Federal Office
for Information Security

# Supporting Document for Common Criteria Protection Profile SMAERS

Version 1.0

*Table 1: Document History*

| Document Version | Date | Changes / Status |
|---|---|---|
| 0.33 | 2022-08-03 | 1st public draft |
| 0.42 | 2022-11-02 | 2nd public draft |
| 0.50 | 2023-01-06 | 3rd public draft |
| 0.60 | 2023-04-18 | RC1 |
| 1.0 | 2023-05-16 | Release as V1.0 |

# Table of Contents

# 1 Introduction

This document provides guidelines on how to evaluate a TOE according to [PP SMAERS]. In this document, the term “evaluator” always refers to the CC evaluator of SMAERS, otherwise stated differently.

The protection profile [PP SMAERS] defines several requirements:

- security objectives for the environment, in particular for the underlying hardware and software *platform* on which SMAERS is executed
- requirements w.r.t. to the CSP used in combination with SMAERS

Moreover, [PP SMAERS] allows some flexibility w.r.t. the life cycle of the TOE, how updates are handled, delivered and installed, and how trust provisioning is handled during the life cycle of the TOE. All these imply additional requirements. These requirements are defined and clarified in this supporting document.

A TOE that is not operated adhering to these requirements is not operated as certified, and in such a case, the taxpayer is not meeting the legal requirements. Therefore, the manufacturer must provide additional documentation as listed in Chapter "Security Module Life Cycle Documentation" that describes how the TOE must be operated in order to meet all requirements. Adherence to this documentation is mandatory for all parties concerned. Furthermore, configuration documentation for the integrator (cf. chapter 2.3) must be provided that enables the integrator to set up and configure a certified Technical Security System (TSS) such that it operates as certified. The integrator must confirm in writing that he obliged to all these configuration documents and must provide this document to the taxpayer. This written statement shall be used to aid in demonstration of certified operation of the TSS, c.f. chapter 4.

This additional documentation listed in the previous paragraph must be evaluated such that the TOE - that is accordingly set up, configured and operated – fulfills the requirements of the certification. The implementation of this setup, configuration and operation in the field is ensured by the confirmation of the integrator. The focus of the evaluation is to verify the documentation and to make sure it meets all the requirements for content and presentation of evidence. If reasonable doubt exists concerning the presentation of evidence, the ITSEF may request technical evidence to verify that the document truthfully represents the factual implementation.

This supporting document and the additional life cycle documentation are part of SMAERS requirements and SMAERS evaluation, respectively. However, the requirements given in this document extensively involve the configuration and operation of CSP, which is likely implemented by a third party. The SMAERS manufacturer is responsible to provide detailed information and evidence regarding the CSP where needed, possibly referencing guidance documentation from the Common Criteria evaluation of the CSP on request.

All activities that the evaluator must execute are marked explicitly as "Evaluation Activity" throughout this document. Keywords according to [RFC2119] are to be interpreted as such within the Evaluation Activities.

The evaluation activities defined in this document largely rely on technical and conceptual documentation as evaluation deliverables. However, some evaluation activities additionally require test samples and/or the source code of SMAERS as mandatory evaluation evidence and thus must be provided by the manufacturer.

Further, some evaluation activities require the source code as evaluation evidence ‘at the discretion of the evaluator’. This means: For these evaluation activities the source code, parts of the source code or the implementation representation of SMAERS has to be provided by the manufacturer in case the evaluator decides that he needs the source code to conduct the evaluation activity. Source code does not have to be provided if the evaluator decides that he can perform the evaluation activity without examining the source code. Details on the required evaluation evidence is presented as part of each evaluation activity itself and in the introductory part of its respective chapter in this document.

# 2 TSS as a Composed IT-Product

The purpose of the TSS is to provide cryptographically signed electronic records of financial transactions to prevent tax fraud. Therefore, a TSS must be used by electronic record-keeping systems (ERS), e.g. cash registers of the taxpayer, to send transaction data to and receive transaction log messages, c.f. [AO][KSV] [TR TSEA].

The TSS is composed[1] of the security module and further components, e.g. storage and TSS interface. A TSS has to be certified according to [TR TSEA] in order to prove conformance of the product. This document focuses on the Security Module Application for Electronic Record-Keeping Systems (SMAERS) which itself is part of the security module. It also focuses on the interaction of SMAERS with other components of the security module and the life cycle and required configuration of these components. Concerned in particular are the life cycle and configuration of the Cryptographic Service Provider (CSP). This includes pairing SMAERS with a generic CSP. Here, both CSP and SMAERS can be certified independently from each other, in the sense that no composite certification is required, c.f. [PP SMAERS].

Unless explicitly stated otherwise, the term *CSP* in the context of this document refers to CSP devices according to [PP CSP] and CSPL devices according to [PP CSPLight]. Moreover, CSP or CSPL *clusters* are also referred to as *CSP* or a *CSP device* unless noted otherwise.

## 2.1 TSS Architecture

In addition to the chosen security module architecture, i.e. platform architecture or client-server architecture (cf. [PP SMAERS]), the architecture and type of the TSS as a whole is a distinguishing factor when evaluating the life cycle of the composed product. The evaluator should note that the life cycle varies depending on the chosen TSS implementation. On a high level of abstraction, two different kind of basic architectures and life cycles exist:

- *ready-to-use* TSS devices. These feature a finalized security module, i.e. SMAERS and CSP components that are personalized, initialized and fully operational at the time of distribution by the TSS manufacturer. This is typically found for ‘tokenized’ TSS devices that physically enclose a security module or chip as CSP and further components forming the TSS device. SMAERS is implemented either on the CSP platform or on a different microcontroller. As all personalization activities are performed during the manufacturing process, potentially in a CC-audited environment, some life cycle requirements might be intrinsically fulfilled.
- *integration-ready* TSS devices. These are most commonly physically separated into SMAERS and CSP components, whose security module needs to be personalized and provisioned with critical assets in the operational environment of the ERS. This scenario is typically found for ‘cloud’ TSS solutions, where CSP is located in a securely operated data center and SMAERS (software) is running on a platform in the operational environment of the ERS.

## 2.2 Security Module Life Cycle

In general, both the CSP and SMAERS component of a TSS security module have separate (but related) life cycles. They are desynchronized but consecutive, i.e. during the interaction of SMAERS and CSP, the CSP is assumed to be in its life cycle phase "operational". Furthermore, SMAERS expects CSP to be properly configured to serve as the cryptographic core of a TSS device, e.g. considering its audit configuration and availability of a key for timestamped signature creation. The evaluator has to verify that the personalization and initialization activities for the CSP are suitable and conform to the requirements given in this document. The requirements are detailed in the following chapters.

[1]The term “composed” used in this document has no relation to CC part3, chapter 9. It is here merely used to describe an IT product that is constructed of several components.

During personalization and initialization, SMAERS has to be provisioned with confidential passwords or keys to allow for the authentication of SMAERS administrator(s) and mutual authentication with CSP. The latter applies for client-server architecture only. The security module is considered operational once the personalization of SMAERS is finalized and its connection to CSP is established. It is further recommended to utilize CSP remote attestation to assure that SMAERS is connected to a genuine and compatible CSP. Only an initialized and personalized security module is allowed to interact with the TSS interface, in turn allowing for the initialization of the TSS itself, i.e. configuration of the TSS administrator credentials and clientIDs of ERS to be connected.

Both SMAERS and CSP provide functionality to update their respective implementation via Update Code Packages (UCP). It is assumed, that the successful deployment of a UCP does not interfere with the life cycle state of the security module, i.e. the security module remains in its operational phase. However, this assumption does not hold true for the updated component itself, as a successful update terminates the life cycle of the old component and initializes a new component with inherited assets.

Although the specifics of a future UCP are unknown at the time of evaluation, especially regarding its certification status, life cycle requirements and ramifications, the life cycle documentation shall include plans to handle a future UCP. This includes details about its creation, distribution and enforcement. In particular, the following two items should be considered: a) The documentation concerning the UCPs is created by the manufacturer and examined by the evaluator and b) The life cycle describes the transition “certified product” -> “UCP” -> “certified product” and is examined by the evaluator. If the TOE itself is or might be the result of a successfully deployed UCP, life cycle documentation of the new TOE must provide a detailed analysis of the impact of the UCP on the life cycle and certification status of the former product.

## 2.3 Roles and Attack Scenarios

In the scope of the TSS life cycle, five notable (groups of) roles are typically found that are relevant for security evaluation purposes:

- The *TSS Manufacturer*, which includes manufacturers of the security module and its components. Those are assumed to be trustworthy and acting in good faith. However, as the scope of the SMAERS and CSPL certification (EAL2+) does not mandate a security site audit the life cycle documentation must include a description of the development process and handling of sensitive assets by the TSS manufacturer.
- *Trust Service Provider*, e.g. PKI service provider and data centers hosting CSPL devices. This group plays an integral part in the operation of TSS components or supporting systems and is assumed trustworthy and acting in good faith. The evaluator has to check if the CSPL operation is certified, cf. Appendix [PP SMAERS].
- The *Integrator* of the security module of the TSS, especially SMAERS. The TSS manufacturer may use third parties to integrate, personalize and initialize the security module of the TSS. As the integrator is expected to handle sensitive assets, e.g. PACE[2] key and SMAERS administrator credentials, this role must be assumed trustworthy and acting in good faith. It is strongly recommended to prefer tools and implement technical solutions over organizational means to limit the integrators necessary access to sensitive assets. It is the manufacturer’s responsibility to appoint only trustworthy and skilled parties and personnel as integrators.
- *ERS Manufacturer*, ERS provider and related services providers, acting as TSS-integrator. These parties must not be part of the personalization or initialization of the security module or get access to its sensitive assets. They typically act as the integrator of the TSS itself and may initialize the TSS on behalf of the taxpayer.

[2] Password Authenticated Connection Establishment, cf. glossary in chapter 12.

- The *taxpayer*, including associated parties, as the primary threat agents. The taxpayer must not gain access to sensitive assets and the personalization and initialization process must not assume a taxpayer acting in good faith. Secure personalization, initialization and operation must not rely on the assistance of the taxpayer beyond providing access to the operational environment and systems therein, as required.

SMAERS has to be operated in the same operational environment as the ERS. Thus, it has to be assumed that the attacker has unrestricted physical access to the TOE or its platform. The personalization and initialization process must be sufficiently secured by organizational or preferably technical means under these circumstances. The evaluator must consider the scenario of the attacker having physical access to the TOE as the default one when conducting the evaluation activities.

Note: If the ERS itself is operated in an environment that plausibly denies the attacker access to SMAERS or its platform, e.g. if ERS and SMAERS are hosted in an audited environment implementing secure client separation, the assumption of unrestricted access as well as certain attack scenarios might be voided with corresponding evidence; in particular cf. chapter 8 " Secure Platform Concept (Umgebungsschutzkonzept)".

# 3 Evaluation Activities for SARs

The sections below specify Evaluation Activities (EAs) in *addition* to the work units of the Security Assurance Requirements (SARs) included in the [PP SMAERS]. For all SFRs and SARs that are included resp. referenced in [PP SMAERS], the evaluator is expected to perform the CEM work units associated with the EAL2 SFRs and SARs augmented with ALC_LCD.1, ALC_CMS.3 (refined) as defined in the [PP SMAERS].

The terms used to describe the EAs, are used as defined in [CEM]:

**check** – generate a **verdict** by a simple comparison. Evaluator expertise is not required.

The statement that uses this verb describes what is mapped.

**examine** - generate a **verdict** by analysis using evaluator expertise.

The statement that uses this verb identifies what is analyzed and the properties for which it is analyzed.

# 4 Security Module Life Cycle Documentation

The TOE manufacturer must provide documentation describing the complete life cycle of the TSS including details necessary for the understanding of the interaction with and configuration of the CSP, cf. [PP SMAERS].The life cycle within the [PP SMAERS] has been deliberately left open as it differs depending on the implementation. However, for the concrete product evaluation, the life cycle must be specified. Therefore, the following documentation is in addition to the documentation already required within the EAL2+ evaluation.

The [PP SMAERS] requires concepts as a result of the description in [PP SMAERS] chapter 1.2 "TOE Overview". These are the following:

- A documentation of the provisioning of the CSP within the life cycle of the TSS 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.

  The documentation is in the following referred to as *"CSP Configuration and Operation Concept"* (cf. chapter 5 "CSP Configuration and Operation Concept (CSP-Konfigurationskonzept)") and covers the objectives for the operational environment “OE.CSP” and “OE.SecCommCSP (partially)”.

- For the objectives for the operational environment "OE.SUCP" and "OE.SecUCP" [PP SMAERS] a documentation of the update procedure to allow for recovery from security incidents including the procedures for creating, distributing, and enforcing installation of Update Code Packages as detailed out in chapter 6.

  This documentation is in the following referred to as *"Update Concept"*, cf. chapter 6.

- A documentation of the personalization of assets of the TOE and its initialization.

  The documentation is in the following referred to as *"Trust Provisioning Concept"* (cf. chapter 7 "SMAERS Trust Provisioning Concept (Trust-Provisioning-Konzept)") and covers the objectives for the operational environment “OE.SecOEnv (regarding administration)” and “OE.SecCommCSP (partially)”.

- A documentation of the underlying public key infrastructure (PKI) and the audit reports of the involved trust centers to ensure the verifiability of generated signatures by third parties.

  The documentation is in the following referred to as *"PKI Concept"* (cf. chapter 9 "PKI Concept (PKI-Konzept)").

Furthermore, the manufacturer has to provide documentation describing the (security of the) operational environment of SMAERS as a result of the objective for the operational environment "OE.SMAERSPlatform" and “OE.SecOEnv”:

- Describing the platform(s) that the TOE is intended to be executed on, what facilities the platform provides to ensure that the security objectives on the environment are met, and if required, how the platform must be configured in order to meet these requirements.

  The documentation is in the following referred to as *"Secure Platform Concept"* (cf. chapter 8 "Secure Platform Concept (Umgebungsschutzkonzept)".

The concepts must be evaluated during the SMAERS CC-certification procedure and are functional specification documents to be used in further inspections of the certified operational TSS during its complete life cycle. For this chapter the term “documentation” always refers to all additional documents described above.

The additional life cycle documents include mandatory requirements to be implemented or organizationally realized regarding the initialization, personalization and operation of the TSS. The target audience for these requirements are the *manufacturer* and the *integrator*. Note, that the additional life cycle documents must be made available to the BSI and are forwarded to the fiscal authorities [TR TSEA].

The integrator has to confirm in a written statement that the initialization, configuration and personalization of each specific SMAERS and SMAERS Platform was carried out completely as required and the security module of the TSS is set up for operation as certified. This written statement shall be used by the taxpayer to aid in demonstration of certified operation of the TSS. It has to be provided to the taxpayer in 'Schriftform' following the successful integration referencing each affected TSS.

This document (Supporting Document for Common Criteria Protection Profile SMAERS) does not cover aspects regarding actions and entities that do not affect or interact with the security functionality of the security module. This includes:

- The correct usage of the ERS as in the objective for the operational environment "OE.ERS".
- The verification of the log messages as in the objective for the operational environment "OE.Transaction".

Further, the security of the execution environment if SMAERS is operated on the CSP platform (platform architecture) as in the objectives for the operational environment "OE.CSPPlatform" is not in scope of this document.

**Evaluation Activity (EA4.1)**

*The evaluator **shall check** if the additional documentation listed above is provided. The concepts shall be provided each in a self-contained document.*

**Evaluation Activity (EA4.2)**

*The evaluator **shall examine** the documentation to determine that each document contains a complete list of sensitive assets required for a) technical functionality of the described TSS component and b) organizational measures. In particular, this means*

- *assets needed in addition to those listed in [PP SMAERS] or [PP CSP], respectively, including assets needed for secure life cycle management of the TSS security module*
- *as well as assets w.r.t. the objectives of the operational environment.*

**Evaluation Activity (EA4.3)**

*The evaluator **shall examine** the documentation to determine that each document lists all involved parties and their roles, as well as their tasks, requirements and obligations. The evaluator **shall examine** the documentation to determine if the respective rights and roles are coherent and offer protection against unauthorized access to all assets identified in the Evaluation Activity above.*

**Evaluation Activity (EA4.4)**

*The evaluator **shall examine** the documentation to determine that all documentation together include guidance on how the correctness of personalization, initialization and operation of the security module of the TSS is ensured. The audience of this documentation is the integrator.*

**Evaluation Activity (EA4.5)**

*The evaluator **shall check** that the written statement explicitly states that the integrator must confirm in writing towards the taxpayer and fiscal authorities that all configuration and setup instructions that are required to operate the TSS as certified are implemented. The written statement does not have to be signed at the moment of evaluation. It must not be altered after the evaluation is completed, excluding information to be added later to identify the TSS and/or taxpayer. The documentation shall state that a partial implementation of the configuration and setup instructions is not admissible.*

**Evaluation Activity (EA4.6)**

*The evaluator **shall check** that the development process and the assets for the development of SMAERS as a secure IT-product are described. The evaluator **shall examine** the documentation to determine that the description is consistent with the security problem definition, the assumptions and the security objective of the environment of [PP SMAERS].*

# 5 CSP Configuration and Operation Concept (CSP-Konfigurationskonzept)

The CSP is a generic cryptographic core component designed to support a wide set of applications. As such, a CSP used for a specific application has to be configured (and operated) consistent with the security requirements of the specific application. The required configuration for the SMAERS application(s) using the CSP as part of the TSS security module is given in [PP SMAERS], partially detailed and expanded regarding life cycle considerations in the following sub chapters. The CSP Configuration and Operation Concept provided by the manufacturer has to cover all of the requirements listed below, giving evidence for non-applicability where needed.

A CSP in general is multi-applicative, i.e. could potentially serve SMAERS and non-SMAERS applications at the same time. For TSS devices however, one CSP must exclusively be used by SMAERS applications, i.e. no other types of security module applications are allowed.

For this chapter the term “concept” always refers to the “CSP Configuration and Operation Concept”.

For the evaluation activities regarding this concept the term ‘*documentation*’ includes

- the CSP Configuration and Operation Concept,
- the development and guidance documentation of SMAERS,
- the provided guidance documentation of the CSP,
- and, at the discretion of the evaluator, the source code of SMAERS.

This *documentation* shall be used as the input of the evaluation activities, if not noted otherwise.

Evaluation activities requiring a ‘CSP test sample’ shall be carried out either using a physical sample of the CSP or a test setup provided by the CSP manufacturer. In either case, the evaluator must have full control over the sample or setup. Deviations in configuration or functionality of the test sample or setup from those used in the certified TSS must be documented and the evaluator must assess if those deviations still allow finding a verdict regarding the evaluation activity.

**Evaluation Activity (EA5.1)**

*The evaluator **shall examine** the documentation to determine, that CSP must not be used for non-SMAERS applications. For this purpose, the evaluator **shall examine** the documentation to determine whether the SMAERS manufacturer meets the requirements via organizational or technical measures. The evaluator **shall examine** on a documentary basis that the process described is suitable.*

## 5.1 Scope of Evaluation

Security relevant services, methods and functionality of the CSP that are used in the context of the TSS must be certified, i.e. they must be part of the corresponding CC evaluation of the CSP or part of an extended evaluation of the CSP and its operational environment, e.g. those in chapter 10. This requirement holds for all kinds of security relevant services, methods and functionality that are either directly used by the SMAERS TOE or used by other components or parties during the complete life cycle of the TSS.

For CSP devices certified according to [PP CSP] (EAL 4+) it is assumed that this requirement is fulfilled either due to the CSP platform, e.g. certified card management services allowing for secure installation, personalization, initialization and update, or due to evaluation activities during CSP evaluation. CSPs certified according to [PP CSPLight] (EAL 2+, software) typically exclude life cycle management and associated tooling from within the TOE boundaries. These parts are required to be evaluated in the scope of this supporting document, i.e. as part of the evaluation of the CSP Configuration and Operation Concept and/or the associated ISO/IEC 27001 audit, see chapter 10.

**Evaluation Activity (EA5.2)**

*The evaluator **shall examine** the implementation of the TOE to determine, that the listed CSP services, methods and functionality are correctly used. Therefore, at the discretion of the evaluator, the SMAERS Manufacturer has to provide the interface description of the CSP as well as the implementation representation of SMAERS (cf. Refinement ALC_CMS.3.1C).*

**Evaluation Activity (EA5.3)**

*The evaluator **shall examine** the CSP test sample to determine whether the CSP configuration is applied as specified in the documentation or deviates in configuration or functionality from those used in the documentation. The evaluator **shall examine** the CSP test sample documentation to determine that those deviations are completely described and still allow finding a verdict regarding the applicability of the configuration for evaluation purposes.*

**Evaluation Activity (EA5.4)**

*If a CSP certified according to [PP CSPLight] is used as the CSP component, the evaluator **shall check** that the CSP Configuration and Operation Concept claims conformance to the 'Operation Requirements of CSPLight' outlined in chapter 10 and instructs the integrator of the security module to operate the CSP in accordance to this claim.*

Note: This evaluation activity only covers the presence of the conformance claim in the provided documentation. It does not cover the actual evaluation of conformity during operation of the TSS and its security module.

## 5.2 Life Cycle Alignment

In order to be paired with a SMAERS instance, the CSP has to be in its life cycle phase "operational". Thus, the CSP must be initialized and personalized concerning its global configuration and non-SMAERS instance specific assets. This must be done before the CSP is configured for one or more SMAERS instances.

Regarding the assets specific to each SMAERS instance presented in chapter 5.3, two options exist:

- The CSP may be pre-configured and pre-personalized for one or more SMAERS instances that are expected to be coupled (batch configuration and personalization), or
- the CSP is configured and personalized for a single SMAERS instance on request during SMAERS initialization and personalization.

Note: CSP devices that are used with a single fixed SMAERS instance over the full life time of the TSS device, e.g. as a component in a TSS hardware token, might be initialized and personalized within the same production step as SMAERS. The sequence of actions in this production step should still allow for a life cycle alignment as described above. If it is not feasible to carry out the initialization and personalization in this sequence, the manufacturer has to provide extensive evidence that the deviating sequence of actions leads to a secure composed product and thereby opened attack surfaces are effectively mitigated.

In the case of an update of the CSP by execution of an UCP, SMAERS instances are only allowed a connection to the CSP in its life cycle phase “operational”. I.e. the CSP has to terminate connections to SMAERS instances, leave the life cycle state “operational”, execute the update and perform steps required for the retransition to the life cycle state “operational”. Subsequently, SMAERS instances are again allowed to (re)connect to the CSP.

**Evaluation Activity (EA5.5)**

*The evaluator **shall examine** the documentation to determine that CSP and the SMAERS instances are coupled in a secure way and in the correct order according to the two options of the description in ch. 5.2.*

## 5.3 SMAERS and TSS-Specific Assets

The term ‘asset’ within this chapter refers to an asset of the CSP.

**Evaluation Activity (EA5.6)**

*The evaluator **shall examine** the documentation to determine that for each SMAERS instance connecting to and using the CSP, the CSP assets 'signing key' and 'PACE key' (if present) are configured individually, specifically no default passwords, no group keys etc. are used for these assets. The evaluator **shall examine** the documentation to determine that, according to CSP configuration, no two different SMAERS instances use the same assets 'signing key' and 'PACE key'.*

**Evaluation Activity (EA5.7)**

*The evaluator **shall examine** the documentation to determine that it describes the actions prepared and executed to configure the CSP for the connection of a new SMAERS instance listing each action carried out, as well as who and in which role these actions are conducted.*

### 5.3.1 Signing Key

Signature creation and verification in the context of the TSS is accomplished by using an asymmetric ECC key pair, see [PP SMAERS][TR TSEA][TR CRYPTO].

**Evaluation Activity (EA5.8)**

*The evaluator **shall check** that the concept assigns the correct usage type of the signing key as ‘signature creation with timestamp and usage counter’, c.f. [PP-CSP].*

**Evaluation Activity (EA5.9)**

*The evaluator **shall examine** the documentation to determine that the signing key pair is created, i.e. configured and generated, on the CSP device itself. As the CSP prohibits key export and import for private key objects with an attached usage counter, this assures that the private key is only ever present on the CSP itself. The export and import of those keys to perform key migration or synchronization to other CSP devices of the same CSP cluster is not restricted.*

**Evaluation Activity (EA5.10)**

*The evaluator **shall examine** the documentation to determine that the usage of the signing key reference[3] prior to key generation is not possible.*

**Evaluation Activity (EA5.11)**

*The evaluator **shall examine** the documentation to determine that it is not allowed to renew or exchange the signing key material during the life cycle of the TSS.*

**Evaluation Activity (EA5.12)**

*The evaluator **shall examine** the documentation to determine that the signing key material can only be destroyed a) on request of an entity acting as CSP-Administrator or CSP-Crypto-Officer or b) if the TSS is terminated due to the explicit termination command given by the TSS administrator channeled through SMAERS.*

**Evaluation Activity (EA5.13)**

*The evaluator **shall examine** the documentation to determine that the signing key reference is connected to exactly one PACE key reference for the complete life cycle of the TSS.*

Note: As the first usage of the private key is to self-sign the public key or key certificate as a proof of possession, the signature counter in the operational phase of SMAERS does not necessarily start with the

[3] See the glossary in chapter 12 for a definition of a key reference.

initialized value. All usages of the signing key prior to regular usage, i.e. signing of log messages subsequently exported to the SMAERS component, as well as the expected starting value have to be documented in the CSP Configuration and Operation Concept document and in public guidance documentation. Further requirements and clarifications regarding the counting method and the expected starting value are specified in [TR TSEA].

### 5.3.2 PACE Key

The PACE key is a symmetric key or passphrase that is shared between the CSP and SMAERS instances in order to connect them to form the security module of a TSS instance. It is used for mutual authentication of SMAERS instances and the CSP during the establishment of a secure channel between both components using the PACE protocol, c.f. [TR ID-PROT]. The requirement of a trusted channel and hence the existence of a PACE key is only given if the security module utilizes the client-server architecture.

If a symmetric key is used as the PACE key, it is assumed that the key is used 'as is' in the PACE protocol, i.e. no further key derivation may be performed by the PACE implementation and the PACE key equals the derived PACE key. Further, if a passphrase is used as the PACE key, the derived AES key may directly be stored and used by the CSP or SMAERS component and its PACE implementation.

The derived PACE key is required to completely utilize the implementation specific AES key length, i.e. 128 bit, 192 bit or 256 bit, with random bits. The key can be generated by the CSP and exported to provision SMAERS, or generated externally and imported into the CSP and SMAERS.

**Evaluation Activity (EA5.14)**

*The evaluator **shall examine** the documentation to determine that it describes how the PACE key is generated and how it is ensured that the PACE key complies to the requirements regarding key generation.*

**Evaluation Activity (EA5.15)**

*The evaluator **shall examine** the documentation to determine how to prevent the usage of the PACE key reference prior to key generation or import, to prohibit authentication using uninitialized key material.*

**Evaluation Activity (EA5.16)**

*The evaluator **shall examine** the documentation to determine that the PACE key material cannot be renewed or exchanged during the life cycle of the TSS.*

**Evaluation Activity (EA5.17)**

*The evaluator **shall examine** the documentation to determine that each security module uses an individual PACE key.*

**Evaluation Activity (EA5.18)**

*The evaluator **shall examine** the documentation to determine that the PACE key reference is indivisibly connected to exactly one signing key reference.*

**Evaluation Activity (EA5.19)**

*The PACE key is sensitive key material. The evaluator **shall examine** the documentation to determine that the described personalization and distribution involves only trusted parties and suitable procedures so the key remains confidential.*

**Evaluation Activity (EA5.20)**

*The evaluator **shall examine** the documentation to determine that once the PACE key is provisioned to both the CSP and SMAERS instance, all further occurrences of the key are deleted.*

**Evaluation Activity (EA5.21)**

*The evaluator **shall examine** the documentation to determine that the trusted channel protects as a minimum the integrity and confidentiality of the communication, i.e. the trusted channel utilizes message authentication as well as encryption.*

## 5.4 Global Assets

The CSP maintains and uses specific assets for its own security functionality that are also partially independent from the intended usage as the TSS security module cryptographic core component.

### 5.4.1 Attestation Key

The CSP attestation mechanism is used as a means to give evidence about the genuineness of the CSP itself, i.e. to authenticate the certified CSP to external parties. It is not used to identify or authenticate the user or operator of the CSP. Thus, the attestation key is technically and organizationally coupled to the type and version of the certified CSP implementation or appliance, or batches thereof, sharing the same key. For clusters of CSPs the batch size may be one, i.e. each CSP cluster may utilize its own individual attestation key.

The attestation key used in the context of the TSS is an asymmetric key pair, see [PP CSP]. CSP clusters that utilize their own individual authentication key generate their own key material. Otherwise, the key material is generated externally and provisioned to the CSP.

The attestation private key is sensitive key material and remains confidential. Handling of the private key is restricted to a small number of selected persons of the CSP manufacturer and must be thoroughly described in the CSP Configuration and Operation Concept. Handling means active or passive action of the key, starting from generation, storage, transport up to provisioning.

**Evaluation Activity (EA5.22)**

*The evaluator **shall examine** the documentation to determine if in the TSS context, the attestation mechanism of the CSP is used during the initialization and personalization of SMAERS on first connection, and after each successful installation of an Update Code Package for SMAERS. If remote attestation is used, the attestation has to ensure a cryptographically secure CSP authentication, e.g. by utilizing a challenge-response procedure with a random challenge, i.e. the CSP attestates towards SMAERS that the CSP is genuine. In the case of the client-server architecture, the attestation after installation or update must be conducted within the secure channel.*

**Evaluation Activity (EA5.23)**

*The attestation private key is sensitive key material. The evaluator **shall examine** the documentation to determine that the generation, personalization, distribution and storage for later use involve only trusted parties and suitable procedures so the key remains confidential.*

### 5.4.2 Time

CSP implements a time source [PP CSP], where the correctness of the time asset depends on an external entity.

As a correct time can only be known to and present in the CSP after setting or requesting the time or time offset from an external entity, there might be a period, e.g. after booting the CSP, where no correct time is known. To identify time stamped signatures created during this time period, the CSP must use a time offset of ‘0’ (zero) per default on start-up. Further, the CSP must enforce the setting of a time offset before regular operation, c.f. [TR TSEA].

For decentralized CSP appliances, e.g. utilized in tokenized TSS, the provided external time offset is assumed to be correct, although the entity providing the time offset might not be trustworthy. Detection of manipulated time offsets is technically not feasible for those devices and out of scope. For those devices,

only the correctness of the elapsed time since a known reference, e.g. time since boot or the time since the last update, remains as the relevant value of the asset time. Regulations about this correctness, e.g. allowed time drift or deviation between measured and real time, is given in [TR TSEA].

Centralized CSP devices or CSP devices maintaining more than one signature key, i.e. CSP devices being utilized by more than one SMAERS instance, must use a trustworthy time source, e.g. authenticated NTP. The time must not be adjustable by any of the connected SMAERS instances.

**Evaluation Activity (EA5.24)**

*In case of centralized CSP devices or CSP devices maintaining more than one signature key, the evaluator **shall examine** the documentation to determine that:*

- *the time is not adjustable by a connected SMAERS application instance,*
- *the role time admin is adopted by a trusted entity and*
- *the CSP and its platform is configured to use a trustworthy time source.*

### 5.4.3 Role Model and Administrative Access

PP-CSP defines administrative roles, i.e. roles with enhanced administrative rights regarding certain aspects of the CSP that might be divided further into more detailed variants of the base roles.

CSPs that are part of *ready-to-use* TSS devices, i.e. decentralized devices that utilize a local CSP component, must technically restrict the possibility for administration of the CSP. Rights only needed during initial personalization and initialization of the CSP must not be accessible afterwards, i.e. corresponding roles must be deactivated, their rights revoked and/or credentials randomized or securely deleted. However, the right to set time in a role derived from *timekeeper* as well as the possibility to trigger updates in a role derived from ‘update agent’ must be obtainable by the taxpayer either directly or indirectly channeled through the TSS-interface and SMAERS component.

Centralized CSP appliances must be administrated from within the operational environment of the CSP, i.e. the data center hosting the CSP appliance, or via a secured connection according to the documented guidelines and security concepts of the data center. Administrative access must be limited to trustworthy personnel of the CSP manufacturer or trust service provider. Secure CSP administration must be part of the ISO/IEC security audit of the data center, see Appendix [PP SMAERS].

**Evaluation Activity (EA5.25)**

*The evaluator **shall check** that the concept describes for each implemented CSP role:*

- *what rights are associated with this role*
- *how is this role authenticated, e.g. authentication by password or other means of authentication*
- *which entity is taking this role*
- *what is this role used for, i.e. the purpose of this role during the life cycle*
- *when is this role taken and used, i.e. in which life cycle state*
- *the status of the corresponding authentication credentials in each life cycle state*

*The evaluator **shall examine** the documentation to determine that the implemented role model ensures that no role has more rights than the minimum required for operation. The trustworthiness of the five typically found roles (cf. Chapter "TSS as a Composed IT-Product") must be taken into account, and the role model should be as restrictive as possible concerning the trustworthiness of these roles. In particular, the taxpayer must not be granted administrative access to CSP. Further, SMAERS must only be able to obtain the right to retrieve signed*

*audit log messages of the CSP TSF in a restricted role derived from auditor without access or the ability to alter the CSP TSF audit log configuration.*

## 5.5 Audit Events and Logging

The CSP TSF audit functionality logs security critical events as audit events. These events must be exported as audit log messages, see [PP CSP][PP SMAERS][TR TSEA] for requirements regarding formatting, structure, content, export and storage. [PP CSP] lists all mandatory and the most common optional events to be logged in a generic CSP, however the CSP implementation is free to define additional events as required or deemed useful by the manufacturer. For this reason, the requirements and life cycle considerations regarding the TSS, as given in this chapter, may not be exhaustive.

Unless ruled otherwise in this chapter, all audit events must be exported to all SMAERS instances initialized on the CSP, i.e. each log event must be signed with each initialized signing key that is used in a TSS security module on the CSP. Exceptions to this requirement apply only to centralized CSP devices in data centers for one reason:

- The audit event is of significance only to a single TSS instance. In this case the event must be exported using only the corresponding signing key, thus the log message is only present in the audit trail of the corresponding TSS.

The logging of non-security related events is out of scope. However, the signing keys used in the context of the TSS must not be used for those events.

**Evaluation Activity (EA5.26)**

*The evaluator **shall examine** the documentation to determine that all mandatory, optional and additionally defined audit events of the CSP are exported to all initialized SMAERS instances, exceptions are only allowed for events especially listed in chapter 5.5.1 "Log Messages" below.*

**Evaluation Activity (EA5.27)**

*The evaluator **shall examine** the documentation to determine that only security relevant events are signed and exported utilizing the configured TSS signing key(s).*

### 5.5.1 Audit Log Messages

The CSP configuration concept must contain a list of all generated audit events. For each event, the list must contain a detailed description of the event, its trigger and the logged content. Further, for centralized CSP devices in data centers, the receiver of the corresponding exported log message must be designated, i.e. all SMAERS instances or a single SMAERS instance. The receiver(s) of log messages can be found in the description of the audit events below. One identical audit configuration for all SMAERS instances connected to a specific CSP device or cluster must be applied and audit events shall be created individually for each configured SMAERS instance.

Note: Although the content of audit log messages is not standardized, the content must contain a conclusive and non-confounding identifier /name for each logged audit event.

Note: The list only requires the description of CSP audit events / audit log messages. However, it might be of value to also include SMAERS audit events / system log messages into the same document.

The following audit events are mandatory to log, c.f. FAU_GEN.1.1 in [PPC-CSP-TS-Au][ PPC-CSPLight-TS-Au-Cl]:

- **start-up after power-up** (FAU_GEN.1.1 d) (1)): The event indicating the start of the CSP, i.e. after powering CSP and platform (PP-CSP, EAL4+) or after starting of the CSP software (PP-CSPL, EAL2+). This event is of significance to all TSS instances.
  Note: If there is reasonable evidence that activating this audit event may lead to unintended deadlocking or bricking of the CSP, e.g. implementations using a secure element with limited

memory capacity, this event may be omitted. If this event is omitted, the start-up of the CSP must be comprehensible indirectly, e.g. by logging a discrete adjustment of system time at a time close to zero, cf. 4.2.

- **start-up and shutdown of the audit functions** (FAU_GEN.1.1 a)): The event indicating a change in the audit configuration leading to the start-up or shutdown of some or all audit events. One audit log message indicating the start-up of the audit functions must be created for each connected SMAERS instance.
  For CSP devices using only a fixed signing key during their whole life cycle, this event shall be triggered during or immediately after the initialization and personalization of the CSP. For CSP devices hosting more than one signing key during their whole life cycle, this event shall be triggered before, during or immediately after the initialization and personalization phase of the SMAERS component. This event must be triggered for each newly added TSS instance, i.e. whenever a new signing key and PACE key are configured. The resulting log message is typically the first log message present in the audit trail of a TSS instance. This event shall not be triggered after each start-up of the CSP. This event is of significance to all TSS instances affected.
- **authentication failure handling** (FAU_GEN.1.1 d) (3)): The event indicating an exhausted retry counter of a configured PIN or other failures indicating a repeated attempt of unauthorized access. Events indicating failed access to administrative CSP users or roles are of significance to all TSS instances. Events indicating failed access to user roles, e.g. role SMAERS application, are of significance to the affected TSS instance.
- **Import of UCP** (FAU_GEN.1.1 d) (2)): The event indicating success or failure of Update Code Package execution. This event is of significance to all TSS instances.
- **Discrete adjustment of the real time clock** (FAU_GEN.1.1 c)): The event indicating a **discrete** time adjustment. This event is of significance to all TSS instances.
  To reduce performance impacts during regular adjustments of CSP time, centralized CSP appliances securely operated in a data center may: a) Make use of time skewing within limits given in [TR TSEA], avoiding a discrete adjustment, and b) omit the generation of the audit log message for TSS instances if a corresponding system log message is created instead, thus avoiding duplicated logged content in the log trail of the TSS.

The following audit event is mandatory to log for a CSP certified according to [PP CSPL] and optional if a CSP is certified according to [PP CSP]:

- **generation and destruction of cryptographic keys and key material** (FAU_GEN.1.1 d) (4) and (6)): The events indicating the configuration, generation, destruction and de-configuration of signing keys. These events are of significance to the affected TSS instance.

The following audit events are optional to log for a CSP operating in cluster mode and certified according to [PP CSPL] or [PP CSP]:

- **generation and destruction of cryptographic keys and key material for cluster operation** (Fau_GEN.1.1 d) (4) and (6)) (only CSP in cluster operation): The events indicating the configuration, generation, destruction and de-configuration of keys used for the trusted channel between devices operating in cluster mode. These events are of significance to all TSS instances.
- **import and export of signing keys in cluster operation** (only CSP in cluster operation): The events indicating import and export of signing keys between CSP appliances operating in cluster mode. These events are of significance to the affected TSS instance.

Additional audit log messages, as e.g. defined in FAU_GEN.1.1 (5), (7)-(9) & (11) may be created. However, log messages that do not concern security functionality, must not be signed with the TSS signing key (chapter 5.3.1).

# 6 Update Concept (Update-Konzept)

In the context of the TSS, the update functionality primarily is a tool to recover from security incidents, but may be used to apply functional updates as well. Both components of the security module, SMAERS and CSP, provide the functionality to install updates to its implementation in the form of Update Code Packages. While the implementation of UCP handling is covered in the corresponding protection profiles by security functional requirements (SFRs), and thus directly part of the (technical) security evaluation activities, most of the organizational life cycle aspects must be evaluated based on this supporting document. The Update Concept and its requirements are directly linked to the assessment of OE.SUCP, OE.SecUCP [PP SMAERS] and OE.SUCP [PP CSP], respectively.

For this chapter the term “concept” always refers to the “Update Concept”.

For the evaluation activities regarding this concept the term ‘*documentation*’ includes

- the Update Concept,
- the development and guidance documentation of SMAERS,
- the provided guidance documentation of the CSP,
- the Secure Platform Concept,
- and, at the discretion of the evaluator, the source code of SMAERS.

This *documentation* shall be used as the input of the evaluation activities, if not noted otherwise.

**Evaluation Activity (EA6.1)**

*The evaluator **shall examine** the documentation to determine that the mapping of the requirements within the Update Concept and the objectives OE.SecUCP [PP SMAERS] and OE.SUCP [PP CSP] are consistent. Consistency means that the implementations described in the Update Concept must not contradict the requirements of the PP.*

**Evaluation Activity (EA6.2)**

*The evaluator **shall examine** the documentation to determine that the manufacturer provides a detailed concept describing the update processes covering the full life cycle of both SMAERS and CSP in the context of the TSS.*

**Evaluation Activity (EA6.3)**

*The evaluator **shall examine** the documentation to determine that the Update Concept contains complete descriptions of the technical background, used tools, actions to perform and the implementation of functionality used in this context. The concept must also contain thorough descriptions of organizational concepts including roles and responsibilities.*

**Evaluation Activity (EA6.4)**

*The evaluator **shall check** that the Update Concept includes a statement from the respective component manufacturer, i.e. SMAERS and CSP manufacturer, to actively contribute to solutions mitigating a security incident and a commitment to develop, test and deploy corresponding Update Code Packages in a timely manner.*

**Evaluation Activity (EA6.5)**

*The evaluator **shall examine** the documentation to determine that the Update Concept describes which parts of the components and respective platforms are subject to potential updates of their respective implementations. This description must include technical considerations as well as organizational aspects, e.g. dependencies on third parties, which parts of the components from third parties can be updated, and that the components of the third parties are actively maintained.*

**Evaluation Activity (EA6.6)**

*The evaluator **shall examine** the documentation to determine that for each security relevant asset of the respective component, the Update Concept describes to what extent the protective goals, i.e. integrity, authenticity and confidentiality, are affected. The concept must discuss the viability of termination of the affected component (and thus the TSS instance) and initialization of a new component – thus initializing a new TSS instance - as an alternative to the deployment of an Update Code Package to recover from severe security or functionality related incidents.*

**Evaluation Activity (EA6.7)**

*The evaluator **shall examine** the documentation to determine that the documentation describes the life cycle of the TOE concerning its certification status when applying an update. In particular, the evaluator shall verify that*

- *at the start, the TOE is in the life cycle state operational and the implementation corresponds to the valid CC certificate, i.e. the update shall target a certified TOE,*
- *the steps that update the TOE with certified Update Code Package are described and*
- *how the application of this update leads again to an implementation that corresponds to a valid CC certificate (that is or would be the result of a Maintenance or Re-Certification).*

*The evaluator **shall check** that an exemplary time schedule is included in the concept that illustrates the activities in the time period covering the identification of a security incident and the in-field application of the Update Code Package.*

## 6.1 Creation and Signing

The Update Concept must describe the functions and methods used to sign UCPs and enforce the installation of authenticated UCPs for the corresponding component. The Update Concept must provide evidence to assess the level of assurance of those functions and methods, if those functions and methods were not evaluated according to the PP the component is based on, i.e. if functions and methods of the underlying platform are used in a non-composite CC evaluation. Such evidence must at least include a survey of information available in the public domain or requested documentation. Some examples for such documentation are:

- public documentation that is the result of a Common Criteria certification of the underlying platform, for example for the CC certification of the operating system if one has been conducted
- product manuals that describe security functionality or functionality that is used by the update process, i.e. technical documentation available on the website of the platform vendor.
- security hardening and security configuration guides provided by the platform vendor.

For those documents the term '*additional platform documentation*' is used in this context.

**Evaluation Activity (EA6.8)**

*The evaluator **shall examine** the documentation to determine that the Update Concept describes the process starting from a feature request and/or security incident until a signed Update Code Package is created. It must further describe the associated quality management of the UCP that mitigates the risk of introducing new security relevant faults and ensures a reliable UCP deployment.*

**Evaluation Activity (EA6.9)**

*The evaluator **shall examine** the documentation and the additional platform documentation to determine that the respective component can only install authenticated Update Code Packages, i.e. UCPs must be cryptographically signed. The evaluator **shall examine** the documentation and the additional platform documentation to determine that only the respective component manufacturer is able to create or initiate the creation of authentic UCPs.*

**Evaluation Activity (EA6.10)**

*The evaluator **shall check** that the handling of the signing key of the UCP (or equivalent private keying material or secret passwords, e.g. access credentials to the platform's app distribution management) used for the creation of the authenticated UCP is described in the Update Concept. The evaluator **shall examine** the documentation to determine that the manufacturer of the to be updated component has restrictively limited access to those keys and enforces secure creation and storage of those keys.*

## 6.2 Distribution, Deployment and Enforcement

**Evaluation Activity (EA6.11)**

*The evaluator **shall examine** the documentation to determine that the Update Concept describes how the UCP is distributed and deployed on the target platform. If the target must be configured for secure deployment and installation of an authenticated UCP, the configuration and further necessities must be described. Again, the Update Concept must provide evidence to assess the level of assurance the platform provides when configured in the described manner. Those descriptions must not contradict those given in the Trust-Provisioning concept and the Secure Platform Concept.*

# 7 SMAERS Trust Provisioning Concept (Trust-Provisioning-Konzept)

SMAERS is a certified software component utilizing its operational environment, particularly CSP, to implement the application logic of the security module of the TSS. As a software component, it is assumed that life cycle considerations, specifically the provisioning with security related assets, is not in the scope of the evaluation of the TOE according to [PP SMAERS]. The Trust Provisioning Concept is required to fill this gap, detailing the processes and actions required to configure and initialize the software TOE and its assets as an operating part of the security module of the TSS in its proposed use case. The concept must present evidence as appropriate.

Note: All requirements given in this supporting document hold for all types of SMAERS components regardless of its factual implementation and usage type. However, certain types of TOEs, e.g. those in 'integration ready' TSS devices, might implicitly fulfill the listed requirements due to its specific life cycle considerations.

For this chapter the term "concept" always refers to the "SMAERS Trust Provisioning Concept".

For the evaluation activities regarding this concept the term '*documentation*' includes

- the SMAERS Trust Provisioning Concept,
- the development and guidance documentation of SMAERS,
- the provided guidance documentation of the CSP,
- the Secure Platform Concept,
- and, at the discretion of the evaluator, the source code of SMAERS.

This *documentation* shall be used as the input of the evaluation activities, if not noted otherwise.

## 7.1 Operational Environment and Life Cycle Alignment

SMAERS must be operated in the same physical operational environment as the electronic record-keeping system (ERS), cf. A.ProtComERS/OE.SecOEnv [PP SMAERS]. Thus, SMAERS (and thus the TSS) is always considered 'local'. This supporting document does not further define nor specify the ERS component.

The ERS, its supplementary systems and the operational environment as well as the TSS device are assumed to be operated and administrated by the taxpayer. Here, administration of the TSS device is limited to the capabilities of the TSS interface and does not include administration of the security module of the TSS device itself.

**Evaluation Activity (EA7.1)**

*The evaluator **shall examine** the documentation to determine that administrative access to the TOE is limited to the manufacturer or the integrator of the security module, cf. Chapter 2.3. The taxpayer must not be able to gain administrative access apart from triggering an UCP, if necessary.*

Note: The TSS interface, SMAERS and the CSP all implement their own role model. In particular, each component utilizes their own administrator role(s) for configuration and/or operation and must be implemented as such.

Part of the operational environment of SMAERS is the (hardware and software) platform the TOE is executed on or otherwise depending on. The platform must provide secure storage and means to protect the integrity of the TOE and its assets, cf. OE.SMAERSPlatform [PP SMAERS]. Details regarding the platform and how to accomplish the associated security objectives must be presented in an additional document, cf. Chapter 8.

**Evaluation Activity (EA7.2)**

*The evaluator **shall examine** the documentation to determine that the Trust Provisioning Concept describes by whom and when the platform is configured according to the Secure Platform Concept during trust provisioning, i.e. how the initialization and configuration of the platform aligns with the trust provisioning of the TOE.*

Note: Contrary to the above notion about the administration of the operational environment, the Secure Platform Concept might likely restrict administrative access of the platform to trusted roles.

The CSP is conceptually also part of the operational environment, but might be physically separated, cf. OE.CSP and OE.SecCommCSP in [PP SMAERS]. It is assumed that the corresponding CSP instance is in its operational state during the complete life cycle of the SMAERS instance. CSP devices that are used with a single fixed SMAERS instance over the full life time of the TSS device, e.g. as a component in a TSS hardware token, might be initialized and personalized within the same production step as SMAERS.

## 7.2 Trust Provisioning and Assets

**Evaluation Activity (EA7.3)**

*The evaluator **shall examine** the documentation to determine that the trust provisioning process is described in detail. This includes the initialization and personalization of the TOE, i.e. the configuration of the SMAERS software component and its provisioning with the required assets to form the application part of operating TSS security module. The evaluator has to verify that the process adheres to the requirements listed below:*

- ***Mapping of Components and Instances***

  *The TSS requires a direct unique bidirectional mapping between its main assets and components. That is, each TSS instance requires the existence of exactly one signing key with signature counter, exactly one corresponding strict monotonically increasing transaction number managed by exactly one corresponding SMAERS instance, cf. [TR TSEA]. Thus, and to achieve integrity of the transaction number, the trust provisioning process must ensure that only one unique SMAERS instance is coupled to a unique CSP during the life time of the TSS instance and a SMAERS instance must only be initialized once. For this, technical means enforcing this requirement are preferred.*
  *Note: 'Instance' should be interpreted as a specific incarnation of a component in this context, thus e.g. a single physical CSP device managing more than one signing key effectively serves more than one SMAERS instances. The CSP manages exactly one unique set of respectively required assets for each TSS.*

  *On first connection of the SMAERS instance and after each successful installation of an Update Code Package of SMAERS, the attestation mechanism of the CSP may be used to verify the authenticity of the CSP component, see Chapter 5.4.1. If remote attestation is used, the evaluator **shall examine** the source code of SMAERS to verify that behavior.*

- ***PACE Key and Initial Seed***

  *The PACE key is a symmetric secret key used to mutually authenticate the SMAERS and CSP component of the TSS, see also Chapter 5.3.2. The trust provisioning of the SMAERS component must ensure confidentiality of the PACE key and additional secrets used for this purpose. The latter includes key material and authentication reference data used for retrieving and transportation of the PACE key, e.g. TLS ephemeral keys and passwords used by the integrator during the integration and personalization process.*

  *If the SMAERS TSF implementation requires an initial seed, the same requirements as for the provisioning of the PACE key apply for the provisioning of the initial seed. Each SMAERS instance must use an initial seed that is individual w.r.t. each instance.*

- ***Administrator Credentials***

  *Authentication reference data used to gain access to the SMAERS admin role must be set to an instance individual value during the personalization process. The authentication reference data must only be known to trustworthy entities. If the SMAERS administrator role is not required during SMAERS operation, the authentication reference data must be set to a random value or the administrator role must be permanently deactivated.*

- ***SMAERS Configuration***

  *During personalization and initialization, the following configuration must be applied: All SMAERS audit events must be enabled. The transaction number must be initialized to the value 0 (zero). Note: Further clarification on the counting method is found in [TR TSEA].*

# 8 Secure Platform Concept (Umgebungsschutzkonzept)

The TOE is a software component. This software component is executed on a platform and must be run in the same physical operational environment as the electronic record keeping systems [PP SMAERS]. The TOE relies on the operational environment to ensure its integrity and authenticity as well as the integrity and authenticity of its assets. The manufacturer must provide a detailed description to the evaluator on how the operational environment ensures these tasks. These requirements strongly depend on the underlying platform. The manufacturer must describe what platform the TOE is intended to run on, and the platform must be supplied with updates by the platform manufacturer.

The evaluator activities are in addition to the refined SAR's defined in [PP SMAERS].

Requirements differ with respect to the following platform categories. If a manufacturer’s hard- and software platform fits into one of the following categories, than a successful evaluation by the evaluator are deemed sufficient to ensure that all requirements are met and that the TOE can be operated as certified.

If the underlying hard- and software platform does not fit into one of the categories listed below, or alternative measures to secure the platform according to the required security level are used (e.g. WhiteBoxCrypto), the Secure Platform Concept requires explicit approval by BSI.

The manufacturer must provide documentation in form of a step-by-step guide that enables an integrator to ensure that a TOE is operated as certified and that all platform requirements are met. This includes in particular, but not only, instructions to verify that the integrity of the TOE and the integrity and confidentiality of its assets are not violated. The document should enable fiscal authorities to execute the verification steps without requiring expert IT knowledge.

**Requirements for test samples**

The manufacturer must provide test samples for the hard- and software platforms that the TOE is intended to run on, such that the evaluator is able to verify the steps outlined in the provided documentation. One test sample for each class of platform configurations has to be provided. One platform configuration is defined by the following parameters:

- major versions of operating systems, e.g. Windows 10 Home, Windows 11 Pro, IoT Enterprise, Windows Server 2022, Ubuntu 20.04, Ubuntu 22.04, Android 12, Android 13 etc.
- major versions of essential services, e.g. JRE 11
- hard- and firmware revisions of microcontrollers

All required non-TOE-components must be defined and provided by the manufacturer.

For this chapter the term “concept” always refers to the “Secure Platform Concept”.

For the evaluation activities regarding this concept the term ‘*documentation*’ includes

- the Secure Platform Concept,
- the development and guidance documentation of SMAERS,
- sources of information publicly available regarding the respective platform,
- and, at the discretion of the evaluator, the source code of SMAERS.

This *documentation* shall be used as the input of the evaluation activities, if not noted otherwise.

**Evaluation Activity (EA8.1)**

*The evaluator **shall examine** the documentation and provided test samples of the hard- and software platform to determine that the configuration steps outlined in the evaluation activities are possible and effective.*

**Evaluation Activity (EA8.2)**

*The evaluator **shall check** that the concept lists all classes of platforms that the TOE is intended to run on, including specific platform identifiers and version numbers, as described above in section 8 "Requirements for test samples".*

**Evaluation Activity (EA8.3)**

*The evaluator **shall examine** the sources of information publicly available to determine that all platforms the TOE is intended to run on, are supplied with security updates timely when required by the platform manufacturer. The evaluator shall verify that the Secure Platform Concept contains a viable concept on how these platforms are provided with security patches for the whole life time of SMAERS. If the provisioning of security updates for the platform for the whole life time of SMAERS cannot be guaranteed at the time of evaluation or is otherwise infeasible, the documentation shall contain a description on how the manufacturer intends to inform his customers by organizational or technical means that SMAERS must no longer be used on that platform, or alternatively how it is technically enforced that SMAERS cannot be used on that platform anymore. By utilizing the UCP, the secure platform concept must describe how in such a case a migration to a configuration with a supported platform plus SMAERS is conducted.*

**Evaluation Activity (EA8.4)**

*The evaluator **shall check** that each platform that the TOE is intended to run on fits to one of the categories described below, or that explicit approval by BSI exists. The evaluator must conduct the evaluation activities of the respective section below for each platform, if applicable.*

**Evaluation Activity (EA8.5)**

*The TOE shall prevent the reset of the transaction number to a previous value, e.g. by replay attacks. The evaluator **shall examine** the documentation to determine that the concept contains information how this is achieved.*

**Evaluation Activity (EA8.6)**

*The evaluator **shall examine** the documentation to determine that the concept provides guidance documentation in form of a step-by-step guide that enables an integrator to ensure that a TOE is operatedas certified and that all platform requirements are met. This includes both operational requirements as well as technical functionality, e.g. how to start self-tests by SMAERS and/or the underlying platform.*

**SMAERS operated in the same physical operational environment as the ERS**

Note that [PP SMAERS] requires that the "operational environment shall protect the integrity of the communication between the electronic record-keeping system and the TOE."

The ERS and the TOE must be contained in the same physical operation environment.

Regarding the security requirements, the physical operational environment of the ERS extends to the entire contiguous area in which the ERS is located and for which the operator of the ERS is directly responsible. Therefore, e.g. operation of the SMAERS component located in a different room of the branch in whose salesroom the ERS is located is compliant (i.e. different room on the same premises).

Note: The operator of the ERS is in principle assumed to be the taxpayer. However, if the ERS is exclusively hosted in a certified secure environment provided by a trusted and independent third party, e.g. a cloud service provider, the 'operator of the ERS' also covers this trust service provider. Consequently, the locality requirement of SMAERS and the ERS here is fulfilled if both are hosted by the aforementioned trusted third party.

The "Secure Platform Concept" has to describe how this is ensured, and what technical and/or organizational measures are in place in order to prevent an ERS to access and use a TOE that is outside the same physical operational environment as the ERS. The evaluator must verify that it is both plausible and

practical to set up and operate SMAERS according to these requirements. As a last resort, the taxpayer may become contractually obligated to use the TOE in the operational environment of the ERS as required.

**Evaluation Activity (EA8.7)**

*As defined in [PP SMAERS], the TOE must be operated in the same physical operational environment as the ERS. The evaluator **shall examine** the documentation to determine that the concept describes how this is achieved by organizational or preferably technical means and the concept targeted to the integrator explicitly states that the local operation is a mandatory requirement.*

**Attack Scenario**

According to chapter 2.3 the default attack scenario to consider while evaluating includes unrestricted physical access of the attacker to the SMAERS component and its execution platform. However, certain environments allow to deviate from this default scenario if physical access is plausibly denied. Some of the requirements and associated evaluation activities presented in the following subchapters may depend on the attack scenario to be applied and are indicated as such.

**Evaluation Activity (EA8.8)**

*The evaluator **shall check** that the documentation contains a description of the attack scenario claiming whether physical access to the SMAERS platform for the attacker is possible or not.*

**Evaluation Activity (EA8.9)**

*If the documentation claims that physical access to the platform is not possible (c.f. EA8.8), the evaluator **shall examine** the documentation and additional documentation of the operation environment of SMAERS to determine if access to the SMAERS platform is not possible for an attacker, both logically and physically. For this, SMAERS and its platform must be hosted by a trusted third party that is independent from the taxpayer in an audited environment implementing secure client separation.*

## 8.1 Devices running the Microsoft Windows Operating System

The operating system must be hardened to ensure the integrity and authenticity of SMAERS. To ensure this by the platform the SMAERS component is executed on, a computer running Microsoft Windows must be equipped with a Trusted Platform Module 2.0, if access to the platform is not ruled out for an attacker, c.f. EA8.8.

**Evaluation Activity (EA8.10)**

*The evaluator **shall check** that the concept explicitly states that only a restricted amount of user applications are configured on the system, i.e. only the SMAERS application, application components of the ERS and the minimum of applications required for business operation and administrational purposes and applications provided by the operating system are configured. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that either with technical or organizational means.*

**Evaluation Activity (EA8.11)**

*The evaluator **shall check** that the concept explicitly states that the Built-in administrator account (local default administrator account) must be deactivated. Those user accounts that are able to execute administrative functions must only be held by the SMAERS platform administrator. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.12)**

*The evaluator **shall check** that the concept explicitly states that antivirus protection must be installed on the host system. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.13)**

*The evaluator **shall check** that the concept explicitly states that secure boot must be activated on the host system. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.14)**

*The evaluator **shall check** that the concept explicitly states that secure credential entry must be activated via group policy settings. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.15)**

*The evaluator **shall check** that the concept explicitly states that booting from external devices must be deactivated, if access to the platform is not ruled out for an attacker, c.f. EA8.8. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.16)**

*The evaluator **shall check** that the concept explicitly states that early launch anti-malware (ELAM)[4] is configured to allow only 'known good' drivers to initialize. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.17)**

*The evaluator **shall check** that the concept explicitly states that user account control is configured such that all sensitive actions require user interaction for privilege escalation. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that, by e.g. group policy settings.*

**Evaluation Activity (EA8.18)**

*The evaluator **shall check** that the concept explicitly states that Windows Updates must be configured and enabled to install security updates. The concept must describe how it is ensured that security updates are installed in a timely manner, e.g. by turning on automatic updates or technical or organizational means. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.19)**

*The evaluator **shall check** that the concept explicitly states that Windows audit mechanisms are configured such that security related audit events are captured and can be analyzed. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.20)**

*The evaluator **shall check** that the concept explicitly states that Autoplay and Autorun must be deactivated. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.21)**

*The evaluator **shall check** that the concept explicitly states that communication interfaces that allow direct memory access, such as for example FireWire and Thunderbolt, are deactivated, if access to the platform is not ruled out for an attacker, c.f. EA8.8.. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

[4] https://learn.microsoft.com/en-us/windows-hardware/drivers/install/elam-driver-requirements

**Evaluation Activity (EA8.22)**

*The evaluator **shall check** that the source code of SMAERS is not trivially obtainable, e.g. no trivial decompilation of the SMAERS binary is possible. This requirement shall be assumed to be fulfilled if either native code (e.g. C/C++) is used to build the application or if code obfuscation techniques are applied. It is recommended to apply code obfuscation regardless of the used development language.*

**Evaluation Activity (EA8.23)**

*The evaluator **shall check** that the concept explicitly states that strong authentication, e.g. using strong passwords or asymmetric cryptographic keys, must be enforced for all accounts. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.24)**

*The evaluator **shall check** that the concept explicitly states that drive encryption is activated and SMAERS assets are stored encrypted and integrity protected. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.25)**

*The evaluator **shall check** that the concept explicitly states that the hardware platform that SMAERS is intended to run on must be equipped with a Trusted Platform Module (TPM) Version 2.0 according to [TPM, if access to the platform is not ruled out for an attacker, c.f. EA8.8.].*

**Evaluation Activity (EA8.26)**

*If access to the platform is not ruled out for an attacker, c.f. EA8.8, the evaluator **shall examine** the documentation to determine that the concept provides detailed configuration instructions that ensure that SMAERS stores its assets either directly on the TPM, or on the host file system that is encrypted by the platform with the encryption key stored on the TPM.*

**Evaluation Activity (EA8.27)**

*The evaluator **shall examine** the documentation to determine that the concept provides detailed configuration instructions that protect the access and usage of assets.*

**Evaluation Activity (EA8.28)**

*If access to the platform is not ruled out for an attacker, c.f. EA8.8, SMAERS assets on the TPM, such as e.g. the PACE key, must be sealed to a known valid software state using platform control registers. The integrity of the device shall be verified by the manufacturer in defined intervals using remote integrity verification mechanisms of the TPM (remote attestation). The evaluator **shall examine** the documentation that the concept provides detailed guidance for such a setup and verify with the provided source code, that sealing and remote integrity verification are implemented in the TOE. The evaluator shall also technically verify the attestation mechanisms by validating generated remote attestation signatures with provided test keys.*

**Evaluation Activity (EA8.29)**

*If access to the platform is not ruled out for an attacker, c.f. EA8.8, drive encryption using Bitlocker (Windows) must be enabled on the hardware platform. The evaluator **shall examine** the documentation to determine that the concept contains detailed instructions on how to setup up drive encryption and seal the decryption key to a successful login using platform control registers.*

**Evaluation Activity (EA8.30)**

*Access to files and folders should be configured according to the need-to-know principle, i.e. only those users, groups and services must have access that are required for operation. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.31)**

*The evaluator **shall examine** that the concept explicitly states that running services of the operating system must be kept to the minimum required for operation. For third-party services, groups of services covering a dedicated functionality, e.g. 'antivirus' or 'VPN connector', should be listed and it must be explained, why each service group is required for operation and why it does not have negative impact to the operation of SMAERS or opens threats to the assets of SMAERS.*

## 8.2 Devices running the Linux Operating System

The operating system must be hardened to ensure the integrity and authenticity of SMAERS. To ensure this by the platform the SMAERS component is executed on, a computer running the Linux Operating System must be equipped with a Trusted Platform Module 2.0, if access to the platform is not ruled out for an attacker, c.f. EA8.8.

**Evaluation Activity (EA8.32)**

*The evaluator **shall check** that the concept explicitly states that only a restricted amount of user applications are configured on the system, i.e. only the SMAERS application, application components of the ERS and the minimum of applications required for business operation and administrational purposes and applications provided by the operating system are configured. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that either with technical or organizational means.*

**Evaluation Activity (EA8.33)**

*The evaluator **shall check** that the concept explicitly states that the platform's programs and services must be kept to the minimum required for running SMAERS, e.g. by applying a minimal installation. For third-party services, each service should be listed and it must be explained, why this service is required for operation and why it does not impact operation of SMAERS.*

**Evaluation Activity (EA8.34)**

*The evaluator **shall check** that the concept explicitly states that the root account must be deactivated. Those user accounts that are able to execute administrative functions via 'sudo' must be held by the SMAERS platform administrator. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.35)**

*The evaluator **shall check** that the concept explicitly states that secure boot must be activated on the host system. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.36)**

*The evaluator **shall check** that the concept explicitly states that booting from external devices must be deactivated*, if access to the platform is not ruled out for an attacker, c.f. EA8.8. *The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.37)**

*The evaluator **shall check** that the concept explicitly states that the operating systems security update mechanism must be configured and enabled. The concept must describe how it is ensured that security updates are installed in a timely manner, e.g. by turning on 'unattended-upgrades' or technical or organizational means. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.38)**

*The evaluator **shall check** that the concept states that the Linux audit framework must be activated and configured to log all security related incidents. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.39)**

*The evaluator **shall check** that the concept states that an application security framework such as e.g. AppArmor, SELinux or equivalent must be installed and activated. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.40)**

*The evaluator **shall check** that the concept states that a firewall must be installed, activated, and configured such that the bare minimum of traffic that is required for SMAERS, components of the ERS and essential system components to operate is allowed. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.41)**

*The evaluator **shall check** that the source code of SMAERS is not trivially obtainable, e.g. no trivial decompilation of the SMAERS binary is possible. This requirement shall be assumed to be fulfilled if either native code (e.g. C/C++) is used to build the application or if code obfuscation techniques are applied. It is recommended to apply code obfuscation regardless of the used development language.*

**Evaluation Activity (EA8.42)**

*The evaluator **shall check** that the concept explicitly states that strong authentication, e.g. using strong passwords or asymmetric cryptographic keys, must be enforced for all accounts. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.43)**

*The evaluator **shall check** that the concept explicitly states that drive encryption is activated and SMAERS assets are stored encrypted and integrity protected. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

**Evaluation Activity (EA8.44)**

*If access to the platform is not ruled out for an attacker, c.f. EA8.8, the evaluator **shall check** that the concept explicitly states that the hardware platform that SMAERS is intended to run on must be equipped with a Trusted Platform Module (TPM) Version 2.0 according to [TPM].*

**Evaluation Activity (EA8.45)**

*If access to the platform is not ruled out for an attacker, c.f. EA8.8, the evaluator **shall examine** the documentation to determine that the concept provides detailed configuration instructions that ensure that SMAERS stores its assets either directly on the TPM, or on the host file system that is encrypted by the platform with the encryption key stored on the TPM.*

**Evaluation Activity (EA8.46)**

*The evaluator **shall examine** the documentation to determine that the concept provides detailed configuration instructions that protect the access and usage of assets.*

**Evaluation Activity (EA8.47)**

*If access to the platform is not ruled out for an attacker, c.f. EA8.8, SMAERS assets on the TPM, such as e.g. the PACE key, must be sealed to a known valid software state using platform control registers. The integrity of the device shall be verified by the manufacturer in defined intervals using remote integrity verification mechanisms of the TPM (remote attestation). The evaluator **shall examine** the documentation to determine that the concept provides detailed guidance for such a setup and verify with the provided source code, that sealing and remote*

*integrity verification are implemented in the TOE. The evaluator shall also technically verify the attestation mechanisms by validating generated remote attestation signatures with provided test keys.*

**Evaluation Activity (EA8.48)**

*If access to the platform is not ruled out for an attacker, c.f. EA8.8, Drive encryption using LUKS (Linux) must be enabled on the hardware platform. The evaluator **shall examine** the documentation to determine that the concept contains detailed instructions on how to setup up drive encryption and seal the decryption key to a successful login using platform control registers.*

**Evaluation Activity (EA8.49)**

*Access to files and folders should be configured according to the need-to-know principle, i.e. only those users, groups and services must have access that are required for operation. The evaluator **shall examine** the documentation to determine that the concept contains instructions how to achieve that.*

## 8.3 Devices running the Android Operating System

**Evaluation Activity (EA8.50)**

*The Android device must fulfill the Android compatibility guidelines. The evaluator **shall examine** the documentation to determine that the concept contains detailed instructions on how to verify this.*

**Evaluation Activity (EA8.51)**

*The Android device must be a certified play-protected device. The evaluator **shall examine** the source code to determine, that the TOE verifies technically that the device is play-protected and restricts the installation to play-protected devices only.*

**Evaluation Activity (EA8.52)**

*SMAERS assets, such as e.g. the PACE key, must be protected by a hardware-backed keystore to ensure their integrity and confidentiality. The evaluator **shall examine** the source code to determine, that the TOE uses the keystore to secure its assets and verifies that the keystore is backed by hardware.*

**Evaluation Activity (EA8.53)**

*The Android device must not be rooted. The evaluator **shall examine** the source code to determine that the TOE verifies the root status of the device and prohibits operation if rooting of the device is detected.*

**Evaluation Activity (EA8.54)**

*The evaluator **shall examine** the source code to determine that the TOE verifies that it is executed on an actual physical device and not a simulator, and prohibits operation on a simulator.*

**Evaluation Activity (EA8.55)**

*The evaluator **shall examine** the source code and building tool chain to determine that the source code of SMAERS is not trivially obtainable, e.g. no trivial decompilation of the SMAERS binary is possible. This requirement shall be assumed to be fulfilled if either native code (e.g. C/C++) is used to build the application or if code obfuscation techniques are applied. It is recommended to apply code obfuscation regardless of the used development language.*

**Evaluation Activity (EA8.56)**

*The TOE must be distributed via the Google Play store. Sideloading must not be used. The evaluator shall examine the documentation, the Trust Provisioning Concept and the personalization concept to determine that they contain detailed information about the distribution process and that the described distribution process is technically and organizationally feasible.*

## 8.4 Devices running the iOS Operating System

**Evaluation Activity (EA8.57)**

*SMAERS assets, such as e.g. the PACE key, must be protected by the secure enclave to ensure their integrity and confidentiality. The evaluator **shall examine** the source code to determine, that the TOE uses the secure enclave to secure its assets.*

**Evaluation Activity (EA8.58)**

*The iOS device must not be jailbroken. The evaluator **shall examine** the source code to determine that the TOE verifies the jailbreak status of the device and prohibits operation if jailbreaking of the device is detected.*

**Evaluation Activity (EA8.59)**

*The evaluator **shall examine** the source code to determine that the TOE verifies that it is executed on an actual physical device and not a simulator, and prohibits operation on a simulator.*

**Evaluation Activity (EA8.60)**

*The evaluator **shall examine** the source code and building tool chain to determine that no trivial decompilation of the binary is possible. This requirement shall be assumed to be fulfilled if either native code (e.g. C/C++) is used to build the application or if code obfuscation techniques are applied. It is recommended to apply code obfuscation regardless of the used development language.*

**Evaluation Activity (EA8.61)**

*The TOE must be distributed via the Apple App Store. Sideloading must not be used. The evaluator **shall examine** the documentation, the Trust Provisioning Concept and the personalization concept to determine that they contain detailed information about the distribution process and that the described distribution process is technically and organizationally feasible.*

## 8.5 Microcontrollers

The term ‘microcontroller’ here describes programmable devices directly executing compiled custom code without utilizing a rich operating system capable of advanced features like e.g. multitasking, on chip application management and the like. Thus, advanced microcontrollers, e.g. SoCs and Secure Elements running a JavaCard-OS, are not in scope of this chapter.

**Evaluation Activity (EA8.62)**

*The evaluator **shall examine** the documentation to determine that the platform only executes code needed for the operation of the TOE and TSS components.*

**Evaluation Activity (EA8.63)**

*The evaluator **shall check** that the microcontroller possesses a readout-protection mechanism. The evaluator **shall examine** the test sample and its technical documentation to determine that the readout-protection is activated and cannot be trivially circumvented, by e.g. setting a jumper or changing a dip-switch.*

**Evaluation Activity (EA8.64)**

*The evaluator **shall examine** sources of information publicly available to determine that there are no publicly known exploits to circumvent the readout protection of the chip, i.e. the firmware is securely protected by the chip. The literature survey shall include CVE's as well as scientific literature. The evaluator shall in particular examine the difficulty of reproducing such an attack, i.e. by applying a publicly known exploit or exploit method.*

**Evaluation Activity (EA8.65)**

*The evaluator **shall examine** the test sample and its technical documentation to determine that debugging interfaces - such as e.g. JTAG - are permanently deactivated if possible. If impossible, the evaluator **shall examine** the documentation to determine that the interface in question does not interfere with the TOE TSF. Further, the evaluator **shall examine** the documentation to determine that if the manufacturer delegates provisioning of the TOE with the microcontroller to the role integrator that detailed and effective instructions are provided in the documentation on how to deactivate all debugging interfaces for production.*

**Evaluation Activity (EA8.66)**

*The evaluator **shall examine** the documentation including the source code to determine that all SMAERS assets are securely stored on the microcontroller, i.e. confidentiality and integrity are preserved in the given attack scenario. If the microcontroller has to use external storage for this, e.g. additional flash memory, the evaluator **shall examine** the documentation including the source code to determine that SMAERS assets are stored encrypted and integrity protected and the encryption key is securely stored on the microcontroller. .*

## 8.6 CC-Certified CSP in platform architecture

**Evaluation Activity (EA8.67)**

*The evaluator **shall check** that the TOE uses a CC-certified CSP as its execution environment according to 'OE.CSPPlatform' in [PP SMAERS]. The evaluator **shall examine** the documentation to determine that no other execution platforms are able to operate the TOE.*

**Evaluation Activity (EA8.68)**

*The evaluator **shall examine** the documentation to determine that the TOE exclusively uses certified functionality of the platform to ensure integrity of the TOE itself and integrity and confidentiality of its security relevant assets.*

# 9 PKI Concept (PKI-Konzept)

Requirements for the PKI, PKI operation and PKI Concept(s) are out of scope of this document and regulated by [TR TSEA]. This includes requirements regarding the correct identification of the taxpayer, the binding of the TSS and keying material to the taxpayer and the verifiability of generated signatures by third parties.

# 10 SMAERS Appendix: Operational Requirements for CSPLight

CSPLight [PP CSPLight] is a software component that requires a secure platform, i.e. a hardware component and/or operating system to run on (cf. Non-TOE Hardware/Software/Firmware available to the TOE as described below). An instantiation of CSPLight used in the context of the TOE must provide the same level of security as a certified CSP, however, some physical security requirements are satisfiable by the operational environment in combination with operational security requirements.

**Hardware Certification**

A certified hardware platform must be used to execute CSPLight. For details, cf. [TR TSEA].

**Security Audit**

The following aspects must be considered for the operation of a CSPLight within the security audit according to ISO/IEC 27001:

- The hardware platform on which CSPLight runs must be certified.
- The operating environment of CSPLight must be protected such that loss or theft of CSPLight and its underlying hardware platform is prevented.
- Inspections at regular intervals must be conducted to ensure that CSPLight and its underlying hardware platform has not been physically tampered with, that CSPLight and its underlying software platform is in a trusted state, and that CSPLight and its underlying hardware/software platform is running in the intended configuration.
- Audit trails that are generated by CSPLight and its underlying hardware/software platform must be collected and regularly reviewed by the system administrator according to a specified audit process.
- The CSPLight must be configured to disallow external backup of private keys, instead clustering must be used to provide business continuity.
- Access to CSPLight and/or its underlying platform must enforce the principle of dual control. For all of the above, guidance given in the controls of ISO/IEC 27002 SHOULD be taken into account.

# 11 References

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

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

[PP CSPLight] Common Criteria Protection Profile Cryptographic Service Provider Light, BSI-CC-PP-0111-2019

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

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

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

[TPM] ISO/IEC 11889:2015: Trusted platform module library

[AO] Abgabenordnung

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

[TR TSEA] Technische Richtlinie BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme

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

[TR ID-PROT] Technische Richtlinie BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token Part 2 – Protocols for electronic Identification, Authentication and trust Services (eIDAS)

[RFC2119] Bradner, S.: Key words for use in RFCs to indicate requirement levels

# 12 Glossary

*Table 2: Glossary*

| *Term* | *Description* |
|---|---|
| | |
| **CSP/SMAERS/TSS device** | A physical entity of the respective type. E.g. a CSP(L) device might be a Secure Element, a hardware security module or a server appliance running the CSP(L) as an applet, firmware or software application. |
| **CSP/SMAERS component** | A (generic) part of a composed product. E.g. the TSS consists of a SMAERS component, a CSP component and other components. A component might exist physically or virtually, e.g. a CSPL device might be understood as a collection of multiple virtual CSP components each serving a different TSS. |
| **SMAERS instance** | A specific incarnation of a SMAERS component. The distinction between instance and component in this document shall emphasize the requirements for instance specific actions and handling of assets, where applicable. |
| **ITSEF** | Information Technology Security Evaluation Facility |
| **key reference** | Object containing key material and key specific meta data. |
| **key material** | The actual secret or public key or passphrase. |
| **PACE** | Password Authenticated Connection Establishment. PACE is a cryptographic protocol to derive ephemeral keys used to establish a secure channel between two components mutually authenticated by a shared secret (the PACE key), c.f. [TR ID-PROT]. |
| **signing key** | The 'signing key' in the context of this document refers to the key used to sign log messages of a TSS. |
| **TSS/CTSS** | The Technical Security System (Technische Sicherheitseinrichtung) is the composed IT-product consisting of CSP, SMAERS, interface and storage components. |
| | |
| | |