fiskaly.

Operational Environment Protection Concept (Umgebungsschutzkonzept)

fiskaly Security Module Application for Electronic Record-keeping Systems

TOE Version 1.0.15

Document Version 2.0.6

2025-01-23

fiskaly GmbH

Contents

Chapter 1

Introduction

This document is the Operational Environment Protection Concept (Umgebungsschutzkonzept) for the fiskaly Security Module Application for Electronic Record-keeping Systems (with the short name "fiskaly SMAERS"). This document discusses technical and organizational means for the secure operational environment of fiskaly SMAERS.

The document starts by defining the involved roles and stating the requirements given by the Protection Profile [2]. Thereafter, the document discusses, how to install, execute, and use the TOE such that the requirements concerning the operational environment of fiskaly SMAERS are met.

1.1 Document and TOE Reference

Document Type:	Operational Environment Protection Concept (Umgebungsschutzkonzept)
Document Version:	2.0.6
Document Status:	Released
Document built from commit:	55d0d8d75a9c9b971ffae60861decf54401c3541
Date:	2025-01-23
Author:	fiskaly GmbH
Certification-ID:	BSI-DSZ-CC-1130-V4
TOE Identification:	fiskaly Security Module Application for Electronic Record-keeping Systems
TOE Version:	1.0.15
CC Version:	CC:2022 Revision 1
Assurance Level:	EAL2 augmented with ALC_LCD.1 and ALC_CMS.3
PP Conformance:	BSI-CC-PP-0105-V2-2020 including the package *Trusted Channel between TOE and CSP* from BSI-CC-PP-0105-V2-2020

Chapter 2

Roles

The following roles are important to understand and realize a secure operational environment for the fiskaly SMAERS:

- *Tax Payer* (or persons being dependent on the *Tax Payer*)
- *ERS Manufacturer*
- *SMAERS Administrator*
- *SMAERS Manufacturer*
- *Cloud Provider*

Please not that one entity can hold multiple roles unless this is prohibited by a stipulation in any of the following paragraphs.

2.1 Tax Payer

The *Tax Payer* is the user of the TSS according to §146a (1) AO. It is a taxable company (corporation) or sole proprietorship. This document does not delegate requirements of the CTSS protection to the *Tax Payer*.

2.2 ERS Manufacturer

The *ERS Manufacturer* is the developer of the ERS. This document does not delegate requirements of the CTSS protection to the *ERS Manufacturer*.

2.3 SMAERS Administrator

The *SMAERS Administrator* is the administrator of the fiskaly SMAERS and at the same time of the SMAERS platform. The role of the *SMAERS Administrator* is defined in the Protection Profile for SMAERS ([2]). According to [2], the *SMAERS Administrator* shall be different from and independent of the Taxpayer.

SMAERS Administrator are employees of fiskaly GmbH or commissioned by fiskaly GmbH to be *SMAERS Administrator*.

2.4 Cloud Provider

Cloud Provider provides a cloud computing infrastructure and allows third parties to use it for cloud computing services. Other roles of this document are able to use the cloud such that it executes (parts of) the ERS and the TSS. The *Cloud Provider* shall be different from and independent of the *Tax Payer*.

2.5 SMAERS Manufacturer

The *SMAERS Manufacturer* (i.e. fiskaly GmbH) develops the SMAERS software, i.e. the TOE and makes it available to *SMAERS Administrator*. It is provided in the form of a signed Docker image.

Chapter 3

Requirements

The requirements that are fulfilled by the implementation of the technical and operational means described in this document originate from the Security Objectives for the Operational Environment defined in SMAERS-PP [2]. These are specified as follows:

OE.SMAERSPlatform Secure platform storage

The platform that executes the TOE has to ensure the integrity of the TOE itself and to provide secure storage which protects the integrity and confidentiality of stored security relevant objects as required (cf. Chapter 1.1.2 'TOE Type'). The platform verifies and installs the UCP.

OE.SecOEnv Secure Operational Environment

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

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

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

Chapter 4

Protection concept

The following discusses how the operational environment must be implemented such that the requirements from Chapter 3 are met.

In a cloud scenario the SMAERS is installed on cloud computing infrastructure provided by a Cloud Provider. It is assumed that the *Cloud Provider* has no intention to attack SMAERS on its own or give the *Tax Payer* administrative access to SMAERS Hosts. This assumption results from the independence of the *Cloud Provider* and the trustworthiness that goes along with the ISO 27001 certification of the cloud operation. SMAERS communicates with a remotely connected CSP-L. This scenario complies with the "client-server architecture with remote computing center" as shown by Figure 2c) in [2].

4.1 Overview

Figure 4.1 provides an overview of the cloud architecture. The SMAERS is executed on a SMAERS Host (i.e. SMAERS Platform) being operated by the *SMAERS Administrator*. Multiple SMAERS instances may be executed on the same SMAERS Host. The ERS must not be executed on the SMAERS Host.

A Geographical Data Center Region is a physical location where multiple data centers of a Cloud Provider are clustered. Hence, a region is a set of collaborating data centers grouped together based on their geographical proximity.

The Security Objectives for the Operational Environment (cf. Chapter 4.2 of SMAERS Protection Profile [2]) of the TOE shall be implemented in a concrete Geographical Data Center Region by the *SMAERS Administrator*. The *SMAERS Administrator* is responsible for setting up technical measures to enforce secure communication between the ERS and the SMAERS, and to protect access to SMAERS instances. The SMAERS communicates securely with a remote CSP-L.

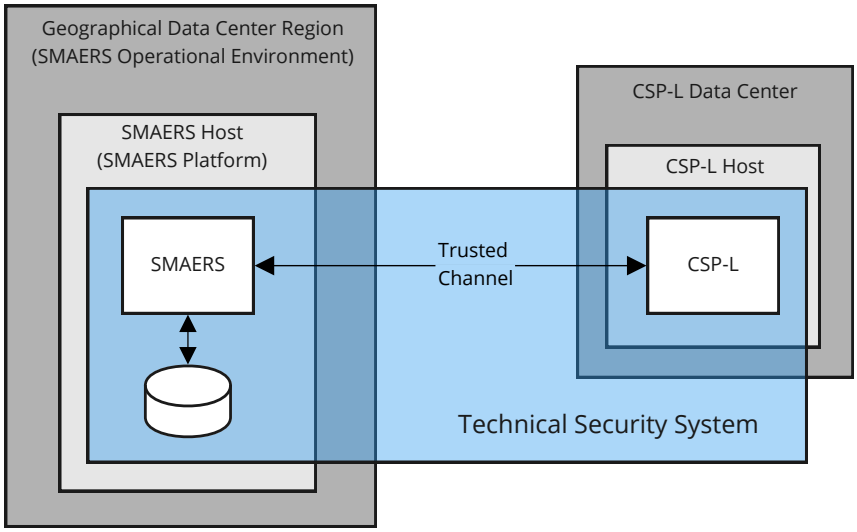

Figure 4.1: Overview of cloud architecture

4.2 Organizational realization

SMAERS Administrator shall use the Google Cloud Platform as ISO 27001 certified *Cloud Provider*.

SMAERS Administrator shall set up and operate SMAERS instances in accordance to Preparative Procedures & Operational User Guidance Document (AGD) [4].

The *SMAERS Administrator* shall check the availability of security updates regularly and apply those security updates to the SMAERS platform timely.

4.3 Technical realization

SMAERS Administrator shall set up the operational environment as follows:

(1) The secure storage of the SMAERS Platform shall be encrypted by means of the *Cloud Provider*.

(2) The operating system shall be a Linux distribution with long term support (e.g. Ubuntu 20.04 LTS).

(3) The operating system shall have been in the scope of the test of the SMAERS during the Common Criteria evaluation.

(4) Docker shall be installed.

(5) Docker Content Trust shall be enforced such that it only runs images that have been signed by the *SMAERS Manufacturer*.

(6) A reverse proxy and firewall shall be used to secure the communication between ERS and SMAERS.

(7) The firewall shall accept encrypted HTTPS traffic.

(8) The firewall shall reject plain HTTP traffic.

(9) The firewall shall only accept HTTPS traffic originating from hosts located within the same Geographical Data Center Region (e.g. IP Whitelisting).

(10) The reverse proxy shall only accept TLS 1.2 and TLS 1.3 connections with cipher suites that are recommended by BSI TR-02102.

(11) ERS shall be able to access SMAERS via the reverse proxy.

(12) The process data provided by the ERS interacting with SMAERS shall remain unaltered.

(13) Identity and Access Management (IAM) shall be implemented such that (1) only authorized ERS are allowed to access SMAERS, and (2) it is ensured that taxpayers are only allowed to access SMAERS that are associated with them.

(14) A firewall shall reject all incoming connections except SSH and HTTPS.

(15) The following steps shall be carried out in order to harden SSH:

  (1) The SSH default port shall be changed.
  (2) SSH login for the root account shall be prohibited; management can be performed by dedicated user accounts in the role *SMAERS Administrator* with sudo privileges.
  (3) SSH shall be configured to be key-based only, i.e. prevent SSH logins based on passwords.
  (4) Remote access via SSH shall only be possible for users in the role *SMAERS Administrator*.
  (5) SSH shall be configured to disable protocol version 1.
  (6) SSH shall be configured to only accept strong ciphers suites (as recommended by BSI TR-02102)

4.4 Rationale

Tax Payer has access to the TOE interface through a TLS channel and can use the TOE's functionality this way. TLS protects the communication between ERS and TOE. By this and the separation of roles, OE.SecOEnv is met.

The integrity of the TOE is ensured by *Docker Content Trust* and the usage of signed docker images. The integrity of the data managed by the TOE is guaranteed by the TOE itself that protects the authenticity of snapshots and log messages via the signature creation service provided by the CSP-L. Together with the reduction of the access to the TOE, docker installation and data to *SMAERS Administrator* (and *Cloud Provider*), the requirements of OE.SMAERSPlatform are met.

To implement the requirements of OE.SecUCP, again signed docker images and *Docker Content Trust* are used. This way, only images which were signed by fiskaly GmbH can be executed. In addition, the TOE itself detects up- and downgrades reliably, cf. [5].

Bibliography

[1] Federal Office for Information Security. Common Criteria Protection Profile Cryptographic Service Provider Light (CSPL), Version 1.0, BSI-CC-PP-0111-2019. https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0111.html, 12.11.2019.

[2] Federal Office for Information Security. Common Criteria Protection Profile Security Module Application for Electronic Record-keeping Systems (SMAERS), Version 1.0, BSI-CC-PP-0105-V2-2020. https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0105_0105_V2.html, 28.07.2020.

[3] Common Criteria. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1, Revision 5. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf, April 2017.

[4] fiskaly GmbH. fiskaly Security Module Application for Electronic Record-keeping Systems, Version 1.0.15 – Preparative Procedures & Operational User Guidance Documentation, Version 1.4.1, 2025.

[5] fiskaly GmbH. fiskaly Security Module Application for Electronic Record-keeping Systems, Version 1.0.15 – Security Architecture, Version 1.4.1, 2025.

Keywords

Term	Description
authentication reference data	data used by the TOE to verify the authentication attempt of a user
authentication verification data	data used by the user to authenticate themselves to the TOE
authenticity	the property that ensures that the identity of a subject or resource is the one claimed (cf. ISO/IEC 7498-2:1989)
cluster	a system of TOE samples initialized by an administrator and communication through trusted channels in order to manage known users and to share the cryptographic keys
cryptographic key	a variable parameter which is used in a cryptographic algorithm or protocol
data integrity	the property that data has not been altered or destroyed in an unauthorized manner (cf. ISO/IEC 7498-2:1989)
firmware	executable code that is stored in hardware and cannot be dynamically written or modified during execution while operating on a non-modifiable or limited execution platform, cf. ISO/IEC 19790
hardware	physical equipment or comprises the physical components used to process programs and data or to protect physically the processing components, cf. ISO/IEC 19790
Issuer of update code package	Trusted authority issuing an update code package (UCP) and holding the signature private key for signing the UCP and corresponding to the public key implemented in the TOE for verification of the UCP. The issuer is typically the TOE manufacturer. The issuer of an UCP is identified by the security attribute Issuer of the UCP.
Platform guidance	All documentation provided by the hardware manufacturer, or software platform manufacturer, that provides information on how to securely implement functionality.

private key	confidential key used for asymmetric cryptographic mechanisms like decryption of cipher text, signature-creation or authentication proof, where it is difficult for the adversary to derive the confidential private key from the known public key
public key	public known used for asymmetric cryptographic mechanisms like encryption of cipher text, signature-verification or authentication verification, where it is difficult for the adversary to derive the confidential private key from the known public key
secret key	key of symmetric cryptographic mechanisms, using two identical keys with the same secret value or two different values, where one may be easy calculated from the other one, for complementary operations like encryption / decryption, signature-creation / signature-verification, or authentication proof / authentication verification
secure channel	a trusted channel which is physically protected and logical separated communication channel between the TOE and the user, or is protected by means of cryptographic mechanisms
software	executable code that is stored on erasable media which can be dynamically written and modified during execution while operating on a modifiable execution platform, cf. ISO/IEC 19790
trusted channel	a means by which a TSF and another trusted IT product can communicate with necessary confidence (cf. CC part 1 [3], paragraph 97)
update code package	code if implemented changing the TOE implementation at the end of the TOE life time

Table 4.1: Glossary (Table 8 in Base-PP [1])

Abbreviations

Acronym	**Term**
A.xxx	Assumption
CC	Common Criteria
CSP	Cryptographic Service Provider
CSPLight	Cryptographic Service Provider Light
ECC	Elliptic curve cryptography
HMAC	Keyed-Hash Message Authentication Code
KDF	Key derivation function
MAC	Message Authentication Code
n. a.	Not applicable
O.xxx	Security objective for the TOE
OE.xxx	Security objective for the TOE environment
OSP.xxx	Organisational security policy
PACE	Password Authenticated Connection Establishment
PKI	Public key infrastructure
PP	Protection profile
SAR	Security assurance requirements
SFR	Security functional requirement
T.xxx	Threat
TOE	Target of Evaluation
TSF	TOE security functionality
UCP	update code package

Table 4.2: Abbreviations (Table 9 in Base-PP [1])