Bundesamt
für Sicherheit in der
Informationstechnik

Zertifikat

nach Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik

BSI-K-TR-0477-2021

Swissbit USB TSE, Version 1.0.4/1.1.0

der	Swissbit AG
Konformität zu:	**BSI TR-03153** – Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme
gültig bis:	24. Juni 2029

Die Konformität des Prüfgegenstands Swissbit USB TSE, Version 1.0.4/1.1.0 zur Technischen Richtlinie BSI TR-03153 wurde von einer gemäß DIN ISO/IEC 17025 anerkannten Prüfstelle überprüft und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bestätigt.

Als Prüfgrundlage für die Konformitätsprüfung diente:

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

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

Der Prüfgegenstand erfüllt die Anforderungen der Technischen Richtlinie BSI TR-03153.

Dieses Zertifikat gilt nur in Verbindung mit dem vollständigen Konformitätsreport BSI-K-TR-0477-2021. Die Gültigkeit ist ausschließlich auf die geprüfte und im Konformitätsreport angegebene Version und Konfiguration des Prüfgegenstands beschränkt.

Das Zertifizierungsverfahren wurde in Übereinstimmung mit den Bestimmungen des BSI-Schemas zur Zertifizierung nach Technischen Richtlinien durchgeführt.

Dieses Zertifikat ist keine Empfehlung des genannten Prüfgegenstands durch das Bundesamt für Sicherheit in der Informationstechnik. Eine Gewährleistung für den genannten Prüfgegenstand durch das Bundesamt für Sicherheit in der Informationstechnik ist weder enthalten noch zum Ausdruck gebracht.

Bonn, den 25. Juni 2021
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag

Sandro Amendola
Abteilungspräsident

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

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 • Infoline: +49 (0)800 274-1000 • Internet: www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Konformitätsreport

BSI-K-TR-0477-2021

Swissbit USB TSE, Version 1.0.4/1.1.0

(nach Firmware-Update von Version 1.0.4/1.0.3)

der

Swissbit AG

Leuchtenbergring 3, D-81677 München

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, zuletzt geändert durch Artikel 13 des Gesetzes vom 20. November 2019 (BGBl I S. 1626), [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 1.5 vom 14. Juni 2021, [TR-Produkte]

3 Hinweise für den Antragsteller

1. Das vom BSI erteilte Zertifikat nach Technischen Richtlinien BSI-K-TR-0477-2021 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 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

Swissbit AG
Leuchtenbergring 3
81677 München

Deutschland

Ansprechpartner:

Hubertus Grobbel (hubertus.grobbel@swissbit.com)

mit Antragsdatum 22. April 2021 (Eingangsdatum BSI: 26. April 2021) beim BSI eine Re-Zertifizierung nach Technischen Richtlinien beantragt.

Vorherige Zertifizierungen erfolgten unter folgenden Zertifizierungs-IDs:

BSI-K-TR-0412-2020
BSI-K-TR-0362-2019

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]
>
> **BSI TR-03153-TS** – Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme – Testspezifikation, Version 1.0.1 vom 05. Februar 2019, [BSI TR-03153-TS]
>
> **BSI TR-03151** – Secure Element API (SE API), Version 1.0.1 vom 20. Dezember 2018, [BSI TR-03151]
>
> **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-0105-2019, Version 0.7.5, [PP_SMAERS]
>
> **PP_CSP** – Common Criteria Protection Profile – Cryptographic Service Provider (CSP), BSI-CC-PP-0104-2019, Version 0.9.8, [PP_CSP]

6 Prüfstelle

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

Prüfbereich: BSI TR-03153

MTG AG
Prüfstelle für IT-Sicherheit
Dolivostraße 11

64293 Darmstadt
Deutschland

www.mtg.de

7 Prüfgegenstand

7.1 Beschreibung des Prüfgegenstands

Prüfgegenstand ist das IT-Produkt/-System:

Swissbit USB TSE, Version 1.0.4/1.1.0

Bei dem Prüfgegenstand handelt es sich um eine Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme gemäß Kassensicherungsverordnung [KassenSichV] in Form eines USB-Tokens.

Für die Swissbit USB TSE in der Version 1.0.4/1.0.3 wurde vom BSI das Zertifikat BSI-K-TR-0362-2019 erteilt. Zur Behebung eines Fehlers in Softwareversion 1.0.3 ist ein Firmwareupdate auf die im Rahmen des Zertifizierungsverfahrens BSI-K-TR-0412-2020 zertifizierte Version 1.1.0 erforderlich, die per UCP-Mechanismus (Update Code Package) auf die Hardwareversion 1.0.4 aufgespielt wird. Die daraus resultierende Konfiguration der Swissbit USB TSE, Version 1.0.4/1.1.0 ist der Prüfgegenstand dieses Zertifizierungsverfahrens.

7.2 Komponenten des Prüfgegenstands

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

Tabelle 1: Komponenten des Prüfgegenstands

Swissbit USB TSE, Version 1.0.4/1.1.0			
Nr	**Typ**	**Identifier**	**Release**
1	HW	Swissbit TSE SMAERS Hardware[1]	v1.0.4
2	FW	Swissbit TSE SMAERS Firmware[2]	v1.1.0
3	SW/ HW	CSP[3]	TCOS CSP 2.0 Release 1/P60D145

7.3 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].

1 BSI Zertifizierungs-ID (Common Criteria, [PP_SMAERS]) für diese Komponente: BSI-DSZ-CC-1121
2 BSI Zertifizierungs-ID (Common Criteria, [PP_SMAERS]) für diese Komponente: BSI-DSZ-CC-1121-V2
3 BSI Zertifizierungs-ID (Common Criteria, [PP_CSP]) für diese Komponente: BSI-DSZ-CC-1118-2020

Tabelle 2: Unterstützte Profile

Profile ID	**Supported** (Yes/No)	**Comment**
STORAGE_BASIC	Yes	Has local storage (6.5 GB)
STORAGE_REMOTE	No	
SM_BASIC	Yes	Has a local Secure Element (384 bit ECDSA, signature time <250ms)
SM_NOAGG	Yes	Supports signed transaction updates (saves 1 signature per receipt)
SM_AGG	No	
SM_MULTI	Yes	Supports managing multiple transactions in parallel (up to 512)
SM_REMOTE	No	
SDI	No	
SDI_RESTORE	No	
SDI_DELETE	Yes	Supports method deleteStoredData
CUSTOM_INTEGRATION_INTERFACE	Yes	Manufacture specific interface (Android, Linux, Windows, Java, embedded)
TIME_SYNC	No	
NO_TIME_SYNC	Yes	Time is set by host
MULTI_CLIENT	Yes	Supports multiple clients (up to 100)
NO_MULTI_CLIENT	No	

Der Prüfgegenstand implementiert nicht die standardisierte Einbindungsschnittstelle gemäß [BSI TR-03151] (Profil: SDI).

Die herstellerspezifische Einbindungsschnittstelle (Profil: CUSTOM_INTEGRATION_INTERFACE) des Prüfgegenstands implementiert jedoch alle Funktionen gemäß [BSI TR-03153], Kapitel 5.2 außer:

- restoreFromBackup
- exportCertificates
- exportSerialNumbers

Bei folgenden Funktionalitäten gelten Einschränkungen:

- logOut – kein zeitgesteuertes Abmelden von *Admin* bzw. *TimeAdmin* implementiert
- exportData – die Anzahl der zu exportierenden Records kann ich begrenzt werden

Tabelle 3: Verwendeter Signaturalgorithmus

Verwendete Kryptofunktionen	Angaben des Antragstellers
Signaturalgorithmus	ECDSA
Parameter zum Signaturalgorithmus (inkl. Hashfunktion und Schlüssellängen	bsiEcdsaWithSHA384 (Object Identifier 0.4.0.127.0.7.1.1.4.1.4) 384 bit ECC Key der Kurve brainpoolP384r1 mit SHA384 als Hashalgorithmus

8 Konformitätsprüfung

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

Um die Konformität des Prüfgegenstands zu [BSI TR-03153] nach dem durchgeführten Firmwareupdate sicherzustellen, wurden im Rahmen der Konformitätsprüfung verschiedene Szenarien anhand ausgewählter Testfälle betrachtet.

1. Szenario A – Firmware-Update mit unbenutzter TSE v1.0.4/1.0.3
2. Szenario B – Firmware-Update mit bereits benutzter TSE v1.0.4/1.0.3 benutzt und teilweise befülltem TSE Store
3. Szenario C – Unbenutzte TSE v1.0.4/1.0.3 & unbenutzte TSE v1.0.4/1.1.0; Abgleich ob Log Nachrichten beider TSEn bei gleicher Befüllung identisch sind

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.

Tabelle 4 enthält die Zusammenfassung der durchgeführten Testfälle. Für Szenario A & B wurden dabei identische Prüfergebnisse erzielt.

Bei der Analyse der Log Nachrichten gemäß Szenario C konnten, keine Unterschiede zwischen den beiden TSE Versionen identifiziert werden.

Tabelle 4: 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.
STO_FUN_02	SM_NOAGG	Pass
STO_FUN_03	SM_AGG	n.a.
STO_FUN_04	SM_NOAGG	Pass
STO_FUN_05	SM_AGG	n.a.
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	-
5.1.3 Prüfungen der Zuverlässigkeit von Speichermedien (STO_REL)		
STO_REL_01	STORAGE_BASIC	-
5.1.4 Prüfungen für fernverbundene Speichermedien (STO_REM)		
STO_REM_01	STORAGE_REMOTE	n.a.

Testcase ID	Profile	Verdict
5.1 Modul Storage – Speichermedium (STO)		
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.
SM_CON_03	SM_NOAGG	Pass
SM_CON_04	SM_AGG	n.a.
SM_CON_05	SM_AGG	n.a.
SM_CON_06	SM_NOAGG SM_MULTI	Pass
SM_CON_07	SM_AGG SM_MULTI	n.a.
SM_CON_08	SM_NOAGG SM_MULTI	Pass
SM_CON_09	SM_AGG SM_MULTI	n.a.
SM_CON_10	SM_AGG SM_MULTI	n.a.
SM_CON_11	SM_AGG SM_MULTI	n.a.
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	Pass
SM_TME_05	SM_AGG SM_MULTI	n.a.
SM_TME_06	SM_NOAGG SM_MULTI	Pass
SM_TME_07	SM_NOAGG	Pass
SM_TME_08	SM_AGG	n.a.
SM_TME_09	SM_BASIC SDI	Pass

Testcase ID	Profile	Verdict
5.1 Modul Storage – Speichermedium (STO)		
SM_TME_10	SM_AGG	n.a.[4]
SM_TME_11	SM_BASIC	Pass
5.2.3 Prüfungen zum Signaturzähler im Sicherheitsmodul (SM_SIG)		
SM_SIG_01	SM_NOAGG	Pass
SM_SIG_02	SM_AGG	n.a.
SM_SIG_03	SM_NOAGG SM_MULTI	Pass
SM_SIG_04	SM_AGG	n.a.
SM_SIG_05	SM_BASIC	-
SM_SIG_06	SM_NOAGG	Pass
SM_SIG_07	SM_AGG	n.a.
SM_SIG_08	SM_BASIC SDI	Pass
5.2.4 Prüfungen zur Transaktionsnummer im Sicherheitsmodul (SM_TRA)		
SM_TRA_01	SM_BASIC	-
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	-
SM_KRY_02	SM_BASIC	Pass
SM_KRY_03	SM_BASIC	Pass
SM_KRY_04	SM_BASIC	Pass
5.2.6 Prüfungen der PKI von Sicherheitsmodulen (SM_PKI)		
SM_PKI_01	SM_BASIC	-
SM_PKI_02	SM_BASIC	-
SM_PKI_03	SM_BASIC	-
5.2.7 Prüfungen für fernverbundene Sicherheitsmodule (SM_REM)		
SM_REM_01	SM_REMOTE	n.a.
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.
5.3.1.2 Initialisierung der Technischen Sicherheitseinrichtung (II_INI)		
II_INI_01	SM_BASIC	n.a.[5]

4 Zeit wird in SM nicht zwischengespeichert.

Testcase ID	Profile	Verdict
5.1 Modul Storage – Speichermedium (STO)		
II_INI_02	SM_BASIC	n.a.[6]
II_INI_03	SM_BASIC	Pass
II_INI_04	SM_BASIC	Pass
II_INI_05	SM_BASIC	Pass
II_INI_06	SM_BASIC	n.a.[7]
II_INI_07	SM_BASIC	Pass
II_INI_08	SM_BASIC	Pass
II_INI_09	SM_BASIC	Pass
II_INI_10	SM_BASIC	Pass
II_INI_11	SM_BASIC	Pass
II_INI_12	SM_BASIC	Pass
II_INI_13	SM_BASIC SM_REMOTE	n.a.
II_INI_14	SM_BASIC STORAGE_REMOTE	n.a.
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	n.a.
II_DSE_07	SM_BASIC STORAGE_REMOTE	n.a.
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	Pass
II_STA_04	SM_BASIC	Pass
II_STA_05	SM_BASIC	Pass
II_STA_06	SM_BASIC SM_REMOTE	n.a.
II_STA_07	SM_BASIC STORAGE_REMOTE	n.a.
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

5 Description wird vom Hersteller gesetzt.
6 Description wird vom Hersteller gesetzt.
7 Description wird vom Hersteller gesetzt.

Testcase ID	Profile	Verdict
5.1 Modul Storage – Speichermedium (STO)		
II_UPD_03	SM_AGG	n.a.
II_UPD_04	SM_NOAGG	Pass
II_UPD_05	SM_BASIC SM_REMOTE	n.a.
II_UPD_06	SM_BASIC STORAGE_REMOTE	n.a.
II_UPD_07	SM_AGG STORAGE_REMOTE	n.a.
II_UPD_08	SM_BASIC SM_NOAGG	Pass
II_UPD_09	SM_BASIC SM_AGG	n.a.
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	Pass
II_FIN_04	SM_BASIC	Pass
II_FIN_05	SM_BASIC SM_REMOTE	n.a.
II_FIN_06	SM_BASIC STORAGE_REMOTE	n.a.
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.
II_MCU_03	MULTI_CLIENT SM_NOAGG	Pass
II_MCU_04	MULTI_CLIENT SM_AGG	n.a.
II_MCU_05	MULTI_CLIENT SM_BASIC	Pass
II_MCU_06	NO_MULTI_CLIENT SM_BASIC	n.a.
5.3.2 Prüfungen der Einbindungsschnittstellen gemäß BSI TR-03153		
5.3.2.1 Aktualisierung der Uhrzeit (SDI_UDT)		
SDI_UDT_01	SDI	Pass

Testcase ID	Profile	Verdict
5.1 Modul Storage – Speichermedium (STO)		
	NO_TIME_SYNC	
SDI_UDT_02	SDI TIME_SYNC	n.a.
SDI_UDT_03	SDI NO_TIME_SYNC	Pass
SDI_UDT_04	SDI SM_REMOTE	n.a.
SDI_UDT_05	SDI STORAGE_REMOTE	n.a.
SDI_UDT_06	SDI	Pass
SDI_UDT_07	SDI	Pass[8]
5.3.2.2 Export des Archivs (SDI_EXP)		
SDI_EXP_01	SDI	Pass
SDI_EXP_02	SDI	Pass
SDI_EXP_03	SDI	Pass[9]
SDI_EXP_04	SDI	Pass
SDI_EXP_05	SDI	Pass
SDI_EXP_06	SDI	Pass
SDI_EXP_07	SDI	Pass[10]
SDI_EXP_08	SDI	Pass[11]
SDI_EXP_09	SDI	Pass
SDI_EXP_10	SDI	Pass
SDI_EXP_11	SDI	Pass
SDI_EXP_12	SDI	Pass
SDI_EXP_13	SDI	Pass
SDI_EXP_14	SDI	Pass[12]
SDI_EXP_15	SDI	Pass[13]
SDI_EXP_16	SDI	n.a.[14]
SDI_EXP_17	SDI	n.a.[15]
SDI_EXP_18	SDI	n.a.[16]
SDI_EXP_19	SDI	Pass
SDI_EXP_20	SDI	Pass
SDI_EXP_21	SDI	Pass
SDI_EXP_22	SDI	Pass
SDI_EXP_23	SDI	Pass

8 Siehe Kapitel 8.1.1
10 Siehe Kapitel 8.1.1
16 Parameter *maximumNumberRecords* <> 0
15 Parameter *maximumNumberRecords* <> 0
14 Parameter *maximumNumberRecords* <> 0
13 Siehe Kapitel 8.1.1
12 Siehe Kapitel 8.1.1
11 Siehe Kapitel 8.1.1
9 Siehe Kapitel 8.1.1

Testcase ID	Profile	Verdict
5.1 Modul Storage – Speichermedium (STO)		
SDI_EXP_24	SDI	Pass
SDI_EXP_25	SDI	Pass
SDI_EXP_26	SDI	Pass
SDI_EXP_27	SDI	n.a.[17]
SDI_EXP_28	SDI	n.a.[18]
SDI_EXP_29	SDI	Pass
SDI_EXP_30	SDI	Pass[19]
SDI_EXP_31	SDI	n.a.[20]
SDI_EXP_32	SDI	Pass
SDI_EXP_33	SDI	Pass
SDI_EXP_34	SDI	Pass
SDI_EXP_35	SDI	Pass
SDI_EXP_36	SDI	Pass
SDI_EXP_37	SDI	Pass
SDI_EXP_38	SDI	Pass
SDI_EXP_39	SDI	n.a.[21]
SDI_EXP_40	SDI	n.a.[22]
SDI_EXP_41	SDI	n.a.[23]
SDI_EXP_42	SDI	Pass
5.3.2.3 Zertifikatsabruf (SDI_EXC)		
SDI_EXC_01	SDI	n.a.[24]
5.3.2.4 Wiederherstellen durch ein Backup (SDI_RFB)		
SDI_RFB_01	SDI_RESTORE	n.a.[25]
SDI_RFB_02	SDI_RESTORE	n.a.[26]
SDI_RFB_03	SDI_RESTORE STORAGE_REMOTE	n.a.[27]
SDI_RFB_04	SDI_RESTORE	n.a.[28]
SDI_RFB_05	SDI_RESTORE	n.a.[29]
5.3.2.5 Lesen einer Log-Nachricht (SDI_RLM)		
SDI_RLM_01	SDI SM_NOAGG	Pass

17 Parameter *maximumNumberRecords* <> 0
18 Parameter *maximumNumberRecords* <> 0
19 Siehe Kapitel 8.1.1
20 Parameter *maximumNumberRecords* <> 0
21 Parameter *maximumNumberRecords* <> 0
22 Parameter *maximumNumberRecords* <> 0
23 Parameter *maximumNumberRecords* <> 0
24 exportCertificates nicht implementiert
25 restoreFromBackup nicht implementiert
26 restoreFromBackup nicht implementiert
27 restoreFromBackup nicht implementiert
28 restoreFromBackup nicht implementiert
29 restoreFromBackup nicht implementiert

Testcase ID	Profile	Verdict
5.1 Modul Storage – Speichermedium (STO)		
SDI_RLM_02	SDI SM_AGG	n.a.
SDI_RLM_03	SDI SM_REMOTE	n.a.
5.3.2.6 Export von Seriennummern (SDI_ESN)		
SDI_ESN_01	SDI	n.a.[30]
SDI_ESN_02	SDI	n.a.[31]
SDI_ESN_03	SDI	n.a.[32]
5.3.2.7 Initialisierung der Sicherheitseinrichtung (SDI_INI)		
SDI_INI_01	SDI	Pass
SDI_INI_02	SDI	Pass
SDI_INI_03	SDI	Pass
SDI_INI_04	SDI	Pass[33]
SDI_INI_05	SDI	Pass
5.3.2.8 Außerbetriebnahme des Sicherheitsmoduls (SDI_DSE)		
SDI_DSE_01	SDI	Pass
SDI_DSE_02	SDI	Pass[34]
SDI_DSE_03	SDI	Pass
5.3.2.9 Abfrage der maximalen Anzahl von simultanen Clients der TSE (SDI_MNC)		
SDI_MNC_01	SDI MULTI_CLIENT	Pass
5.3.2.10 Abfrage der aktuellen Anzahl von Clients der TSE (SDI_CNC)		
SDI_CNC_01	SDI MULTI_CLIENT	Pass
SDI_CNC_02	SDI MULTI_CLIENT	Pass
SDI_CNC_03	SDI MULTI_CLIENT	Pass
SDI_CNC_04	SDI MULTI_CLIENT	Pass
5.3.2.11 Abfrage der maximalen Anzahl von parallelen Transaktionen (SDI_MNT)		
SDI_MNT_01	SDI SM_MULTI	Pass
5.2.3.12 Abfrage aktuelle Anzahl parallel geöffneter Transaktionen (SDI_CNT)		
SDI_CNT_01	SDI SM_MULTI	Pass
SDI_CNT_02	SDI SM_MULTI	Pass
SDI_CNT_03	SDI	Pass

30 eExportSerialNumber nicht implementiert
31 eExportSerialNumber nicht implementiert
32 eExportSerialNumber nicht implementiert
33 Siehe Kapitel 8.1.1
34 Siehe Kapitel 8.1.1

Testcase ID	Profile	Verdict
5.1 Modul Storage – Speichermedium (STO)		
	SM_MULTI	
SDI_CNT_04	SDI SM_MULTI	Pass
5.3.2.13 Abfrage unterstützte Varianten der Aktualisierungen von Transaktionen (SDI_UTV)		
SDI_UTV_01	SDI	Pass
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.
SDI_DSD_04	SDI	Pass[35]
SDI_DSD_05	SDI	Pass
5.3.2.15 Authentifizierung von Benutzern der TSE (SDI_AUT)		
SDI_AUT_01	SDI	Pass
SDI_AUT_02	SDI	Pass
SDI_AUT_03	SDI	Pass[36]
SDI_AUT_04	SDI	Pass[37]
SDI_AUT_05	SDI	Pass[38]
SDI_AUT_06	SDI SM_REMOTE	n.a.
SDI_AUT_07	SDI STORAGE_REMOTE	n.a.
5.3.2.16 Abmeldung von Benutzern der TSE (SDI_LGO)		
SDI_LGO_01	SDI	Pass[39]
SDI_LGO_02	SDI	Pass
SDI_LGO_03	SDI	Pass
SDI_LGO_04	SDI	n.a.[40]
SDI_LGO_05	SDI SM_REMOTE	n.a.
SDI_LGO_06	SDI STORAGE_REMOTE	n.a.
5.3.2.17 Entsperren von Benutzern(SDI_UBU)		
SDI_UBU_01	SDI	Pass
SDI_UBU_02	SDI	Pass
SDI_UBU_03	SDI	Pass
SDI_UBU_04	SDI	Pass
SDI_UBU_05	SDI	n.a.

35 Siehe Kapitel 8.1.1
36 Siehe Kapitel 8.1.1
37 Siehe Kapitel 8.1.1
38 Siehe Kapitel 8.1.1
39 Siehe Kapitel 8.1.1
40 Kein zeitgesteuertes automatisches Logout.

Testcase ID	Profile	Verdict
5.1 Modul Storage – Speichermedium (STO)		
	SM_REMOTE	
SDI_UBU_06	SDI STORAGE_REMOTE	n.a.
5.3.3 Prüfungen für herstellerspezifische Einbindungsschnittstellen (CI)		
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	n.a.
CI_UDT_03	CUSTOM_INTEGRATION_ INTERFACE STORAGE_REMOTE	n.a.
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	n.a.[41]
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.
EXP_LOG_10	SM_AGG	n.a.
EXP_LOG_11	SM_NOAGG	Pass
EXP_LOG_12	SM_AGG	n.a.
EXP_LOG_13	SM_BASIC	n.a.[42]
EXP_LOG_14	SM_BASIC	Pass
EXP_LOG_15	SM_BASIC	Pass
EXP_LOG_16	SM_BASIC	Pass

41 Description wird durch Hersteller gesetzt.
42 Description wird durch Hersteller gesetzt.

Testcase ID	Profile	Verdict
5.1 Modul Storage – Speichermedium (STO)		
EXP_LOG_17	SM_BASIC	Pass
5.4.4 Zertifikatsexport (EXP_CER)		
EXP_CER_01	SM_BASIC	Pass

8.1 Festgestellte Abweichungen

8.1.1 Abweichende Fehlercodes

Festgestellte Abweichung: Beim Testen der SE-API Funktionen gemäß dem Profil SDI wurden bei einigen Testfällen Abweichungen zu den dort spezifizierten Fehlercodes festgestellt (→ Tabelle 5).

Tabelle 5: Abweichende Fehlercodes

Testfall	Spezifizierter Fehlercode	Tatsächlicher Fehlercode
SDI_UDT_07	ErrorUserNotAuthenticated	ERROR_USER_NOT_AUTHORIZED
SDI_EXP_03	ErrorTransactionNumberNot-Found	ERROR_NO_DATA_AVAILABLE
SDI_EXP_07	ErrorTransactionNumberNot-Found	ERROR_NO_DATA_AVAILABLE
SDI_EXP_08	ErrorIdNotFound	ERROR_NO_DATA_AVAILABLE
SDI_EXP_14	ErrorTransactionNumberNot-Found	ERROR_NO_DATA_AVAILABLE
SDI_EXP_15	ErrorIdNotFound	ERROR_NO_DATA_AVAILABLE
SDI_EXP_30	ErrorIdNotFound	ERROR_NO_DATA_AVAILABLE
SDI_INI_04	ErrorUserNotAuthenticated	ERROR_USER_NOT_AUTHORIZED
SDI_DSE_02	ErrorUserNotAuthenticated	ERROR_USER_NOT_AUTHORIZED
SDI_DSD_04	ErrorUserNotAuthenticated	ERROR_USER_NOT_AUTHORIZED
SDI_AUT_03	ErrorUserNotAuthenticated	ERROR_USER_NOT_AUTHORIZED
SDI_AUT_04	ErrorUserNotAuthenticated	ERROR_USER_NOT_AUTHORIZED
SDI_AUT_05	ErrorUserNotAuthenticated	ERROR_USER_NOT_AUTHORIZED
SDI_LGO_01	ErrorUserNotAuthenticated	ERROR_USER_NOT_AUTHORIZED

Bewertung: Da der Prüfgegenstand gemäß ICS über eine herstellerspezifische Einbindungsschnittstelle verfügt, besitzt die Abweichung keine Relevanz für die Feststellung der Konformität zur [BSI TR-03153].

Erforderliche Maßnahme: -

9 Ergebnis der Konformitätsprüfung

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

MTG AG Prüfbericht zum Konformitätsrest nach
BSI TR-03153 / TR-03153-TS
Swissbit USB TSE v1.0.4/1.1.0
BSI-K-TR-0477
Version 1.0
Erstellungsdatum: 20. Mai 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;
- alle relevanten Testfälle des Moduls *Integration Interface – Einbindungsschnittstelle* konnten mit „Pass“ bewertet werden;
- alle relevanten Testfälle des Moduls *Prüfung der Exportdaten gemäß BSI TR-03153* konnten mit „Pass“ bewertet werden.

Das erzielte Gesamtergebnis der Konformitätsprüfung ist: Pass

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-0477-2021 vom 25. Juni 2021 bestätigt.

Das Zertifikat nach Technischen Richtlinien ist gültig bis zum 24. Juni 2029.

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, zuletzt geändert durch Artikel 13 des Gesetzes vom 20. November 2019 (BGBl I S. 1626)
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
VB-Produkte	Verfahrensbeschreibung zur Zertifizierung von Produkten, Version 2.5 vom 19. März 2020
KassenSichV	Verordnung zur Bestimmung der technischen Anforderungen an elektronische Aufzeichnungs- und Sicherungssysteme im Geschäftsverkehr (Kassensicherungsverordnung - KassenSichV) vom 26. September 2017, Bundesgesetzblatt I, S3515
PP_CSP	PP_CSP – Common Criteria Protection Profile – Cryptographic Service Provider (CSP), BSI-CC-PP-0104-2019, Version 0.9.8
PP_SMAERS	PP_SMAERS – Common Criteria Protection Profile – Security Module Application for Electronic Record-keeping Systems (SMAERS), BSI-CC-PP-0105-2019, Version 0.7.5
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
BSI TR-03151	BSI TR-03151 – Secure Element API (SE API), Version 1.0.1 vom 20. Dezember 2018
BSI TR-03153-TS	BSI TR-03153 – Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme – Testspezifikation, Version 1.0.1 vom 05. Februar 2019
BSI TR-03153	BSI TR-03153 – Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, Version 1.0.1 vom 20. Dezember 2018
TR-Produkte	Anforderungen an Antragsteller zur Zertifizierung von Produkten nach Technischen Richtlinien, Version 1.5 vom 14. Juni 2021
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