Bundesamt
für Sicherheit in der
Informationstechnik

**Konformitätsreport**

# BSI-K-TR-0403-2021

## fiskaly sign Cloud-TSE

Version 1.2.0-1.0.5

der

## fiskaly GmbH

Stutterheimstraße 16-18 / 2 / 20e, 1150 Wien, Österreich

**Bundesamt für Sicherheit in der Informationstechnik**
Godesberger Allee 185-189, D-53175 Bonn ♦ Postfach 20 03 63, D-53113 Bonn
Tel.: +49 (0)228 9582-0 ♦ Fax: +49 (0)228 9582-5400 ♦ Internet: www.bsi.bund.de

# Inhaltsverzeichnis



# Abbildungsverzeichnis

# Tabellenverzeichnis

# 1 Vorbemerkung

Die Zertifizierung von IT-Produkten oder -Systemen – im Folgenden Prüfgegenstand genannt – nach Technischen Richtlinien (TR) wird auf Veranlassung des Herstellers – im folgenden Antragsteller genannt – durchgeführt.

Technische Richtlinien, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellt und veröffentlicht werden, bilden die Grundlage für Konformitätsprüfungen. Anhand einer Konformitätsprüfung wird sichergestellt, dass ein Prüfgegenstand die technischen, funktionalen und qualitativen Anforderungen einer TR erfüllt.

Konformitätsprüfungen werden von einer vom BSI anerkannten Prüfstelle gemäß den in der jeweiligen TR definierten Prüfspezifikationen und Tests durchgeführt. Die Konformitätsprüfung eines Prüfgegenstands erfolgt in Übereinstimmung mit den Bestimmungen des entsprechenden BSI-Schemas zur Zertifizierung nach Technischen Richtlinien.

Für jedes Zertifizierungsverfahren nach TR führt das BSI eine Prüfbegleitung durch, um einheitliches Vorgehen, einheitliche Interpretation der Kriterienwerke und einheitliche Bewertungen sicherzustellen.

Das Ergebnis eines Zertifizierungsverfahrens nach TR wird in einem abschließenden Konformitätsreport zusammengefasst.

Das im Rahmen einer Zertifizierung nach TR ausgestellte Zertifikat ist keine Empfehlung des Prüfgegenstands durch das Bundesamt für Sicherheit in der Informationstechnik. Eine Gewährleistung für den Prüfgegenstand durch das BSI ist weder enthalten noch zum Ausdruck gebracht.

# 2 Grundlagen des Zertifizierungsverfahrens

Das Zertifizierungsverfahren wurde vom Bundesamt für Sicherheit in der Informationstechnik nach Maßgabe der folgenden Vorgaben durchgeführt:

- BSI-Gesetz – Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009, Bundesgesetzblatt Teil I Nr. 54, S. 2821, [BSIG]
- BSI-Zertifizierungs- und Anerkennungsverordnung – Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSIZertV), vom 17. Dezember 2014, Bundesgesetzblatt Teil I Nr. 61, S. 2231, [BSIZertV]
- Besondere Gebührenverordnung des Bundesministeriums des Inneren, für Bau und Heimat für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (Besondere Gebührenverordnung BMI, BMIBGebV) vom 02. September 2019, Bundesgesetzblatt I, S. 1359, [BMIBGebV]
- Verfahrensbeschreibung zur Zertifizierung von Produkten, Version 2.5 vom 19. März 2020, [VB-Produkte]
- Anforderungen an Antragsteller zur Zertifizierung von Produkten nach Technischen Richtlinien, Version 1.4 vom 17. Oktober 2019, [TR-Produkte]

# 3 Hinweise für den Antragsteller

1. Das vom BSI erteilte Zertifikat nach Technischen Richtlinien BSI-K-TR-0403-2021 ist nur in Zusammenhang mit dem vollständigen Konformitätsreport gültig.
2. Die Gültigkeit des Zertifikats erstreckt sich ausschließlich auf die geprüfte Version des Prüfgegenstands. Alle geprüften Komponenten des Prüfgegenstands und deren Versionsstände sind in Tabelle 1 des Konformitätsreports festgeschrieben.
3. Die reguläre Gültigkeit eines Zertifikats nach der Technischen Richtlinie BSI TR-03153 beträgt acht Jahre.
4. Bei Änderungen, Weiterentwicklungen oder Ergänzungen der Komponenten des Prüfgegenstands um zusätzliche Versionen hat das BSI, ggf. unter Einbeziehung der Prüfstelle, zu beurteilen, ob das Zertifikat entsprechend erweitert werden kann oder ob eine erneute Konformitätsprüfung notwendig ist.
5. Nur dem Zertifikat entsprechende Ausführungen des Prüfgegenstands dürfen als vom BSI zertifiziert bezeichnet und als solche beworben werden. Stellt das BSI diesbezüglich eine Zuwiderhandlung fest, erfolgt eine Abmahnung des Antragstellers. Daneben ist das BSI berechtigt, den Eintrag des Prüfgegenstands von der Veröffentlichungsliste der nach Technischen Richtlinien erteilten Zertifikate auf der BSI-Webseite zu streichen.
6. Das BSI kann den Antragsteller jederzeit auffordern, ein dem Zertifikat entsprechendes Exemplar des Prüfgegenstands aus der laufenden Produktion zur Überprüfung bereitzustellen. Kommt der Antragsteller der Aufforderung nicht innerhalb einer gesetzten Frist nach, ist das BSI berechtigt, den Eintrag des Prüfgegenstands von der Veröffentlichungsliste der nach Technischen Richtlinien erteilten Zertifikate auf der BSI-Webseite zu streichen.

# 4 Antrag

Für den in Kapitel 7 genannten Prüfgegenstand wurde vom Hersteller

**fiskaly GmbH**
Stutterheimstraße 16-18 / 2 / 20e
1150 Wien

Österreich

Ansprechpartner:

Dr. Patrick Gaubatz (patrick.gaubatz@fiskaly.com)

mit Antragsdatum 01. April 2020 (Eingangsdatum BSI: 06. April 2020) beim BSI eine Zertifizierung nach Technischen Richtlinien beantragt.

# 5 Prüfbereich und Prüfgrundlage

Beantragt wurde eine Zertifizierung nach der Technischen Richtlinie:

> **BSI TR-03153** – Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme

Die Konformitätsprüfung nach der Technischen Richtlinie BSI TR-03153 erfolgte für den Prüfbereich:

> **BSI TR-03153** – Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme

Die Prüfgrundlage für Konformitätsprüfungen in diesen Prüfbereichen bildeten folgende Dokumente:

> **BSI TR-03153** – Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, Version 1.0.1 vom 20. Dezember 2018, [BSI TR-03153]
>
> **Ergänzungen der BSI TR-03153** vom 02. Dezember 2019, [BSI TR-03153-ERG]
>
> **Klarstellungen und Anwendungshinweise zur BSI TR-03153 und BSI-CC-PP-0105-V2-2020** vom 13. November 2020, [BSI TR-03153-KuA]
>
> **BSI TR-03153-TS** – Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme – Testspezifikation, Version 1.0.1 vom 05. Februar 2019, [BSI TR-03153-TS]
>
> **Ergänzungen der BSI TR-03153-TS** vom 02. Dezember 2019, [BSI TR-03153-TS-ERG]
>
> **Klarstellungen und Anwendungshinweise zur BSI TR-03153-TS und BSI-CC-PP-0105-V2-2020** vom 13. November 2020, [BSI TR-03153-TS-KuA]
>
> **BSI TR-03151** – Secure Element API (SE API), Version 1.0.1 vom 20. Dezember 2018, [BSI TR-03151]
>
> **Amendment to BSI TR-03151** Secure Element API (SE API) vom 02. Dezember 2019, [BSI TR-03151-AMT]
>
> **BSI TR-03116-5** – Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 5: Anwendungen der Secure Element API, Stand 2019 vom 01. Februar 2019, [BSI TR-03116-5]
>
> **PP_SMAERS** – Common Criteria Protection Profile – Security Module Application for Electronic Record-keeping Systems (SMAERS), BSI-CC-PP-0105-V2-2020, Version 1.0, [PP_SMAERS]
>
> **PP_CSPL** – Common Criteria Protection Profile – Cryptographic Service Provider (CSP) Light, BSI-CC-PP-0111-2019, Version 1.0, [PP-CSPL]

# 6 Prüfstelle

Mit der Durchführung der Konformitätsprüfung wurde folgende, vom BSI gemäß DIN ISO/IEC 17025 anerkannte Prüfstelle beauftragt:

*Prüfbereich: BSI TR-03153*

**SRC Security Research & Consulting GmbH**
Emil-Nolde-Str. 7

53113 Bonn
Deutschland

# 7 Prüfgegenstand

## 7.1 Beschreibung des Prüfgegenstands

Prüfgegenstand ist das IT-Produkt/-System:

**fiskaly sign Cloud-TSE**, Version 1.2.0-1.0.5

Bei dem Prüfgegenstand handelt es sich um eine softwarebasierte Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme gemäß Kassensicherungsverordnung [KassenSichV].

Der Prüfgegenstands besteht aus den folgenden Teilkomponenten:

- **TSE-Host**, bestehend aus
  - Security Module Application for Electronic Record-keeping Systems (SMAERS) und
  - Speichermedium
- **Crypto Service Provider Light** (CSP-L)

CSP-L wurde nach dem CC Schutzprofil [PP-CSPL] evaluiert (BSI-DSZ-CC-1153-2021).

SMAERS wurde nach dem CC Schutzprofil [PP_SMAERS] zertifiziert (BSI-DSZ-CC-1130-2021).

SMAERS und CSP-L bilden das Sicherheitsmodul der TSE, wobei das Sicherheitsmodul zweigeteilt ist, mit einem fernverbundenen CSP, das Bestandteil mehrerer TSEs sein kann, und einem SMAERS, das sich auf dem selben Host wie das Speichermedium befindet.

Die Kommunikation zwischen CSP-L und SMAERS findet über einen Trusted Channel statt. Es handelt sich hierbei um einen PACE-gesicherten Kanal.

Das Elektronische Aufzeichnungssystem (ERS) kommuniziert mit der TSE über die in [BSI TR-03151] und [BSI TR-03151-AMT] spezifizierte Einbindungsschnittstelle (Secure Element API, SE-API) mittels TLS-Verbindung. Die SE-API ist in das SMAERS integriert.

Zur Registrierung einer neuen TSE und der damit verbundenen Schlüsselerzeugung kann auf das CSP-L mit einem Admin-Tool zugegriffen werden. Die Verbindungen zwischen SMAERS und CSP-L, zwischen PKI und Admin-Tool, zwischen ERS und TSE und zwischen CSP-L und NTP-Server erfolgen über das Internet. Die Übertragung der Bootstrap-Datei vom Admin-Tool in die TSE erfolgt über ein Speichermedium.

Im den Kapiteln 7.1.1 – 7.1.7 werden die einzelnen Teilkomponenten näher beschrieben.

### 7.1.1 Elektronisches Aufzeichnungssystem

Eine TSE ist an ein oder mehrere Elektronische Aufzeichnungssysteme (ERS) in Form von Registrierkassen angeschlossen. Das ERS ist nicht Teil des Prüfgegenstands und wurde im Rahmen der Konformitätsprüfung von einem Testsystem simuliert.

Ein ERS kommuniziert über die Einbindungsschnittstelle mit dem SMAERS. Ein ERS darf nur an exakt ein SMAERS angebunden sein. Es können bis zu 200 elektronische ERS auf eine TSE

zugreifen, die Unterscheidung erfolgt über die Client-ID, die einem Aufzeichungssystem eindeutig zugewiesen wird [fiskaly-AGD].

### 7.1.2 TSE-Host

Das Host-System für die TSE (ohne CSP) kann eine reguläre PC-Hardware sein oder eine virtuelle Hosting-Umgebung (Cloud). Es beherbergt eine Installation des SMAERS. Abhängig von der Speicherkapazität des Host-Systems kann dem Speichermedium Speicherkapazität zur Verfügung gestellt werden.

System-Voraussetzungen für das Host-System:

- Cloud:
  - Amazon AWS: EC2-Instanz, AWS-Region Frankfurt, Ubuntu 20.04 LTS, 64 bit, EBS-Verschlüsselung für den Speicher und Root-Laufwerk
  - Google Cloud Platform: Google Compute Engine, Region Frankfurt, Ubuntu 20.04 LTS, Standard Storage (standardmäßig verschlüsselt), OS-Login mit 2-Step-Verifikation
  - Microsoft Azure: Azure Virtual Machine, Region „Germany West Central“, Ubuntu 20.04 LTS, Azure managed disks (Verschlüsselung mit AES-256)
- PC-Hardware:
  - Ubuntu 20.04 LTS, UEFI Secure Boot, Festplattenverschlüsselung mit TPM2, MTBF ≥ 1.000.000 h (oder RAID für Redundanz, falls MTBF nicht erreicht wer-den kann)
- Cloud & PC-Hardware:
  - Vollständige Festplattenverschlüsselung
  - Docker-Installation
  - UFW-Firewall
  - nginx als Reverse-Proxy für TLS, nur TLS 1.2 und 1.3 mit in [TR-2102-2] empfohlenen Cipher-Suiten erlaubt
  - TLS-Zertifikat

Zusätzliche System-Voraussetzung für die Docker-Installation:

- 100 MB freien RAM
- Netzwerkkonnektivität

### 7.1.3 Einbindungsschnittstelle und SMAERS

Da die Einbindungsschnittstelle in das SMAERS integriert ist, wird im Folgenden nur vom SMAERS gesprochen, wenn nicht explizit auf die Einbindungsschnittstelle eingegangen wird.

Gegenstand:

fiskaly Secure Module Application for Electronic Record-keeping Systems, v1.0.5

Bereitstellung über die Docker-Registry:

- docker.fiskaly.com/fiskaly/smaers:1.0.5
  sha256: 5b961395357dab135dc0f9036cb750868c2c00e3f0299405f084147f214ddd95

Der Docker-Container hat den folgenden Inhalt:

- Alpine Linux 3.12.3 Operating System
- Binary: smaers-linux-amd64
  sha256: 99d1dc7adc6c94808ddc27ee86db9870326a77fc27d68beb1f702b64ebc65abf
- Installation von Minisign v0.9
- Volumes „Storage“ (Speichermedium) und „Secure Storage“ (interner Speicher des SMAERS) (siehe Kapitel 7.1.5)

Das verwendete SMAERS wurde nach dem CC Schutzprofil [PP_SMAERS] zertifiziert (BSI-DSZ-CC-1130-2021).

Das SMAERS wird über einen Docker-Container lokal auf einem System oder in einer Cloud installiert. Das verwendete DockerImage ist für die Installation auf Hardware und in der Cloud identisch. Das Docker-Image enthält die Software für die Einbindungsschnittstelle und das SMAERS. Eine Beschreibung zur Installa-tion des Docker-Image findet sich in [fiskaly-AGD] Kapitel 3.1.

Das SMAERS verfügt über einen internen Speicher (Secure Storage). Im Secure Storage werden die folgenden Daten gespeichert:

- das Signatur- und die zugehörigen CA-Zertifikate
- PACE-PIN - Referenz-Hashes für Administrator-Passwörter
- Informiationen zur Verbindung zum CSP-L
- Erwarteter Signaturzähler des CSP-L

Der erweiterte Signaturzähler des CSP-L wird im Secure Storage vorgehalten, so dass im Falle einer Kommunikationsstörung das SMAERS eigenständig feststellen kann, ob eine Anwort vom CSP-L verpasst wurde. Damit kann das SMAERS bei verpasster Nachricht diese erneut abrufen und ist in der Lage sich synchron mit dem CSP-L zu halten.

Desweiteren wird eine Teilmenge der Log-Dateien im Secure Storage vorgehalten, bis diese mit einem Snapshot zusammengefasst werden. Dies sind immer die aktuellsten Log-Dateien, die zusätzlich zur Speicherung im Speichermedium im Secure Storage abgelegt werden. Ein Snapshot dient hierbei dazu, den aktuellen Zustand des SMAERS zu sichern. Snapshots werden ebenfalls im Secure Storage gesichert. Der Secure Storage teilt sich den Speicherplatz mit dem Speichermedium. Für den Secure Storage werden hiervon wenige MB beansprucht [fiskaly-ARC].

Das SMAERS stellt dem CSP-L sämtliche zu signierenden Daten zur Verfügung und sorgt für die Speicherung der signierten Log-Dateien im Speichermedium. Details zur Speicherung sind in Kapitel 7.1.5 zu finden. Es ist genau einem CSP-L zugeordnet. Diese Zuordnung erfolgt

durch die Personalisierung mit einem sogenannten Bootstrap-File, das vom Admin-Tool erstellt wird.

Ein Bootstrap-File enthält hierbei die folgenden Informationen:

- eine initiale Datenbank für den Secure Storage, die die folgenden Informationen enthält:
  - PACE-PIN
  - Informationen zur Verbindung zum CSP-L
  - Hash-Werte der initialen Authentifikationsdaten für SMAERS-Administrator und TR-Administrator
  - Das Signatur-Zertifikat sowie die zugehörigen CA-Zertifikate
- eine initiale Datenbank für das Speichermedium
- Seed für den Zufallszahlengenerator

Ein SMAERS führt exakt einen Transaktionszähler und ist daher Bestandteil von exakt einer TSE. Dieser wird im RAM gehalten und inkrementiert, wenn eine neue Transaktion gestartet wird. Beim Starten des SMAERS rekonstruiert es den Transaktionszähler aus den in der Datenbank des Secure-Storage gespeicherten Log-Dateien und Snapshots.

Die Einbindungsschnittstelle wird über eine Remote Procedure Call (RPC) basierte API angesprochen. Ein RPC-Request wird an einen HTTP-Endpunkt der Einbindungsschnittstelle gesendet, die mit einem RPC-Response antwortet. Die Einbindungsschnittstelle agiert hier als Server. Die Daten einer Anfrage und einer Antwort werden als Protocol Buffers gesendet.

In [fiskaly-AGD] werden für das SMAERS die folgenden Rollen definiert, die verschiedene Funktionen ausführen dürfen:

- SMAERS Administrator: Administrator des SMAERS, kann weitere Benutzer, insbesondere TR Administratoren anlegen. Wird über die Funktion login_admin (siehe Abschnitt 1.1.3) authentifiziert.
- TR Administrator: Administrator gemäß [BSI TR-03151] Kapitel 4.2, kann die Funktionen Initialize, DisableSecureElement und DeleteStoredData ausführen. Wird über die Funktion authenticate_user (entspricht AuthenticateUser gemäß [BSI TR-03151]) authentifiziert.
- CTSS Interface: Benutzer dieser Rolle können Transaktionsdaten übermitteln und entsprechend Transaktionen starten, aktualisieren oder beenden. Sie werden über ihre Client-ID identifiziert.

Die Einbindungsschnittstelle orientiert sich an der SE-API gemäß [BSI TR-03151], weicht aber im Funktionsumfang ab. Die folgenden Funktionen werden nicht unterstützt:

- **updateTime**: Gemäß [BSI TR-03153-KuA] wird die Funktion zwar angeboten, führt aber zu dem Fehler „ErrorFunctionNotSupported“.

Folgende gemäß [BSI TR-03151] optionalen Funktionen werden angeboten:

- **delete_stored_data**: entspricht deleteStoredData gemäß [BSI TR-03151]

Folgende gemäß [BSI TR-03151] verpflichtenden Funktionen werden modifiziert angeboten:

- **export_data** (entspricht exportData): unterstützt zusätzlich die Möglichkeit, Daten auf mehrere Teilexporte (Chunks) aufgeteilt zu exportieren. Die Größe dieser Chunks kann angegeben werden. Wird die Funktion ohne Angabe der Chunk-Größe aufgerufen und sind mehr als 10 MB (Standard-Chunk-Größe) Daten zu exportieren, wird nur der erste Chunk exportiert und die Funktion muss unter Angabe der nächsten Chunk-Nummer erneut aufgerufen werden. Die Chunk-Größe wird über den Parameter chunk_size, die Chunk-Nummer über chunk_number angegeben. Die verbleibende Anzahl an Chunks wird in der Antwort angebeben. Ein komplettes TAR-File muss über die Konkatenation der einzelnen Chunks gebildet werden.

Folgende Funktionen werden zusätzlich angeboten:

- **add_client**: Fügt einen Client für die Durchführung von Transaktionen einer TSE hinzu. Ein Client wird über seine Client-ID identifiziert und repräsentiert ein ERS. Ein Client hat die Rolle „CTSS Interface“
- **remove_client**: Entfernt einen Client für die Durchführung von Transaktionen aus der TSE.
- **self_test**: führt einen Selbsttest durch. Schlägt der Selbsttest fehl, wird ein System-Log vom Typ „selfTest“ erstellt und das System geht in den Status „Secure State“ mit entsprechendem System-Log über, den es erst nach einem erfolgreichen Selbsttest wieder verlässt.
- **identify_ers**: Identifiziert das aufrufende ERS anhand seiner Client-ID.
- **get_status**: liefert den Status der TSE zurück. Dies beinhaltet die Version, die registrierten Clients sowie die offenen Transaktionen, repräsentiert durch deren Transaktionsnummern.
- **personalize**: übergibt die vom CSP-L bei der Registrierung einer neuen TSE erstellte Bootstrap-Datei dem SMAERS. Das SMAERS erhält so die benötigten Zertifikate und Konfigurationen für die Kommunikation mit dem CSP.
- **admin_login**: authentifiziert den SMAERS-Administrator und löst die Erstellung eines System-Logs vom Typ authenticateSmaersAdmin aus.
- **admin_logout**: loggt den SMAERS-Administrator aus.
- **admin_update_password**: ermöglicht den Passwortwechsel des SMAERS-Administrators. Der Aufruf dieser Funktion löst ebenfalls das Schreiben eines System-Logs des Typs authenticateSmaersAdmin aus.
- **admin_set_config**: über diese Funktion können einzelne Konfigurationsparameter gesetzt bzw. geändert werden. Mögliche Parameter sind: pin_length (minimale PIN-Länge eines TR-Administrators), password_length (minimale Länge eines SMAERS-Administrator-Passwort), max_test_interval, min_test_interval, test_interval (maximales, minmales bzw. reguläres Intervall zwischen automatisch ausgelösten Self-Tests)
- **add_user**: Registriert einen neuen Benutzer in der Rolle TR-Admin. Der aufrufende Benutzer muss ein SMAERS-Administrator sein.

- **remove_user**: Entfernt einen Benutzer in der Rolle TR-Admin.
- **set_config**: Setzt einen oder mehrere Konfigurationsparameter. Mögliche Parameter sind: http_proxy (Proxy für ausgehende HTTP(S)-Verbindungen zum CSP), http_timeout (Timeout einer Anfrage an das CSP).
- **cancel_export**: Im Falle von großen Datenmengen beim Export kann es zu einer Instabilität in der Übertragung per HTTP kommen. Es kann daher optional bei exportData angegeben werden, dass die Daten gestückelt übertragen werden. Während eines ge-stückelten Exports kann aber kein weiterer gestartet werden. Daher wird mit cancelEx-port eine Funktion zur Verfügung gestellt, einen gestückelten Export zu unterbrechen.
- **finish_export**: Jeder exportData-Aufruf muss mit finish_export beendet werden. Erst dann werden die Daten zum Löschen freigegeben.
- **shutdown**: Löst einen sauberen Shutdown des SMAERS aus.

### 7.1.4 CSP-L

Das CSP-L ist Teil des Sicherheitsmoduls der TSE. Es wird als Java-Programm in einer virtuellen Maschine mit einem Alpine Linux Betriebssystem ausgeführt. Die virtuelle Maschine ist auf einer PrimeKey-Hardware installiert, welche sich im Rechenzentrum der fiskaly GmbH befindet.

Gegenstand:

fiskaly Cloud Crypto Service Provider v1.2.0 (cspl.jar)
sha256: 0a08589c000eecb89121c3e055bd65a69f278762dcfa65118ffbffff72a36b80)

System-Voraussetzung an die Hardware:

- PrimeKey SEE:
  - 4-core Xeon 3,6 GHz
  - bis zu 64GB RAM
  - Redundante, vor Ort austauschbare Stromversorgung
  - 500 GB Speicher
  - 4 x GB Ethernet
  - Out-of-band Management
  - Zertifizierungen: FIPS 140-2 Level 3, FCC, CE
  - Secure Boot o Nicht-deterministischer Zufallszahlengenerator (Hardware erfüllt NIST SP-800)
- Betrieb einer Virtuellen Maschine

System-Voraussetzungen an die Virtuelle Maschine:

- Betriebssystem: Alpine Linux 3.12.0, Kernel 5.4.72-0-virt auf einer x86-64 Architektur
- OpenJDK v11.0.9+11-alpine-r0

- PostgreSQL v12.5
- chrony v3.5.1

Der verwendete CSP-L ist gemäß [PP-CSPL] evaluiert. Die Hardware-Umgebung von PrimeKey befindet sich im Rechenzentrum der fiskaly GmbH. Damit liegen CSP-L und das SMAERS nicht auf dem selben System.

Zwischen SMAERS und CSP-L besteht eine Client-Server-Verbindung über einen Trusted Channel (PACE), bei der der CSP-L die Server-Rolle einnimmt. Der CSP-L unterstützt die Verwendung von mehreren SMAERS. Hierbei bildet jede Kombination von einem SMAERS und einem CSP-L eine eigenständige TSE im Sinne der [BSI TR-03153]. Soll eine neue TSE angelegt werden, wird der CSP-L über eine Schnittstelle angesprochen, so dass ein neues Schlüsselpaar generiert wird. Hierbei wird eine neue CSP-Einheit mit neuem Signaturzähler angelegt. Den öffentlichen Schlüssel liefert der CSP-L zurück, damit dieser in ein CSR eingebaut werden kann. Das fertige CSR wird dann vom CSP-L signiert, bevor es an die PKI gesendet wird. Hierbei wird der neu erzeugte Signaturschlüssel das erste Mal verwendet. Da es für diesen Vorgang keine definierte Log-Nachricht gibt, [BSI TR-03153-KuA] jedoch das Erstellen von herstellerspezifischen Log-Dateien untersagt, wird kein entsprechen-des Log für diese Vewendung an das SMAERS geliefert und mit exportData() exportiert. Aus diesem Grund startet das erste exportierte Log immer mit einem Signaturzähler von 2. Um höhere Signaturzähler auszuschliessen, die etwa durch Kommunikationsprobleme im Prozess der Zertifikatsbeantragung zustande kommen können, muss entsprechend den Herstelleranweisungen verfahren werden. Es muss mittels eines Skriptes geprüft werden, dass der Signaturzähler nach erstellen einer Bootstrap-Datei den Wert 1 nicht übersteigt. Ansonsten wird die Bootstrap-Datei gelöscht.

Der private Schlüssel verlässt den CSP-L nie. Sobald der CSP-L eine neue CSP-Einheit mit zugehörigem Schlüssel angelegt hat, erstellt es signierte Log-Dateien für Audit-Events.

Für die Kommunikation mit dem CSP-L zur Erstellung des Schlüssels einer neuen TSE stellt die fiskaly GmbH eine Software („Admin-Tool“) zur Verfügung. In Kapitel 7.1.6 wird das Admin-Tool näher beschrieben.

### 7.1.5 Speichermedium

Das Speichermedium ist teil desselben Host-Systems wie das SMAERS und wird als Docker-Volume für den Docker-Container des SMAERS eingerichtet. Über das Bootstrap-File wird im Rahmen der Personalisierung eine initiale Datenbank für das Speichermedium importiert.

Das Speichermedium enthält die folgenden Daten:

- Beschreibung der TSE
- signierte Log-Dateien, die während des Betriebs der TSE anfallen

Die Speicherkapazität ist abhängig vom verwendeten System. Die Docker-Volumes haben keine vordefinierte Größe und skalieren mit ihrem Inhalt, solange Speicherkapazität auf dem Host-System vorhanden ist. Angaben zu den genaueren Mindestkapazitäten finden sich in [fiskaly-ARC]. Für den Betrieb einer TSE in einer lokalen Umgebung wird empfohlen, mindestens 16 GB für das Speichermedium zu reservieren. Läuft die TSE in einer Cloud-Umgebung, kann der Speicherplatz nach Bedarf vergrößert werden. In [fiskaly-AGD] gibt der

Hersteller an, dass pro vorhandenem Gigabyte Speicherkapazität bei einer mittleren Log-Größe von 512 Byte über 2 Millionen Log-Nachrichten gespeichert werden können.

### 7.1.6 Admin-Tool

Das Admin-Tool ist eine adminstrative Anwendung, die durch die fiskaly GmbH entwickelt wurde und dient als Hilfsmittel zur Einrichtung von TSEn (siehe auch [fiskaly-ARC]).

Gegenstand: fiskaly Admin-Tool, v1.1.1; Bereitstellung über die Docker-Registry:

- docker.fiskaly.com/fiskaly/admin-tool:1.1.1
  c4d154875c9df3eefb40862a1d1920b0924d1f0935678af6786fd0a0d0d0c05b

Der Docker-Container hat den folgenden Inhalt:

- Alpine Linux 3.12.3 Operating System
- Binary: admin-tool, sha256:
  b5a1705447c3e9278c458eda7534eeb9d9a8cf5b84b975918e2a67b1f3a37803

System-Anforderungen: Für das Admin-Tool gibt es keine konkreten Anforderungen an das Betriebssstem. Es muss jedoch die Voraussetzungen für eine Installation von Docker erfüllen. Diese sind abhängig vom Betriebssystem:

- MacOS: Version 10.14 oder höher, mindestens 4GB RAM, keine Installation von VirtualBox mit Version kleiner 4.3.30
- Windows:
  - Windows 10 64-bit
    - mit Hyper-V: Pro, Enterprise oder Education (Build 17134 oder höher)
    - WSL 2 Backend: Home, Pro, Enterprise oder Education, version 1903 (Build 18362 oder höher), Linux Kernel Upgrade Package
  - 4GB RAM
  - BIOS-level Hardware Virtualisierungsunterstützung aktiviert in BIOS Einstellungen
- Linux: 64-bit Architekturen
  - Unterstützte Distributionen:
    - CentOS: Version 7 oder 8, centos-extra Repository aktiviert
    - Debian / Raspbian: Debian-Buster 10, Debian Stretch 9 / Raspbian Stretch; x86_64, amd64, armhf oder arm64 Architektur
    - Fedora: Fedora 32 oder Fedora 33
    - Ubuntu: 20.10, 20.04, 18.04 oder 16.04 und zugehörige Derivate; x86_64, amd64, armhf oder arm64 Architektur

Außerdem benötigt es 100 MB freien RAM und Netzwerkkonnektivität.

Es wird über eine HTTP-basierte REST-Schnittstelle angesprochen. Im produktiven Einsatz bietet es nur den folgenden Endpunkt an:

- /bootstrap: Über das Admin-Tool kann ein Aufzeichnungssystem bei einem CSP-L die Vorbedingungen anfragen, um eine neue SMAERS-Instanz und damit eine neue TSE anlegen zu können. Das Admin-Tool stößt die Generierung eines neuen Schlüsselpaars beim CSP-L an, erstellt mit dem öffentlichen Schlüssel ein CSR und sendet die-ses an die PKI. Das zurückgelieferte signierte Zertifikat fügt es zusammen mit einem neu angelegten Benutzer für die SMAERS-Instanz in eine Bootstrap-Datei ein. Diese Bootstrap-Datei wird anschließend verwendet, um das SMAERS zu personalisieren. Desweiteren werden über diesen Endpunkt Benutzer-IDs der Rolle „TR-Administrator“ (entspricht der Rolle „Admin“ aus [BSI TR-03151]) übergeben. Die Antwort enthält neben der Bootstrap-Datei auch die Credentials für diese Benutzer, wie sie in der TSE konfiguriert werden.

Im Rahmen der TR-Prüfung wurde ein erweitertes Admin-Tool mit zusätzlichen Funktionen zur Kommunikation mit dem CSP-L zur Verfügung gestellt, die im produktiven Betrieb nicht ver-fügbar sind. Hierbei bleibt das CSP-L unverändert. Das Admin-Tool spricht nur Schnittstellen an, die das CSP-L regulär zur Verfügung stellt. Die folgenden Funktionen sind zusätzlich ver-fügbar:

- Erstellung von fehlerhaften Bootstrap-Dateien. Die Fehler können das folgende Ausmaß haben:
  - Falsche PACE-PIN, sodass sich das SMAERS nicht mit dem CSP-L verbinden kann (wird im Rahmen der TR-Prüfung nicht verwendet).
  - Abgelaufenes CTSS-Zertifikat, sodass Tests mit abgelaufenem Zertifikat durchgeführt werden können.
  - Erzeugung von Test-Zertifikaten, die von der PKI signiert werden.
  - Gültiges Standard-Zertifikat, das keinen neu erzeugten Signatur-Schlüssel enthält
  - Erstellung von durch das Admin-Tool zertifizierten Zertifikaten.
- Zusätzliche Endpunkte der HTTP-basierten REST-Schnittstelle:
  - /time: Dieser Endpunkt erlaubt es, obwohl die updateTime-Funktionalität über die Einbindungsschnittstelle nicht unterstützt wird (ErrorFunctionNotSupported), direkt die Zeit des CSP-L zu verändern. Hierbei kann entweder eine außerordentliche Aktualisierung mit dem NTP-Server provoziert werden oder direkt ein neuer Zeitstempel übergeben werden. Die außerordentliche Aktualisierung der Zeit läuft hierbei exakt so ab wie die automatische Aktualisierung, mit dem Unterschied, dass sie von außen angestoßen wird. Dieser Endpunkt ist hilfreich, wenn UpdateTime im Ablauf durchgeführt werden soll, der Log-Inhalt aber nicht relevant ist. In letzterem Fall muss ein automatisches Update-Time abgewartet werden.
  - /audit: Dieser Endpunkt erlaubt es, in der Rolle „Auditor“ Audit-Records zu erstellen und somit die Erstellung von Audit-Logs zu triggern. Dieser Endpunkt ist hilfreich, wenn im Ablauf ein Audit-Log gefordert wird, der Inhalt und das Zustandekommen aber nicht relevant ist. Andernfalls muss über den Endpunkt /ucp ein echtes Audit-Event ausgelöst werden, für das ein Audit-Log erstellt wird.

- /ucp: Dieser Endpunkt erlaubt es, im CSP-L ein Update einzuspielen, durch das ein UCP-Audit-Event ausgelöst wird. Dieses Audit-Event wird als Audit-Log an die TSE ausgeliefert.
- /version: Dieser Endpunkt erlaubt es, die Version des CSP-L auszulesen.

Das Admin-Tool wird über ein System, das im selben Netzwerk wie das CSP-L liegt, bedient. Es ist nicht von außen zugänglich und kann im produktiven Einsatz nur von einem Mitarbeiter der fiskaly GmbH benutzt werden. Insbesondere bedeutet das, dass eine neue TSE nur von einem Mitarbeiter der fiskaly GmbH registriert werden kann.

Eine Beschreibung des Admin-Tools mit verbindlichen Hinweisen zum Produktivbetrieb findet sich in [AdminT_Man]. Zudem wird ein Skript zum Überprüfen des Signaturzählers nach Er-zeugen einer Bootstrap-Datei zur Verfügung gestellt (check-key-usage-counter.sh, sha256: 0df2a98566aff02caec43006011ef5b59418749adc4e7190a5be5acc9c6d5e60).

### 7.1.7 PKI

Die PKI dient ausschließlich zum Ausstellen gültiger Zertifikate. Hierzu signiert sie den vom Admin-Tool generierten CSR. Es gibt hierbei eine Test-PKI für Test-Zertifikate und eine Wirk-PKI für Produktiv-Zertifikate.

Produktiv-Zertifikate können nur über das Admin-Tool in den Räumlichkeiten der fiskaly GmbH beantragt werden, da hierzu ein geschützter Kanal zur Wirk-PKI verwendet wird. In der TR-Prüfung verwendete Produktiv-Zertifikate werden nach Beendigung der Prüfung zurückgezogen.

Die Beantragung von Zertifikaten über eine PKI liegt außerhalt des Fokus der TR-Konformitätsprüfung. Damit beschränkt sich der Einfluss der PKI auf den Prüfgegenstand auf die Gültigkeit und Art ihrer Zertifizierung. Für die PKI liegt ein Zertifikat gemäß [BSI TR-03145] vor (BSI-K-TR-0478-2021, siehe Kapitel 7.3).

## 7.2 Komponenten des Prüfgegenstands

Die einzelnen Komponenten des Prüfgegenstands sowie deren zertifizierte Versionsstände sind in Tabelle 1 festgeschrieben.

*Tabelle 1: Komponenten des Prüfgegenstands*

| Fiskaly sign Cloud-TSE v1.2.0-1.0.5 | | | |
|---|---|---|---|
| **Nr** | **Typ** | **Identifier** | **Bemerkung** |
| 1 | SW | docker.fiskaly.com/fiskaly/smaers:1.0.5 | SHA-256 Hash 5b961395357dab135dc0f9036cb750868c2c00e3f0299405f084147f214ddd95<br>SMAERS-Binary: smaers-linux-amd64, sha256: 99d1dc7adc6c94808ddc27ee86db9870326a77fc27d68beb1f702b64ebc65abf<br>Siehe Kapitel 7.1.3 |
| 2 | SW | fiskaly Cloud Crypto Service Provider v1.2.0 | SHA-256 Hash |

| | | | |
|---|---|---|---|
| | | (cspl.jar) | 0a08589c000eecb89121c3e055bd65a69f27876 2dcfa65118ffbffff72a36b80<br>Siehe Kapitel 7.1.4 |
| 3 | SW | docker.fiskaly.com/fiskaly/admin-tool:1.1.1 | SHA-256 Hash c4d154875c9df3eefb40862a1d1920b0924d1f09 35678af6786fd0a0d0d0c05b<br>Binary: admin-tool, sha256: b5a1705447c3e9278c458eda7534eeb9d9a8cf5 b84b975918e2a67b1f3a37803<br>Siehe Kapitel 7.1.6 |

## 7.3 Mitgeltende Zertifizierungen

Für die vom Prüfgegenstand genutzte PKI existiert folgende mitgeltende Zertifizierung:

BSI TR-03145
Zertifikat BSI-K-TR-478-2021 vom 26.05.2021
Sub-CA Services der DARZ GmbH
gültig bis 25. Mai 2024

Hinweis: Die Gültigkeit der Zertifizierung des Prüfgegenstands ist abhängig von der Gültigkeit der mitgeltenden Zertifizierungn. Verliert diese ihre Gültigkeit, wird damit auch das Zertifikat des Prüfgegenstands (BSI-K-TR-0403-2021) ungültig.

Der Antragsteller ist verpflichtet, das BSI über Änderungen an mitgeltenden Zertifizierungen (z. B. Gültigkeitsverlust, Änderung der Zertifizierungs-ID aufgrund von Re-Zertifizierungen, ...) unaufgefordert zu informieren.

## 7.4 Implementation Conformance Statement

Das Implementation Conformance Statement (ICS) enthält die für die Durchführung der Konformitätsprüfung benötigten Informationen zum Prüfgegenstand und gibt Aufschluss über dessen Funktionalität bzw. die vom Prüfgegenstand umgesetzten elektronischen Sicherheitsmechanismen.

Die nachfolgenden Tabellen enthalten das ICS zum Prüfgegenstand für die Konformitätsprüfung gemäß [BSI TR-03153-TS].

*Tabelle 2: Unterstützte Profile*

| **Die TSE...** | **Profile ID** | **Supported** (Yes/No) |
|---|---|---|
| Speichermedium-Profile | | |
| verfügt über ein Speichermedium | STORAGE_BASIC | Yes |
| hat ein fernverbundenes Speichermedium | STORAGE_REMOTE | No |
| Sicherheitsmodul-Profile | | |
| verfügt über ein Sicherheitsmodul | SM_BASIC | Yes |
| signiert Aktualisierungen (Updates) direkt und aggregiert diese nicht | SM_NOAGG | Yes |
| aggregiert Aktualisierungen (Updates) und sichert diese zusammengefasst ab (signiert) | SM_AGG | No |
| kann mehrere Transaktionen parallel verwalten | SM_MULTI | Yes |
| hat ein fernverbundenes Sicherheitsmodul | SM_REMOTE | Yes |
| Schnittstellen-Profile | | |
| implementiert alle Funktionen der Einheitlichen Digitalen Schnittstelle gemäß BSI TR-03153 | SDI | No |
| implementiert die optionale Funktion restoreFromBackup der Einheitlichen Digitalen Schnittstelle gemäß BSI TR-03153 | SDI_RESTORE | No |
| implementiert die empfohlene Funktion deleteStoredData der Einheitlichen Digitalen Schnittstelle gemäß BSI TR-03153 | SDI_DELETE | Yes |
| verfügt über einen Mechanismus zum eigenständigen Stellen der Zeit des Sicherheitsmoduls | TIME_SYNC | Yes |
| verfügt über keinen Mechanismus zum eigenständigen Stellen der Zeit des Sicherheitsmoduls | NO_TIME_SYNC | No |
| besitzt eine herstellerspezifische Einbindungsschnittstelle und setzt den Export-Teil der Einheitlichen Digitalen Schnittstelle um | CUSTOM_INTEGRATION_INTERFACE | Yes |
| kann von mehreren Clients gleichzeitig für die Protokollierung von | MULTI_CLIENT | Yes |

| | | |
|---|---|---|
| Transaktionen verwendet werden | | |
| kann zu einem Zeitpunkt nur von einem Client für die Protokollierung von Transaktionen verwendet werden | NO_MULTI_CLIENT | No |

*Tabelle 3: Verwendeter Signaturalgorithmus*

| Verwendete Kryptofunktionen | Angaben des Antragstellers |
|---|---|
| Signaturalgorithmus | ECDSA-plain-sha256 |
| Parameter zum Signaturalgorithmus (inkl. Hashfunktion und Schlüssellängen | Schlüssellänge: 256 bit<br>Hashfunktion: SHA 256<br>Kurve: NIST P-256 (secp256r1) |

*Tabelle 4: Zusätzliche Angaben*

| Gegenstand | Angaben des Antragstellers |
|---|---|
| Größe des internen Speichers des Sicherheitsmoduls | 500GB |
| Zeitlicher Abstand in dem das Sicherheitsmodul die intern verwaltete Zeit in seinem nichtflüchtigen Speicher speichert | 24h |
| Maximale Anzahl von Clients, die die TSE gleichzeitig zur Absicherung von Transaktionen nutzen können | 200 |
| Maximale Anzahl der parallel geöffneten Transaktionen, die das Sicherheitsmodul verwalten kann | 2000 |

# 8 Konformitätsprüfung

Die Konformitätsprüfung wurde im Zeitraum Jaunar bis Mai 2021 von der beauftragten Prüfstelle durchgeführt.

Der von der Prüfstelle vorgelegte Prüfbericht enthält detaillierte Beschreibungen der durchgeführten Testfälle, der jeweils zu erfüllenden Anforderungen / Vorgaben bzw. einzuhaltenden Wertebereiche / Grenzwerte sowie eine vollständige Aufstellung der erzielten Prüfergebnisse.

## 8.1 Ergebnisse der Konformitätsprüfung

Tabelle 5 enthält die Zusammenfassung der durchgeführten Testfälle.

*Tabelle 5: Konformitätsprüfung gemäß BSI TR-03153-TS*

| Testcase ID | Profile | Verdict |
|---|---|---|
| **5.1 Modul Storage – Speichermedium (STO)** | | |
| **5.1.1 Funktionale Prüfungen von Speichermedien (STO_FUN)** | | |
| STO_FUN_01 | SM_AGG | n.a.[1] |
| STO_FUN_02 | SM_NOAGG | Pass |
| STO_FUN_03 | SM_AGG | n.a.[2] |
| STO_FUN_04 | SM_NOAGG | Pass |
| STO_FUN_05 | SM_AGG | n.a.[3] |
| STO_FUN_06 | SM_NOAGG, SM_MULTI | Pass |
| STO_FUN_07 | STORAGE_BASIC | Pass |
| STO_FUN_08 | STORAGE_BASIC | Pass |
| STO_FUN_09 | STORAGE_BASIC | Pass |
| STO_FUN_10 | STORAGE_BASIC | Pass |
| STO_FUN_11 | STORAGE_BASIC | Pass |
| **5.1.2 Prüfungen der Speicherkapazität von Speichermedien (STO_CAP)** | | |
| STO_CAP_01 | STORAGE_BASIC | Pass |
| **5.1.3 Prüfungen der Zuverlässigkeit von Speichermedien (STO_REL)** | | |
| STO_REL_01 | STORAGE_BASIC | Pass |
| **5.1.4 Prüfungen für fernverbundene Speichermedien (STO_REM)** | | |
| STO_REM_01 | STORAGE_REMOTE | n.a.[4] |
| **5.2 Modul Security Module – Sicherheitsmodul (SM)** | | |
| **5.2.1 Prüfungen zu Konkatenation und Signaturerstellung (SM_CON)** | | |
| SM_CON_01 | SM_NOAGG | Pass |
| SM_CON_02 | SM_AGG | n.a.[5] |
| SM_CON_03 | SM_NOAGG | Pass |

1 n.a. wegen Profil SM_AGG
2 n.a. wegen Profil SM_AGG
3 n.a. wegen Profil SM_AGG
4 n.a. wegen Profil STORAGE_REMOTE
5 n.a. wegen Profil SM_AGG

| Testcase ID | Profile | Verdict |
|---|---|---|
| SM_CON_04 | SM_AGG | n.a.[6] |
| SM_CON_05 | SM_AGG | n.a.[7] |
| SM_CON_06 | SM_NOAGG, SM_MULTI | Pass |
| SM_CON_07 | SM_AGG, SM_MULTI | n.a.[8] |
| SM_CON_08 | SM_NOAGG, SM_MULTI | Pass |
| SM_CON_09 | SM_AGG, SM_MULTI | n.a.[9] |
| SM_CON_10 | SM_AGG, SM_MULTI | n.a.[10] |
| SM_CON_11 | SM_AGG, SM_MULTI | n.a.[11] |
| SM_CON_12 | SM_NOAGG, SM_MULTI | Pass |
| SM_CON_13 | SM_BASIC | Pass |
| SM_CON_14 | SM_BASIC | Pass |
| SM_CON_15 | SM_BASIC, SDI | Pass |
| SM_CON_16 | SM_BASIC, SDI | Pass |
| SM_CON_17 | SM_BASIC, SDI | Pass |
| SM_CON_18 | SM_BASIC | Pass |
| **5.2.2 Prüfungen zur Zeitführung im Sicherheitsmodul (SM_TME)** | | |
| SM_TME_01 | SM_BASIC | Pass |
| SM_TME_02 | SM_BASIC | Pass |
| SM_TME_03 | SM_BASIC | Pass |
| SM_TME_04 | SM_BASIC, NO_TIME_SYNC | n.a.[12] |
| SM_TME_05 | SM_AGG, SM_MULTI | n.a.[13] |
| SM_TME_06 | SM_NOAGG, SM_MULTI | Pass |
| SM_TME_07 | SM_NOAGG | Pass |
| SM_TME_08 | SM_AGG | n.a.[14] |
| SM_TME_09 | SM_BASIC, SDI | Pass |
| SM_TME_10 | SM_BASIC | n.a.[15] |
| SM_TME_11 | SM_BASIC | n.a.[16] |
| **5.2.3 Prüfungen zum Signaturzähler im Sicherheitsmodul (SM_SIG)** | | |
| SM_SIG_01 | SM_NOAGG | Pass |
| SM_SIG_02 | SM_AGG | n.a.[17] |
| SM_SIG_03 | SM_NOAGG, SM_MULTI | Pass |
| SM_SIG_04 | SM_AGG | n.a.[18] |
| SM_SIG_05 | SM_BASIC | Pass |
| SM_SIG_06 | SM_NOAGG | Pass |

6 n.a. wegen Profil SM_AGG
7 n.a. wegen Profil SM_AGG
8 n.a. wegen Profil SM_AGG
9 n.a. wegen Profil SM_AGG
10 n.a. wegen Profil SM_AGG
11 n.a. wegen Profil SM_AGG
12 n.a. wegen Profil SM_NO_TIME_SYNC
13 n.a. wegen Profil SM_AGG
14 n.a. wegen Profil SM_AGG
15 Dieser Testfall ist nach [BSI TR-03153-TS-ERG]optional. Ein Zugriff auf den nichtflüchtigen Speicher ist nicht möglich.
16 Dieser Testfall ist nach [BSI TR-03153-TS-ERG]optional. Ein Zugriff auf den nichtflüchtigen Speicher ist nicht möglich.
17 n.a. wegen Profil SM_AGG
18 n.a. wegen Profil SM_AGG

| Testcase ID | Profile | Verdict |
|---|---|---|
| SM_SIG_07 | SM_AGG | n.a.[19] |
| SM_SIG_08 | SM_BASIC, SDI | Pass |
| **5.2.4 Prüfungen zur Transaktionsnummer im Sicherheitsmodul (SM_TRA)** | | |
| SM_TRA_01 | SM_BASIC | Pass |
| SM_TRA_02 | SM_MULTI | Pass |
| SM_TRA_03 | SM_MULTI | Pass |
| SM_TRA_04 | SM_BASIC | Pass |
| SM_TRA_05 | SM_BASIC | Pass |
| SM_TRA_06 | SM_BASIC | Pass |
| SM_TRA_07 | SM_BASIC | Pass |
| **5.2.5 Prüfungen zur Kryptographieanwendung im Sicherheitsmodul (SM_KRY)** | | |
| SM_KRY_01 | SM_BASIC | Pass |
| SM_KRY_02 | SM_BASIC | Pass |
| SM_KRY_03 | SM_BASIC | n.a.[20] |
| SM_KRY_04 | SM_BASIC | Pass |
| **5.2.6 Prüfungen der PKI von Sicherheitsmodulen (SM_PKI)** | | |
| SM_PKI_01 | SM_BASIC | Pass |
| SM_PKI_02 | SM_BASIC | Pass |
| SM_PKI_03 | SM_BASIC | Pass |
| **5.2.7 Prüfungen für fernverbundene Sicherheitsmodule (SM_REM)** | | |
| SM_REM_01 | SM_REMOTE | Pass |
| **5.3 Modul Integration Interface - Einbindungsschnittstelle** | | |
| **5.3.1 Basisprüfungen der Einbindungsschnittstelle** | | |
| 5.3.1.1 Export des Archivs (II_EXP) | | |
| II_EXP_01 | SM_BASIC | Pass |
| II_EXP_02 | SM_BASIC | Pass |
| II_EXP_03 | SM_BASIC, STORAGE_REMOTE | n.a.[21] |
| 5.3.1.2 Initialisierung der Technischen Sicherheitseinrichtung (II_INI) | | |
| II_INI_01 | SM_BASIC | Pass |
| II_INI_02 | SM_BASIC | Pass |
| II_INI_03 | SM_BASIC | Fail[22] |
| II_INI_04 | SM_BASIC | Pass |
| II_INI_05 | SM_BASIC | Pass |
| II_INI_06 | SM_BASIC | n.a.[23] |
| II_INI_07 | SM_BASIC | Pass |
| II_INI_08 | SM_BASIC | Pass |
| II_INI_09 | SM_BASIC | Pass |
| II_INI_10 | SM_BASIC | Pass |

19 n.a. wegen Profil SM_AGG
20 Testcase nicht verpflichtend gemäß [BSI TR-03153-TS-ERG]
21 n.a. wegen Profil STORAGE_REMOTE
22 Siehe hierzu Kapitel 8.2.1
23 Der Testfall soll prüfen, dass im Falle, dass keine Herstellerbeschreibung gesetzt ist, ein Aufruf von initialize() ohne Beschreibungstext fehlschlägt. Die Vorbedingung, dass keine Herstellerbeschreibung gesetzt ist, ist nicht erfüllbar, da der Hersteller immer eine Beschreibung setzt. Der Testfall kann daher nicht umgesetzt werden.

| Testcase ID | Profile | Verdict |
|---|---|---|
| II_INI_11 | SM_BASIC | Pass |
| II_INI_12 | SM_BASIC | Pass |
| II_INI_13 | SM_BASIC, SM_REMOTE | Pass |
| II_INI_14 | SM_BASIC, STORAGE_REMOTE | n.a.[24] |
| 5.3.1.3 Außerbetriebnahme des Sicherheitsmoduls (II_DSE) | | |
| II_DSE_01 | SM_BASIC | Pass |
| II_DSE_02 | SM_BASIC | Pass |
| II_DSE_03 | SM_BASIC | Pass |
| II_DSE_04 | SM_BASIC | Pass |
| II_DSE_05 | SM_BASIC | Pass |
| II_DSE_06 | SM_BASIC, SM_REMOTE | Pass |
| II_DSE_07 | SM_BASIC, STORAGE_REMOTE | n.a.[25] |
| 5.3.1.4 Starten einer Transaktion (II_STA) | | |
| II_STA_01 | SM_BASIC | Pass |
| II_STA_02 | SM_BASIC | Pass |
| II_STA_03 | SM_BASIC | n.a.[26] |
| II_STA_04 | SM_BASIC | n.a.[27] |
| II_STA_05 | SM_BASIC | n.a.[28] |
| II_STA_06 | SM_BASIC, SM_REMOTE | Pass |
| II_STA_07 | SM_BASIC, STORAGE_REMOTE | n.a.[29] |
| II_STA_08 | SM_BASIC | Pass |
| II_STA_09 | SM_BASIC | Pass |
| 5.3.1.5 Aktualisierung einer Transaktion (II_UPD) | | |
| II_UPD_01 | SM_NOAGG | Pass |
| II_UPD_02 | SM_NOAGG | Pass |
| II_UPD_03 | SM_AGG | n.a.[30] |
| II_UPD_04 | SM_NOAGG | n.a.[31] |

24 n.a. wegen Profil STORAGE_REMOTE
25 n.a. wegen Profil STORAGE_REMOTE
26 Der Testfall prüft, ob für den Fall, dass keine Referenz auf den Speicherbereich für die Rückgabe des Zeitpunkts des Vorgangsbeginns übergeben wird, ein Fehler geworfen wird. Aufgrund der Client-Server-Architektur ist eine Speicherreferenz für den Rückgabewert irrelevant. Es wird eine Protobuf-Nachricht an die Einbindungsschnittstelle erzeugt. Eine hier übergebene Speicherreferenz hat keine Bedeutung. Die Antwort-Nachricht der TSE wird ausgewertet. Wenn es hier zu Fehlern wegen fehlender Speicherreferenzen kommt, dann ist das ein Fehler auf der Seite des ERS, nicht der TSE. Das Testziel kann daher nicht erreicht werden und der Testfall schlägt fehl. Das Verhalten ist jedoch für die Funktionalität der TSE kein Problem. Dieser Testfall ist daher nicht anwendbar.
27 Der Testfall prüft, ob für den Fall, dass keine Referenz auf den Speicherbereich für die Rückgabe des Signaturzählers übergeben wird, ein Fehler geworfen wird. Aufgrund der Client-Server-Architektur ist eine Speicherreferenz für den Rückgabewert irrelevant. Es wird eine Protobuf-Nachricht an die Einbindungsschnittstelle erzeugt. Eine hier übergebene Speicherreferenz hat keine Bedeutung. Die Antwort-Nachricht der TSE wird ausgewertet. Wenn es hier zu Fehlern wegen fehlender Speicherreferenzen kommt, dann ist das ein Fehler auf der Seite des ERS, nicht der TSE. Das Testziel kann daher nicht erreicht werden und der Testfall schlägt fehl. Das Verhalten ist jedoch für die Funktionalität der TSE kein Problem. Dieser Testfall ist daher nicht anwendbar.
28 Der Testfall prüft, ob für den Fall, dass keine Referenz auf den Speicherbereich für die Rückgabe Hashwerts über den öffentlichen Schlüssel übergeben wird, ein Fehler geworfen wird. Aufgrund der Client-Server-Architektur ist eine Speicherreferenz für den Rückgabewert irrelevant. Es wird eine Protobuf-Nachricht an die Einbindungsschnittstelle erzeugt. Eine hier übergebene Speicherreferenz hat keine Bedeutung. Die Antwort-Nachricht der TSE wird ausgewertet. Wenn es hier zu Fehlern wegen fehlender Speicherreferenzen kommt, dann ist das ein Fehler auf der Seite des ERS, nicht der TSE. Das Testziel kann daher nicht erreicht werden und der Testfall schlägt fehl. Das Verhalten ist jedoch für die Funktionalität der TSE kein Problem. Dieser Testfall ist daher nicht anwendbar.
29 n.a. wegen Profil STORAGE_REMOTE
30 n.a. wegen Profil SM_AGG

| Testcase ID | Profile | Verdict |
|---|---|---|
| II_UPD_05 | SM_BASIC, SM_REMOTE | Pass |
| II_UPD_06 | SM_BASIC, STORAGE_REMOTE | n.a.[32] |
| II_UPD_07 | SM_AGG, STORAGE_REMOTE | n.a.[33] |
| II_UPD_08 | SM_BASIC, SM_NOAGG | Pass |
| II_UPD_09 | SM_BASIC, SM_AGG | n.a.[34] |
| II_UPD_10 | SM_BASIC | Pass |
| II_UPD_11 | SM_BASIC | Pass |
| II_UPD_12 | SM_BASIC | Pass |
| 5.3.1.6 Beenden einer Transaktion (II_FIN) | | |
| II_FIN_01 | SM_BASIC | Pass |
| II_FIN_02 | SM_BASIC | Pass |
| II_FIN_03 | SM_BASIC | n.a.[35] |
| II_FIN_04 | SM_BASIC | n.a.[36] |
| II_FIN_05 | SM_BASIC, SM_REMOTE | Pass |
| II_FIN_06 | SM_BASIC, STORAGE_REMOTE | n.a.[37] |
| II_FIN_07 | SM_BASIC | Pass |
| II_FIN_08 | SM_BASIC | Pass |
| II_FIN_09 | SM_BASIC | Pass |
| II_FIN_10 | SM_BASIC | Pass |
| 5.3.1.7 Verwendung der TSE durch mehrere Clients (II_MCU) | | |
| II_MCU_01 | MULTI_CLIENT, SM_NOAGG | Pass |
| II_MCU_02 | MULTI_CLIENT, SM_AGG | n.a.[38] |
| II_MCU_03 | MULTI_CLIENT, SM_NOAGG | Pass |
| II_MCU_04 | MULTI_CLIENT, SM_AGG | n.a.[39] |
| II_MCU_05 | MULTI_CLIENT, SM_BASIC | Pass |
| II_MCU_06 | NO_MULTI_CLIENT, SM_BASIC | n.a.[40] |

31 Der Testfall prüft, ob für den Fall, dass keine Referenz auf den Speicherbereich für die Rückgabe des Zeitpunkts des Vorgangsbeginns übergeben wird, ein Fehler geworfen wird. Aufgrund der Client-Server-Architektur ist eine Speicherreferenz für den Rückgabewert irrelevant. Es wird eine Protobuf-Nachricht an die Einbindungsschnittstelle erzeugt. Eine hier übergebene Speicherreferenz hat keine Bedeutung. Die Antwort-Nachricht der TSE wird ausgewertet. Wenn es hier zu Fehlern wegen fehlender Speicherreferenzen kommt, dann ist das ein Fehler auf der Seite des ERS, nicht der TSE. Dieser Testfall ist daher nicht anwendbar.

32 n.a. wegen Profil STORAGE_REMOTE

33 n.a. wegen Profil STORAGE_REMOTE

34 n.a. wegen Profil SM_AGG

35 Der Testfall prüft, ob für den Fall, dass keine Referenz auf den Speicherbereich für die Rückgabe des Zeitpunkts des Vorgangsbeginns übergeben wird, ein Fehler geworfen wird. Aufgrund der Client-Server-Architektur ist eine Speicherreferenz für den Rückgabewert irrelevant. Es wird eine Protobuf-Nachricht an die Einbindungsschnittstelle erzeugt. Eine hier übergebene Speicherreferenz hat keine Bedeutung. Die Antwort-Nachricht der TSE wird ausgewertet. Wenn es hier zu Fehlern wegen fehlender Speicherreferenzen kommt, dann ist das ein Fehler auf der Seite des ERS, nicht der TSE. Dieser Testfall ist daher nicht anwendbar.

36 Der Testfall prüft, ob für den Fall, dass keine Referenz auf den Speicherbereich für die Rückgabe des Signaturzählers übergeben wird, ein Fehler geworfen wird. Aufgrund der Client-Server-Architektur ist eine Speicherreferenz für den Rückgabewert irrelevant. Es wird eine Protobuf-Nachricht an die Einbindungsschnittstelle erzeugt. Eine hier übergebene Speicherreferenz hat keine Bedeutung. Die Antwort-Nachricht der TSE wird ausgewertet. Wenn es hier zu Fehlern wegen fehlender Speicherreferenzen kommt, dann ist das ein Fehler auf der Seite des ERS, nicht der TSE. Dieser Testfall ist daher nicht anwendbar.

37 n.a. wegen Profil STORAGE_REMOTE

38 n.a. wegen Profil SM_AGG

39 n.a. wegen Profil SM_AGG

40 n.a. wegen Profil NO_MULTI_CLIENT

| Testcase ID | Profile | Verdict |
|---|---|---|
| **5.3.2 Prüfungen der Einbindungsschnittstellen gemäß BSI TR-03153** | | |
| 5.3.2.1 Aktualisierung der Uhrzeit (SDI_UDT) | | |
| SDI_UDT_01 | SDI, NO_TIME_SYNC | n.a.[41] |
| SDI_UDT_02 | SDI, TIME_SYNC | n.a.[41] |
| SDI_UDT_03 | SDI, NO_TIME_SYNC | n.a.[41] |
| SDI_UDT_04 | SDI, SM_REMOTE | n.a.[41] |
| SDI_UDT_05 | SDI, STORAGE_REMOTE | n.a.[41] |
| SDI_UDT_06 | SDI | n.a.[41] |
| SDI_UDT_07 | SDI | n.a.[41] |
| 5.3.2.2 Export des Archivs (SDI_EXP) | | |
| SDI_EXP_01 | SDI | n.a.[41] |
| SDI_EXP_02 | SDI | n.a.[41] |
| SDI_EXP_03 | SDI | n.a.[41] |
| SDI_EXP_04 | SDI | n.a.[41] |
| SDI_EXP_05 | SDI | n.a.[41] |
| SDI_EXP_06 | SDI | n.a.[41] |
| SDI_EXP_07 | SDI | n.a.[41] |
| SDI_EXP_08 | SDI | n.a.[41] |
| SDI_EXP_09 | SDI | n.a.[41] |
| SDI_EXP_10 | SDI | n.a.[41] |
| SDI_EXP_11 | SDI | n.a.[41] |
| SDI_EXP_12 | SDI | n.a.[41] |
| SDI_EXP_13 | SDI | n.a.[41] |
| SDI_EXP_14 | SDI | n.a.[41] |
| SDI_EXP_15 | SDI | n.a.[41] |
| SDI_EXP_16 | SDI | n.a.[41] |
| SDI_EXP_17 | SDI | n.a.[41] |
| SDI_EXP_18 | SDI | n.a.[41] |
| SDI_EXP_19 | SDI | n.a.[41] |
| SDI_EXP_20 | SDI | n.a.[41] |
| SDI_EXP_21 | SDI | n.a.[41] |
| SDI_EXP_22 | SDI | n.a.[41] |
| SDI_EXP_23 | SDI | n.a.[41] |
| SDI_EXP_24 | SDI | n.a.[41] |
| SDI_EXP_25 | SDI | n.a.[41] |
| SDI_EXP_26 | SDI | n.a.[41] |
| SDI_EXP_27 | SDI | n.a.[41] |
| SDI_EXP_28 | SDI | n.a.[41] |
| SDI_EXP_29 | SDI | n.a.[41] |
| SDI_EXP_30 | SDI | n.a.[41] |
| SDI_EXP_31 | SDI | n.a.[41] |

41 n.a. wegen Profil SDI

| Testcase ID | Profile | Verdict |
|---|---|---|
| SDI_EXP_32 | SDI | n.a.[42] |
| SDI_EXP_33 | SDI | n.a.[42] |
| SDI_EXP_34 | SDI | n.a.[42] |
| SDI_EXP_35 | SDI | n.a.[42] |
| SDI_EXP_36 | SDI | n.a.[42] |
| SDI_EXP_37 | SDI | n.a.[42] |
| SDI_EXP_38 | SDI | n.a.[42] |
| SDI_EXP_39 | SDI | n.a.[42] |
| SDI_EXP_40 | SDI | n.a.[42] |
| SDI_EXP_41 | SDI | n.a.[42] |
| SDI_EXP_42 | SDI | n.a.[42] |
| 5.3.2.3 Zertifikatsabruf (SDI_EXC) | | |
| SDI_EXC_01 | SDI | n.a.[42] |
| 5.3.2.4 Wiederherstellen durch ein Backup (SDI_RFB) | | |
| SDI_RFB_01 | SDI_RESTORE | n.a.[42] |
| SDI_RFB_02 | SDI_RESTORE | n.a.[42] |
| SDI_RFB_03 | SDI_RESTORE, STORAGE_REMOTE | n.a.[42] |
| SDI_RFB_04 | SDI_RESTORE | n.a.[42] |
| SDI_RFB_05 | SDI_RESTORE | n.a.[42] |
| 5.3.2.5 Lesen einer Log-Nachricht (SDI_RLM) | | |
| SDI_RLM_01 | SDI, SM_NOAGG | n.a.[42] |
| SDI_RLM_02 | SDI, SM_AGG | n.a.[42] |
| SDI_RLM_03 | SDI, SM_REMOTE | n.a.[42] |
| 5.3.2.6 Export von Seriennummern (SDI_ESN) | | |
| SDI_ESN_01 | SDI | Pass |
| SDI_ESN_02 | SDI | Pass |
| SDI_ESN_03 | SDI | Pass |
| 5.3.2.7 Initialisierung der Sicherheitseinrichtung (SDI_INI) | | |
| SDI_INI_01 | SDI | n.a.[42] |
| SDI_INI_02 | SDI | n.a.[42] |
| SDI_INI_03 | SDI | n.a.[42] |
| SDI_INI_04 | SDI | n.a.[42] |
| SDI_INI_05 | SDI | n.a.[42] |
| 5.3.2.8 Außerbetriebnahme des Sicherheitsmoduls (SDI_DSE) | | |
| SDI_DSE_01 | SDI | n.a.[42] |
| SDI_DSE_02 | SDI | n.a.[42] |
| SDI_DSE_03 | SDI | n.a.[42] |
| 5.3.2.9 Abfrage der maximalen Anzahl von simultanen Clients der TSE (SDI_MNC) | | |
| SDI_MNC_01 | SDI, MULTI_CLIENT | n.a.[42] |
| 5.3.2.10 Abfrage der aktuellen Anzahl von Clients der TSE (SDI_CNC) | | |
| SDI_CNC_01 | SDI, MULTI_CLIENT | n.a.[42] |

42 n.a. wegen Profil SDI

| Testcase ID | Profile | Verdict |
|---|---|---|
| SDI_CNC_02 | SDI, MULTI_CLIENT | n.a.[43] |
| SDI_CNC_03 | SDI, MULTI_CLIENT | n.a.[43] |
| SDI_CNC_04 | SDI, MULTI_CLIENT | n.a.[43] |
| 5.3.2.11 Abfrage der maximalen Anzahl von parallelen Transaktionen (SDI_MNT) | | |
| SDI_MNT_01 | SDI, SM_MULTI | n.a.[43] |
| 5.2.3.12 Abfrage aktuelle Anzahl parallel geöffneter Transaktionen (SDI_CNT) | | |
| SDI_CNT_01 | SDI, SM_MULTI | n.a.[43] |
| SDI_CNT_02 | SDI, SM_MULTI | n.a.[43] |
| SDI_CNT_03 | SDI, SM_MULTI | n.a.[43] |
| SDI_CNT_04 | SDI, SM_MULTI | n.a.[43] |
| 5.3.2.13 Abfrage unterstützte Varianten der Aktualisierungen von Transaktionen (SDI_UTV) | | |
| SDI_UTV_01 | SDI | n.a.[43] |
| 5.3.2.14 Löschen von gespeicherten Daten im Speichermedium (SDI_DSD) | | |
| SDI_DSD_01 | SDI_DELETE | Pass |
| SDI_DSD_02 | SDI_DELETE | Pass |
| SDI_DSD_03 | SDI_DELETE, STORAGE_REMOTE | n.a.[43] |
| SDI_DSD_04 | SDI | Pass |
| SDI_DSD_05 | SDI | n.a.[43] |
| 5.3.2.15 Authentifizierung von Benutzern der TSE (SDI_AUT) | | |
| SDI_AUT_01 | SDI | n.a.[43] |
| SDI_AUT_02 | SDI | n.a.[43] |
| SDI_AUT_03 | SDI | n.a.[43] |
| SDI_AUT_04 | SDI | n.a.[43] |
| SDI_AUT_05 | SDI | n.a.[43] |
| SDI_AUT_06 | SDI, SM_REMOTE | n.a.[43] |
| SDI_AUT_07 | SDI, STORAGE_REMOTE | n.a.[43] |
| 5.3.2.16 Abmeldung von Benutzern der TSE (SDI_LGO) | | |
| SDI_LGO_01 | SDI | n.a.[43] |
| SDI_LGO_02 | SDI | n.a.[43] |
| SDI_LGO_03 | SDI | n.a.[43] |
| SDI_LGO_04 | SDI | n.a.[43] |
| SDI_LGO_05 | SDI, SM_REMOTE | n.a.[43] |
| SDI_LGO_06 | SDI, STORAGE_REMOTE | n.a.[43] |
| 5.3.2.17 Entsperren von Benutzern(SDI_UBU) | | |
| SDI_UBU_01 | SDI | n.a.[43] |
| SDI_UBU_02 | SDI | n.a.[43] |
| SDI_UBU_03 | SDI | n.a.[43] |
| SDI_UBU_04 | SDI | n.a.[43] |
| SDI_UBU_05 | SDI, SM_REMOTE | n.a.[43] |
| SDI_UBU_06 | SDI, STORAGE_REMOTE | n.a.[43] |
| **5.3.3 Prüfungen für herstellerspezifische Einbindungsschnittstellen (CI)** | | |

43 n.a. wegen Profil SDI

| Testcase ID | Profile | Verdict |
|---|---|---|
| 5.3.3.1 Aktualisierung der Zeit innerhalb des Sicherheitsmoduls (CI_UDT) | | |
| CI_UDT_01 | CUSTOM_INTEGRATION_INTERFACE, SM_BASIC | Pass |
| CI_UDT_02 | CUSTOM_INTEGRATION_INTERFACE, SM_REMOTE | Pass |
| CI_UDT_03 | CUSTOM_INTEGRATION_INTERFACE, STORAGE_REMOTE | n.a.[44] |
| **5.4 Prüfung der Exportdaten gemäß BSI TR-03153** | | |
| **5.4.1 TAR-Format (EXP_TAR)** | | |
| EXP_TAR_01 | SM_BASIC | Pass |
| **5.4.2 Initialisierungsdaten (EXP_INI)** | | |
| EXP_INI_01 | SM_BASIC | Pass |
| EXP_INI_02 | SM_BASIC | Pass |
| EXP_INI_03 | SM_BASIC | Pass |
| EXP_INI_04 | SM_BASIC | Pass |
| **5.4.3 Log-Nachrichten (EXP_LOG)** | | |
| EXP_LOG_01 | SM_BASIC | Pass |
| EXP_LOG_02 | SM_BASIC | Pass |
| EXP_LOG_03 | SM_BASIC, SDI | Pass |
| EXP_LOG_04 | SM_BASIC, SDI | Pass |
| EXP_LOG_05 | SM_BASIC | Pass |
| EXP_LOG_06 | SM_BASIC | Pass |
| EXP_LOG_07 | SM_NOAGG | Pass |
| EXP_LOG_08 | SM_NOAGG | Pass |
| EXP_LOG_09 | SM_AGG | n.a.[45] |
| EXP_LOG_10 | SM_AGG | n.a.[46] |
| EXP_LOG_11 | SM_NOAGG | Pass |
| EXP_LOG_12 | SM_AGG | n.a.[47] |
| EXP_LOG_13 | SM_BASIC | Pass |
| EXP_LOG_14 | SM_BASIC | n.a.[48] |
| EXP_LOG_15 | SM_BASIC | Pass |
| EXP_LOG_16 | SM_BASIC | Pass |

44 n.a. wegen Profil STORAGE_REMOTE
45 n.a. wegen Profil SM_AGG
46 n.a. wegen Profil SM_AGG
47 n.a. wegen Profil SM_AGG
48 Das Feld „description“ ist nicht vom Hersteller vorbesetzt.

| Testcase ID | Profile | Verdict |
|---|---|---|
| EXP_LOG_17 | SM_BASIC | Pass |
| **5.4.4 Zertifikatsexport (EXP_CER)** | | |
| EXP_CER_01 | SM_BASIC | Pass |
| **Testcases gemäß [BSI TR-03153-TS-KuA]** | | |
| **2.1 Architektur des Sicherheitsmoduls** | | |
| **2.1 .2 Prüfung zu der genutzten Architektur des Sicherheitsmoduls** | | |
| SM_ARCH_01 | SM_BASIC | Pass |
| SM_ARCH_02 | SM_BASIC | Pass |
| SM_ARCH_03 | SM_BASIC | Pass |
| SM_ARCH_04 | SM_BASIC | Pass |
| SM_ARCH_05 | SM_BASIC | Pass |
| SM_ARCH_06 | SM_BASIC | Pass |
| SM_ARCH_07 | SM_BASIC | Pass |
| SM_ARCH_08 | SM_BASIC | Pass |
| SM_ARCH_09 | SM_BASIC | Pass |
| **2.2 Ergänzende Testfälle zu Log-Nachrichten** | | |
| **2.2.1 Ergänzende ICS-Angaben** | | |
| SM_ICS_01 | - | Pass |
| **2.2.2 Prüfung der ergänzenden Log-Nachrichten** | | |
| EXP_LOG_18 | - | Pass |
| EXP_LOG_19 | - | Pass |
| EXP_LOG_20_A | - | Pass |
| EXP_LOG_20_B | - | Pass |
| EXP_LOG_20_C | - | Pass |
| EXP_LOG_20_D | - | Pass |
| EXP_LOG_20_E | - | Pass |
| EXP_LOG_20_F | - | Pass |
| EXP_LOG_20_G | - | Pass |
| EXP_LOG_20_H | - | Pass |
| EXP_LOG_20_I | - | Pass |
| EXP_LOG_20_J | - | Pass |
| EXP_LOG_20_K | - | Pass |
| EXP_LOG_20_L | - | Pass |

| Testcase ID | Profile | Verdict |
|---|---|---|
| EXP_LOG_20_M | - | Pass |
| EXP_LOG_20_N | - | Pass |
| EXP_LOG_20_O | - | Pass |
| EXP_LOG_20_P | - | n.a.[49] |
| EXP_LOG_20_Q | - | n.a.[50] |
| EXP_LOG_20_R | - | Pass |
| EXP_LOG_20_S | - | Pass |
| EXP_LOG_21_A | - | Pass |
| EXP_LOG_21_B | - | Pass |
| EXP_LOG_21_C | - | Pass |
| EXP_LOG_21_D | - | Pass |
| EXP_LOG_21_E | - | Pass |
| EXP_LOG_21_F | - | Pass |
| EXP_LOG_21_G | - | Pass |
| EXP_LOG_21_H | - | n.a.[51] |
| EXP_LOG_21_I | - | Pass |
| EXP_LOG_21_J | - | Pass |
| EXP_LOG_21_K | - | Pass |
| EXP_LOG_21_L | - | Pass |
| EXP_LOG_21_M | - | Pass |
| EXP_LOG_21_N | - | Pass |
| EXP_LOG_21_O | - | Pass |
| EXP_LOG_21_P | - | n.a.[52] |
| EXP_LOG_21_Q | - | n.a.[53] |
| EXP_LOG_21_R | - | Pass |
| EXP_LOG_21_S | - | Pass |
| EXP_LOG_22_A | - | Pass |
| EXP_LOG_22_B | - | Pass |
| EXP_LOG_22_C | - | Pass |
| EXP_LOG_22_D | - | Pass |
| EXP_LOG_22_E | - | Pass |
| EXP_LOG_22_F | - | Pass |
| EXP_LOG_22_G | - | Pass |
| EXP_LOG_22_H | - | n.a.[54] |
| EXP_LOG_22_I | - | Pass |
| EXP_LOG_22_J | - | Pass |
| EXP_LOG_22_K | - | Pass |
| EXP_LOG_22_L | - | Pass |

49 Log lockTransactionLogging ist optional. Log wird nicht erstellt. Testfall nicht relevant.
50 Log unlockTransactionLogging ist optional. Log wird nicht erstellt. Testfall nicht relevant.
51 Log updateDevice ist optional. Log wird nicht erstellt. Testfall nicht relevant.
52 Log lockTransactionLogging ist optional. Log wird nicht erstellt. Testfall nicht relevant.
53 Log lockTransactionLogging ist optional. Log wird nicht erstellt. Testfall nicht relevant.
54 Log updateDevice ist optional. Log wird nicht erstellt. Testfall nicht relevant.

| Testcase ID | Profile | Verdict |
|---|---|---|
| EXP_LOG_22_M | - | Pass |
| EXP_LOG_22_N | - | Pass |
| EXP_LOG_22_O | - | Pass |
| EXP_LOG_22_P | - | n.a.[55] |
| EXP_LOG_22_Q | - | n.a.[56] |
| EXP_LOG_22_R | - | Pass |
| EXP_LOG_22_S | - | Pass |
| **2.2.3 Ergänzung zu Prüfungen für die Sicherheitsmodule in einer Client-Server-Architektur** | | |
| EXP_LOG_23 | - | Pass |
| EXP_LOG_24 | - | Pass |
| EXP_LOG_25 | - | Pass |
| **2.2.4 Prüfung von additionalExternalData und additionalInternalData** | | |
| EXP_LOG_26 | - | Pass |
| EXP_LOG_27 | - | Pass |
| EXP_LOG_28 | - | Pass |
| EXP_LOG_29 | - | Pass |
| **2.2.5 Ergänzung zu Prüfung zur Zeitführung im Sicherheitsmodul** | | |
| SM_TME_12 | - | Pass |
| SM_TME_13 | - | Pass |
| **2.2.6 Ergänzung zur Außerbetriebnahme des Sicherheitsmoduls der Technischen Sicherheitseinrichtung** | | |
| II_DSE_08 | - | n.a.[57] |
| II_DSE_09 | - | Pass |
| **2.2.7 Ergänzung zu Prüfungen der Herstellerdokumentation** | | |
| DOC_PAR_01 | - | Pass |
| DOC_DLY_01 | - | Pass |

## 8.2 Festgestellte Abweichungen

### 8.2.1 II_INI_03

Festgestelltes Verhalten: Beim Aufruf von initialize() mit Beschreibungstext im Fall, dass die Beschreibung vom Hersteller gesetzt wurde, verlangt der Testfall II_INI_03, dass ein Fehler zurückgegeben wird. Der Prüfgegenstand erlaubt jedoch ein Überschreiben der Hersteller-Beschreibung bei der ersten Initialisierung.

Bewertung: Die Abweichung ist nicht schwerwiegend und zu vernachlässigen.

55 Log lockTransactionLogging ist optional. Log wird nicht erstellt. Testfall nicht relevant.
56 Log lockTransactionLogging ist optional. Log wird nicht erstellt. Testfall nicht relevant.
57 Der Testfall prüft, dass ein Stoppen der Audit-Funktionalität in der Sicherheitsmodulanwendung dazu führt, dass das Sicherheitsmodul permanent deaktiviert wird und ein Log des Typs disableSecureElement geschrieben wird. Die Konfiguration der Audit-Funktionalität wird im Log-File „configureLogging“ hinterlegt. Diese wird bei der Personalisierung der TSE geschrieben. Die Konfiguration der Audit-Funktionalität ist unveränderbar in den Programmcode der Anwendung einkodiert und lässt sich nicht durch beispielsweise ein manipuliertes Bootstrap-File anpassen. Ebenso existiert auch keine Schnittstelle zum SMAERS, die eine solche Manipulation zuließe. Aus diesem Grund kann die Audit-Funktionalität nicht ohne den Aufruf von disableSecureElement gestoppt werden und der Testfall ist nicht anwendbar.

Erforderliche Maßnahme: –

### 8.2.2 SM_CON_13 & EXP_LOG_14

Festgestelltes Verhalten: Beim Aufruf von initialize() ohne Beschreibungstext darf nach [BSI TR-03151], Kapitel 6.1 das Feld description in den systemOperationData des initialize-Logs nicht geschrieben werden. Dies wird vom Prüfgegenstand nicht erfüllt, stattdessen wird das Feld mit der vom Hersteller gesetzten Beschreibung gefüllt.

Bewertung: Die Abweichung ist nicht schwerwiegend und zu vernachlässigen.

Erforderliche Maßnahme: –

### 8.2.3 II_STA_03, II_STA_04, II_STA_05, II_UPD_03, II_FIN_03, II_FIN_04

Festgestelltes Verhalten: Abweichung im Verhalten, wenn einer Funktion Rückgabewerte ohne Referenz auf einen Speicherbereich übergeben werden (Null-Objekte): Aufgrund der Architektur des Prüfgegenstands hat die Referenz auf den Speicherbereich des Rückgabewerts, die bei Funktionsaufruf gemäß [BSI TR-03151] übergeben wird, keinerlei Bedeutung.

Bewertung: Diese Abweichung ist daher als Nichtanwendbarkeit der zugehörigen Testfälle zu werten.

Erforderliche Maßnahme: –

### 8.2.4 System-Logs

Festgestelltes Verhalten: System-Logs zu den Funktionen Initialize, UpdateTime, AuthenticateUser, LogOut, Un-blockUser, DisableSecureElement werden abweichend zu [BSI TR-03151] im Dateinamen mit kleinem Buchstaben begonnen.

Bewertung: Die Abweichung ist nicht schwerwiegend und zu vernachlässigen. Sie wird daher in den einzelnen Testfällen nicht aufgeführt.

Erforderliche Maßnahme: –

### 8.2.5 II_EXP_0

Festgestelltes Verhalten: Vor Inbetriebnahme einer Technischen Sicherheitseinrichtung soll der Aufruf von exportData() einen Fehler zurückgeben. Dies wird vom Prüfgegenstand nicht erfüllt und es werden Logs, die seit bzw. vor der Personalisierung angefallen sind (startAudit, configureLogging, unter Umständen updateTime und Audit-Logs), exportiert.

Bewertung: Die Abweichung ist nicht schwerwiegend und zu vernachlässigen.

Erforderliche Maßnahme: –

### 8.2.6 PKI Hinweis fiskaly: wurde am 11.06.2021 umgesetzt und an das BSI gemeldet.

Festgestelltes Verhalten: Im Rahmen der Konformitätsprüfung wurden für die von der Prüfstelle durchgeführten Tests Zertifikate durch eine „Wirk“-PKI (https://www.da-rz.de /de/ueber-darz/unternehmen/pki/tse-pki/zertifikate-der-tse-pki/) für unzertifzierte

Sicherheitseinrichtungen zu Prüfzwecken ausgestellt. Diese Zertifikate attestieren/ attestierten unzertifizierten Softwarekomponenten und Teststellungen den Status eines gültig zertifizierten Prüfgegenstandes. Weiter wurde durch das Bundesamt für Sicherheit in der Informationstechnik festgestellt, dass durch diese PKI Zertifikate für weitere Hersteller ausgestellt wurden, welche ebenfalls keine gültige Zertifizierung besitzen.

Bewertung: Für eine prüfende Finanzbehörde ist unter diesen Voraussetzungen keine geeignete Unterscheidung zwischen validen Aufzeichnungen zertifizierter Technischer Sicherheitseinrichtungen mehr möglich, da kein eindeutiger und deutlicher Hinweis auf die nicht vorhandenen Zertifizierungen besteht und der Anschein einer Absicherung mit einer zertifizierten TSE erweckt wird.

Erforderliche Maßnahme: Für einen zulässigen Betrieb des Prüfgegenstandes muss eine PKI verwendet werden, die keine Zertifikate für unzertifizierte Technische Sicherheitseinrichtungen ausstellt und diese auch niemals zuvor ausgestellt hat, damit das Vorhandensein eines Zertifikats aus dieser PKI ein eindeutiger Nachweis für die Erfüllung der gesetzlichen Anforderungen an die TSE ist.

Eine Wiederverwendung der bemängelten Zertifikatsstruktur (Root- und Sub-CA) durch eine bloße Sperrung der End-Entitätszertifikate, welche nicht für zertifizierte bzw. zum Zeitpunkt der Ausstellung nicht zertifizierte TSE ausgestellt wurden, ist nicht ausreichend, da diese seitens der prüfenden Finanzbehörden fälschlicher Weise als zum Zeitpunkt der Nutzung valide Zertifikate interpretiert werden könnten. Es ist somit eine neue, „ungenutzte“ PKI zu verwenden (d.h. Erstellung neuer Root-Zertifikate ohne Verlinkung oder Zusammenhang zur bemängelten Zertifikatskette).

Empfehlung: Es wird empfohlen, die am 11. Mai 2021 unter https://www.da-rz.de/de/ueber-darz/unternehmen/pki/tse-pki/zertifikate-der-tse-pki/ veröffentlichte PKI vollständig zu deaktivieren (Sperrung mit Sperrgrund „cessationOfOperation“ und darauf folgend mindestens die Erreichbarkeit aus dem Internet und die Listung in öffentlichen Verzeichnisdiensten beenden) und zukünftig Test-Zertifikate für TSE nur über eine direkt als solche bereits im Namen erkennbare "Test"-PKI erstellt werden.

Weiterhin wird empfohlen, dass, sofern in der PKI Zertifikate für mehrere Hersteller ausgestellt werden, für jeden Hersteller eine andere Sub-CA zu verwenden, um die Auswirkungen eines etwaigen Rückrufs eines CA-Zertifikats zu minimieren.

# 9 Ergebnis der Konformitätsprüfung

Die vollständigen Ergebnisse der Konformitätsprüfung sind in folgendem Prüfbericht und den zugehörigen Anlagen enthalten:

SRC
TR-Prüfbericht nach TR-03153
BSI-K-TR-0403
fiskaly sign Cloud.TSE v1.2.0-1.0.5
Prüfbericht Version 1.6
Erstellungsdatum: 17.05.2021

SRC
Addendum zu Prüfbericht v1.6
Übertragbarkeit der Prüfergebnisse von BSI-K-TR-0403
Admin Tool v1.1.1
Erstellungsdatum 26.05.2021

Die Vollständigkeit und Widerspruchsfreiheit des vorgelegten Prüfberichts wurde durch das Bundesamt für Sicherheit in der Informationstechnik verifiziert und bestätigt.

Die im Rahmen der Konformitätsprüfung erzielten Ergebnisse lassen sich wie folgt zusammenfassen:

- alle relevanten Testfälle des Moduls *Storage – Speichermedium (STO)* konnten mit „Pass“ bewertet werden;
- alle relevanten Testfälle des Moduls *Security Module – Sicherheitsmodul (SM)* konnten mit „Pass“ bewertet werden;
- bei der Durchführung der relevanten Testfälle des Moduls *Integration Interface – Einbindungsschnittstelle* wurden der Testfall II_INI_03 mit „Fail“ bewertet; alle übrigen relevanten Testfälle konnten mit „Pass“ bewertet werden;
- alle relevanten Testfälle des Moduls *Prüfung der Exportdaten gemäß BSI TR-03153* konnten mit „Pass“ bewertet werden;
- bei der Durchführung der relevanten Testfälle gemäß [BSI TR-03153-TS-KuA] konnten alle relevanten Testfälle konnten mit „Pass“ bewertet werden.

**Das erzielte Gesamtergebnis der Konformitätsprüfung ist: Pass** (mit Auflagen)

# 10 Ergebnis des Zertifizierungsverfahrens nach TR

Die Konformität des Prüfgegenstands zur Technischen Richtlinie BSI TR-03153 wird vom Bundesamt für Sicherheit in der Informationstechnik für den untersuchten Prüfbereich mit dem Konformitätsbescheid BSI-K-TR-0403-2021 vom 28. Mai 2021 mit Auflagen bestätigt.

Das Zertifikat nach Technischen Richtlinien ist gültig bis zum 27. Mai 2029.

Um einen zur [BSI TR-03153] konformen Betrieb des Prüfgegenstands sicherzustellen, werden folgende Nebenbestimmungen als Auflagen festgelegt:

1. Der Betrieb des Prüfgegenstandes ist nur unter Verwendung der in Kapitel 7.1.1 – 7.1.7 als System-Voraussetzungen genannten Umgebungen zulässig und durch die Zertifizierung abgedeckt. Für einen Betrieb unter anderen Systemvoraussetzungen besitzt das Zertifikat BSI-K-TR-0403-2021 keine Gültigkeit.
2. Für einen konformen Betrieb des Prüfgegenstandes muss eine PKI verwendet werden, die keine Zertifikate für nicht-zertifizierte Technische Sicherheitseinrichtungen ausstellt und diese auch niemals zuvor ausgestellt hat, damit das Vorhandensein eines Zertifikats aus dieser PKI ein eindeutiger Nachweis für die Erfüllung der gesetzlichen Anforderungen an die TSE ist.

   Eine Wiederverwendung der in Kapitel 8.2.6 bemängelten Zertifikatsstruktur (Root- und Sub-CA) durch eine bloße Sperrung der End-Entitätszertifikate, welche nicht für zertifizierte bzw. zum Zeitpunkt der Ausstellung nicht zertifizierte TSE ausgestellt wurden, ist nicht ausreichend, da diese seitens der prüfenden Finanzbehörden fälschlicher Weise als zum Zeitpunkt der Nutzung valide Zertifikate interpretiert werden könnten. Es ist somit eine neue, „ungenutzte“ PKI zu verwenden (d.h. Erstellung neuer Root-Zertifikate ohne Verlinkung oder Zusammenhang zur bemängelten Zertifikatskette).
3. Der Betrieb des Prüfgegenstands ist nur mit Schlüsseln zulässig, welche nach Erteilung des Zertifikats BSI-K-TR-0403-2021 und unter Verwendung der neuen PKI erstellt und beglaubigt wurden.

   Die Wiederverwendung von bereits erzeugten Schlüsseln ist somit explizit ausgeschlossen und nicht zulässig. Somit müssen alle Instanzen des Prüfgegenstands vor der Nutzung mit den neuen Schlüsseln neu initialisiert werden.
4. Die Vermischung von Aufzeichnungen des zertifizierten Prüfgegenstands mit Aufzeichnungen aus dem nicht-zertifizierten Betrieb, Testbetrieb oder ähnlichen Verhältnissen ist nicht zulässig. Insbesondere dürfen die Aufzeichnungen aus dem nicht zertifizierten Betrieb nicht mit den Exporten (TAR-Container o.ä.) der zertifizierten TSE kombiniert werden.

ad Punkt 2,3 und 4 Hinweis fiskaly: wurde am 11.06.2021 umgesetzt und an das BSI gemeldet. Es gibt keine offenen Auflagen mehr.

# Literaturverzeichnis


BSIG BSI-Gesetz – Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009, Bundesgesetzblatt Teil I Nr. 54, S. 2821

BSIZertV BSI-Zertifizierungs- und Anerkennungsverordnung – Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSIZertV), vom 17. Dezember 2014, Bundesgesetzblatt Teil I Nr. 61, S. 2231

BMIBGebV Besondere Gebührenverordnung des Bundesministeriums des Inneren, für Bau und Heimat für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (Besondere Gebührenverordnung BMI, BMIBGebV) vom02. September 2019, Bundesgesetzblatt I, S. 1359

VB-Produkte Verfahrensbeschreibung zur Zertifizierung von Produkten, Version 2.5 vom 19. März 2020

TR-Produkte Anforderungen an Antragsteller zur Zertifizierung von Produkten nach Technischen Richtlinien, Version 1.4 vom 17. Oktober 2019

BSI TR-03153 BSI TR-03153 – Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, Version 1.0.1 vom 20. Dezember 2018

BSI TR-03153-ERG Ergänzungen der BSI TR-03153 vom 02. Dezember 2019

BSI TR-03153-KuA Klarstellungen und Anwendungshinweise zur BSI TR-03153 und BSI-CC-PP-0105-V2-2020 vom 13. November 2020

BSI TR-03153-TS BSI TR-03153 – Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme – Testspezifikation, Version 1.0.1 vom 05. Februar 2019

BSI TR-03153-TS-ERG Ergänzungen der BSI TR-03153-TS vom 02. Dezember 2019

BSI TR-03153-TS-KuA Klarstellungen und Anwendungshinweise zur BSI TR-03153-TS und BSI-CC-PP-0105-V2-2020 vom 13. November 2020

BSI TR-03151 BSI TR-03151 – Secure Element API (SE API), Version 1.0.1 vom 20. Dezember 2018

BSI TR-03151-AMT Amendment to BSI TR-03151 Secure Element API (SE API) vom 02. Dezember 2019

BSI TR-03116-5 BSI TR-03116-5 – Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 5: Anwendungen der Secure Element API, Stand 2019 vom 01. Februar 2019

PP_SMAERS PP_SMAERS – Common Criteria Protection Profile – Security Module Application for Electronic Record-keeping Systems (SMAERS), BSI-CC-PP-0105-V2-2020, Version 1.0

PP-CSPL PP_CSPL – Common Criteria Protection Profile – Cryptographic Service Provider (CSP) Light, BSI-CC-PP-0111-2019, Version 1.0

Common Criteria Protection Profile Configurations, Cryptographic Service Provider Light – Time Stamp Service and Audit (PPC-CSPLight-TS-Au), Protection Profile-Module CSPLight Time Stamp Service and Audit (PPM-TS-Au), BSI-CC-PP-0112-2020, Version: 1.0

Common Criteria Protection Profile Configuration Cryptographic Service Provider Light - Time Stamp Service and Audit – Clustering (PPC-CSPLight-TS-Au-Cl), Protection Profile-Module CSPLight Clustering (PPM-Cl), BSI-CC-PP-0113-2020, Version: 1.0, Federal Office for In-formation Security

KassenSichV Verordnung zur Bestimmung der technischen Anforderungen an elektronische Aufzeichnungs- und Sicherungssysteme im Geschäftsverkehr

(Kassensicherungsverordnung - KassenSichV) vom 26. September 2017, Bundesgesetzblatt I, S3515

fiskaly-ARC Security Architecture - fiskaly Security Module Application for Electronic Record-keeping Systems, TOE Version 1.0.5, Document Version 1.1.4 vom 21. April 2021

fiskaly-AGD Preparative Procedures & Operational User Guideance Documentation - fiskaly Security Module Application for Electronic Record-keeping Systems, TOE Version 1.0.5, Document-Version 1.1.5 vom 06. Mai 2021