LogMessage parts from the CSP (**FAU_STG.3/SYS**). No audit records are permanently existing within the TOE, the requirements on FMT_MTD.1/SYSAdmin and FMT_MTD.1/SYSCTSS are implicitly fulfilled. No other interface is provided to access the system logs (FAU_STG.1/SYS)

9. References

9.1. Back-Reference to git

This document version has been built from commit b60454f52d184318cf6cec8b6ce687adf8d910af .

9.2. Bibliography

· [BSI-TEST-SUITE] BSI Test suite, Implementation of test procedure A and test procedure B of AIS 31.
· [BSI-TR-03111] Technische Richtlinie BSI TR-03111, Version 2.10
· [BSI-TR-03116] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben fürProjekte der Bundesregierung Teil 5: Anwendungen der Secure Element API, 27. Januar 2020
· [BSI-TR-03151] Technical Guideline BSI TR-03151 Secure Element API (SE API), TR-03151, Version 1.0.1
· [BSI-TR-03153] Technische Richtlinie BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, TR-03153, Version 1.0.1
· [CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5
· [CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security

Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5

- [CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1
- [CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 Revision 5
- [CSP-FSP] D-TRUST-TSE-WEB - Schnittstellen- und Funktionsspezifikation CSP-Light-Modul, Version 1.5.0
- [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)
- [FIPS_186-4] Digital Signature Standard (DSS), FIPS 186-4, July 2013
- [FIPS_197] ADVANCED ENCRYPTION STANDARD (AES), FIPS 197, November 26, 2001
- [ICAO-Doc9303] Machine Readable Travel Documents , ICAO, Doc 9303,Part 11: Security Mechanisms for MRTDSs, Seventh Edition 2015
- [ISMS-Zert-CSP] ISMS Zertifikat für den Betrieb des CSP light
- [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
- [KassenSichV] Verordnung zur Bestimmung der technischen Anforderungen an elektronische Aufzeichnungs- und Sicherungssysteme im Geschäftsverkehr (Kassensicherungsverordnung - KassenSichV
- [NIST800-38A] Recommendation for Block Cipher Modes of Operation: Methods and Techniques, December 2001
- [NIST800-38B] Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication, May 2005
- [NIST800-90A] The NIST SP 800-90A Deterministic Random Bit Generator Validation System (DRBGVS), October 29, 2015
- [PKCS5] PKCS #5: Password-Based Cryptography Specification Version 2.0https://tools.ietf.org/html/rfc2898
- [PKI-Konzept] PKI Konzept für Betrieb des CSP light
- [PP-CSP-LIGHT] Common Criteria Protection Profile Cryptographic Service Provider Light, BSI-CC-PP-0111-2019, 12.11.2019

· [PP-CSP] Common Criteria Protection Profile, Cryptographic Service Provider, Version 0.9.8
· [PP-SMAERS] Common Criteria Protection, Profile Security Module Application for Electronic Record-keeping Systems (SMAERS), Version 1.0, BSI-CC-PP-0105-V2-2020
· [PPC-CSP-TS-Au-Cl] Common Criteria Protection Profile Configuration Cryptographic Service Provider Time Stamp Service and Audit - Clustering, BSI-CC-PP-0108-201, Version 0.9.4
· [PPC-CSP-TS-Au] Common Criteria Protection Profile Configuration, Cryptographic Service Provider - Time Stamp Service and Audit, BSI-CC-PP-0107-2019 Version 0.9.5
· [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
· [RFC5639] Elliptic Curve Cryptography (ECC) Brainpool Standard, Curves and Curve Generation, March 2010, **https://tools.ietf.org/html/rfc5639**
· [SMAERS-API] SMAERS API Schnittstellenspezifikation, SHA-256 hash: 8501b8e9011d2f4acce7efbbcb17ab71cf2d59865d331a892d85068caf45ff74
· [SMAERS-INT] D-TRUST Web-Dienst TSE-SMAERS (für TSE-Web und DF Fiskal Cloud Connect) - API Dokumentation und Integratorhandbuch, Version 1.7.8
· [SMAERS-UMGEBUNG-ANDROID] LEITLINIE ZUM SCHUTZ VON SMAERS DURCH DIE UMGEBUNG - DF FISKAL CLOUD CONNECT , Version 1.6, 17.06.2021
· [SMAERS-UMGEBUNG-CLOUD] LEITLINIE ZUM SCHUTZ VON SMAERS DURCH DIE UMGEBUNG - CLOUD , Version 1.5, 22.09.2021
· [SMAERS-UMGEBUNG] D-TRUST-TSE-WEB SCHUTZ DURCH DIE UMGEBUNG, Version 6.9, 19.08.2021
· [SMAERS-update-concept] Update Konzept für SMAERS