Bundesamt
für Sicherheit in der
Informationstechnik

Konformitätsreport

BSI-K-TR-0482-2023

cryptovision TSE v2

der

cv cryptovision GmbH
Munscheidstraße 14, 45886 Gelsenkirchen

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 10. September 2021, Bundesgesetzblatt I, S. 1359, [BMIBGebV]
- Verfahrensbeschreibung zur Zertifizierung von Produkten, Prozessen und Dienstleistungen, Version 3.2 vom28. Oktober 2022, [VB-Produkte.PD]
- Zertifizierung von Produkten, Prozessen und Dienstleistungen: Programm Technische Richtlinien (TR), Version 2.2 vom 31. Januar 2023, [TR-Produkte.PD]

3 Hinweise für den Antragsteller

1. Das vom BSI erteilte Zertifikat nach Technischen Richtlinien BSI-K-TR-0482-2023 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

cv cryptovision GmbH
Munscheidstraße 14
45886 Gelsenkirchen

Deutschland

Ansprechpartner:

Thomas Zeggel (thomas.zeggel@atos.net)
Franziska Tesche (franziska.tesche@atos.net)

mit Antragsdatum 20. Mai 2021 (Eingangsdatum BSI: 02. Juni 2021) beim BSI eine Re-Zertifizierung nach Technischen Richtlinien beantragt.

Vorherige Zertifizierungen erfolgten unter folgenden Zertifizierungs-IDs:

BSI-K-TR-0374-2020

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]

Darüber hinaus waren folgende Dokumente von Relevanz für Konformitätsprüfung:

> **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, vom 23. Februar 2021 [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:

TÜV Informationstechnik GmbH
Prüfstelle für IT-Sicherheit
Am TÜV 1

45307 Essen

7 Prüfgegenstand

7.1 Beschreibung des Prüfgegenstands

Prüfgegenstand ist das IT-Produkt/-System:

cryptovision TSE v2

Bei dem Prüfgegenstand handelt es sich um eine Technische Sicherheitseinrichtung (TSE) gemäß [BSI TR-03153] in Form einer Micro-SD-Karte, die per Adapter auch als reguläre SD-Karte und USB-Token betrieben werden kann. Der Prüfgegenstand wird von der Cryptovision GmbH entwickelt sowie produziert.

7.2 Komponenten des Prüfgegenstands

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

Tabelle 1: Komponenten des Prüfgegenstands

cryptovision TSE v2			
Nr	**Typ**	**Identifier**	**Bemerkung**
Hardware – Phison Micro-SD card v1.4			
1	HW	Secure Element NXP SE051	Das Sicherheitsmodul NXP SE 051 läuft auf dem Java Card Operating System JCOP 4 SE051 v4.7 R3.01.11 und ist die Plattform für CSP und SMAERS.
2	HW	General Purpose IC NXP LPC54114	
3	HW	Toshiba 8GB Flash Memory	
4	HW	Phison Flash Controller PH8210	
Interne Software der TSE			
5	SW	Cryptovision „Jacolyn" CSP – Cryptographic Service Provider v2.0.3 Rev 18611 RC1	
6	SW	Cryptovision SMAERS – Security Module Application for Record-keeping Systems v2.0.3, Rev 18611 RC	
7	SW	Cryptovision TSE Firmware für die Kommunikation (Transport Layer), v2.0 with identifier 565	
8	SW	Phison Flash-Controller Firmware für Ansteuerung des Flash-Speichers; Version b20	

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].

Tabelle 2: Unterstützte Profile

Die TSE...	**Profile ID**	**Supported** (Yes/No)
verfügt über ein Speichermedium	STORAGE_BASIC	Yes
hat ein fernverbundenes Speichermedium	STORAGE_REMOTE	No
verfügt über ein Sicherheitsmodul	SM_BASIC	Yes
hat ein fernverbundenes Sicherheitsmodul	SM_REMOTE	No
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[1]
besitzt eine herstellerspezifische Einbindungsschnittstelle und setzt den Export-Teil der Einheitlichen Digitalen Schnittstelle um	CUSTOM_INTEGRATION_INTERFACE	No
implementiert alle Funktionen der Einheitlichen Digitalen Schnittstelle gemäß BSI TR-03153	SDI	Yes
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	TIME_SYNC	No

1 Anzahl der maximal parallel offenen Transaktionen: 320

eigenständigen Stellen der Zeit des Sicherheitsmoduls		
verfügt über keinen Mechanismus zum eigenständigen Stellen der Zeit des Sicherheitsmoduls	NO_TIME_SYNC	Yes
kann von mehreren Clients gleichzeitig für die Protokollierung von Transaktionen verwendet werden	MULTI_CLIENT	Yes
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
Parameter zum Signaturalgorithmus (inkl. Hashfunktion und Schlüssellängen	ECDSA-plain-SHA256, 0.4.0.127.0.7.1.1.4.1.3

Tabelle 4: Zusätzliche Angaben

Gegenstand	Angaben des Antragstellers
Größe des internen Speichers des Sicherheitsmoduls	2,5625 GByte
Zeitlicher Abstand in dem das Sicherheitsmodul die intern verwaltete Zeit in seinem nichtflüchtigen Speicher speichert	Entfällt, keine Speicherung
Welche Zeitformate werden von der TSE unterstützt ?	UNIX Time
Maximale Anzahl von Clients, die die TSE gleichzeitig zur Absicherung von Transaktionen nutzen können	128
Maximale Anzahl der parallel geöffneten Transaktionen, die das Sicherheitsmodul verwalten kann	320

8 Konformitätsprüfung

Die Konformitätsprüfung wurde im Zeitraum Mai 2021 bis Mai 2023 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.[2]
STO_FUN_02	SM_NOAGG	Pass
STO_FUN_03	SM_AGG	n.a.[3]
STO_FUN_04	SM_NOAGG	Pass
STO_FUN_05	SM_AGG	n.a.[4]
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.[5]
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.[6]
SM_CON_03	SM_NOAGG	Pass

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

Testcase ID	Profile	Verdict
SM_CON_04	SM_AGG	n.a.[7]
SM_CON_05	SM_AGG	n.a.[8]
SM_CON_06	SM_NOAGG, SM_MULTI	Pass
SM_CON_07	SM_AGG, SM_MULTI	n.a.[9]
SM_CON_08	SM_NOAGG, SM_MULTI	Pass
SM_CON_09	SM_AGG, SM_MULTI	n.a.[10]
SM_CON_10	SM_AGG, SM_MULTI	n.a.[11]
SM_CON_11	SM_AGG, SM_MULTI	n.a.[12]
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	n.a.[13]
SM_CON_16	SM_BASIC, SDI	n.a.[14]
SM_CON_17	SM_BASIC, SDI	n.a.[15]
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.[16]
SM_TME_06	SM_NOAGG, SM_MULTI	Pass
SM_TME_07	SM_NOAGG	Pass
SM_TME_08	SM_AGG	n.a.[17]
SM_TME_09	SM_BASIC, SDI	Pass
SM_TME_10	SM_AGG	n.a.[18]
SM_TME_11	SM_BASIC	n.a.[19]
5.2.3 Prüfungen zum Signaturzähler im Sicherheitsmodul (SM_SIG)		
SM_SIG_01	SM_NOAGG	Pass
SM_SIG_02	SM_AGG	n.a.[20]
SM_SIG_03	SM_NOAGG, SM_MULTI	Pass
SM_SIG_04	SM_AGG	n.a.[21]
SM_SIG_05	SM_BASIC	Pass

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_AGG
13 n.a. wegen Profil SDI
14 n.a. wegen Profil SDI
15 n.a. wegen Profil SDI
16 n.a. wegen Profil SDI
17 n.a. wegen Profil SDI
18 Testcase nicht verpflichtend gemäß [BSI TR-03153-TS-ERG]
19 Testcase nicht verpflichtend gemäß [BSI TR-03153-TS-ERG]
20 n.a. wegen Profil SDI
21 n.a. wegen Profil SDI

Testcase ID	Profile	Verdict
SM_SIG_06	SM_NOAGG	Pass
SM_SIG_07	SM_AGG	n.a.[22]
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.[23]
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	n.a.[24]
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.[25]
5.3.1.2 Initialisierung der Technischen Sicherheitseinrichtung (II_INI)		
II_INI_01	SM_BASIC	n.a.[26]
II_INI_02	SM_BASIC	n.a.[27]
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.[28]
II_INI_07	SM_BASIC	Pass
II_INI_08	SM_BASIC	Pass
II_INI_09	SM_BASIC	Pass

22 n.a. wegen Profil SDI
23 Testcase nicht verpflichtend gemäß [BSI TR-03153-TS-ERG]
24 n.a. wegen Profil SM_REMOTE
25 n.a. wegen Profil STORAGE_REMOTE
26 Siehe Kapitel 8.2.2
27 Siehe Kapitel 8.2.2
28 Siehe Kapitel 8.2.2

Testcase ID	Profile	Verdict
II_INI_10	SM_BASIC	Pass
II_INI_11	SM_BASIC	n.a.[29]
II_INI_12	SM_BASIC	Pass
II_INI_13	SM_BASIC, SM_REMOTE	n.a.[30]
II_INI_14	SM_BASIC, STORAGE_REMOTE	n.a.[31]
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.[32]
II_DSE_07	SM_BASIC, STORAGE_REMOTE	n.a.[33]
5.3.1.4 Starten einer Transaktion (II_STA)		
II_STA_01	SM_BASIC	n.a.[34]
II_STA_02	SM_BASIC	Pass
II_STA_03	SM_BASIC	n.a.[35]
II_STA_04	SM_BASIC	n.a.[36]
II_STA_05	SM_BASIC	n.a.[37]
II_STA_06	SM_BASIC, SM_REMOTE	n.a.[38]
II_STA_07	SM_BASIC, STORAGE_REMOTE	n.a.[39]
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	n.a.[40]
II_UPD_02	SM_NOAGG	Pass
II_UPD_03	SM_AGG	n.a.[41]
II_UPD_04	SM_NOAGG	n.a.[42]
II_UPD_05	SM_BASIC, SM_REMOTE	n.a.[43]
II_UPD_06	SM_BASIC, STORAGE_REMOTE	n.a.[44]
II_UPD_07	SM_AGG, STORAGE_REMOTE	n.a.[45]

29 n.a. da Zeit in der TSE bei 0 startet; daher Zertifikat nie abgelaufen
30 n.a. wegen Profil SM_REMOTE
31 n.a. wegen Profil STORAGE_REMOTE
32 n.a. wegen Profil SM_REMOTE
33 n.a. wegen Profil STORAGE_REMOTE
34 Siehe Kapitel 8.2.1
35 Siehe Kapitel 8.2.1
36 Siehe Kapitel 8.2.1
37 Siehe Kapitel 8.2.1
38 n.a. wegen Profil SM_REMOTE
39 n.a. wegen Profil STORAGE_REMOTE
40 Siehe Kapitel 8.2.1
41 n.a. wegen Profil SM_AGG
42 Siehe Kapitel 8.2.1
43 n.a. wegen Profil SM_REMOTE
44 n.a. wegen Profil STORAGE_REMOTE
45 n.a. wegen Profil STORAGE_REMOTE

Testcase ID	Profile	Verdict
II_UPD_08	SM_BASIC, SM_NOAGG	Pass
II_UPD_09	SM_BASIC, SM_AGG	n.a.[46]
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.[47]
II_FIN_04	SM_BASIC	n.a.[48]
II_FIN_05	SM_BASIC, SM_REMOTE	n.a.[49]
II_FIN_06	SM_BASIC, STORAGE_REMOTE	n.a.[50]
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.[51]
II_MCU_03	MULTI_CLIENT, SM_NOAGG	Pass
II_MCU_04	MULTI_CLIENT, SM_AGG	n.a.[52]
II_MCU_05	MULTI_CLIENT, SM_BASIC	Pass
II_MCU_06	NO_MULTI_CLIENT, SM_BASIC	n.a.[53]
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	Pass
SDI_UDT_02	SDI, TIME_SYNC	n.a.[54]
SDI_UDT_03	SDI, NO_TIME_SYNC	Pass
SDI_UDT_04	SDI, SM_REMOTE	n.a.[55]
SDI_UDT_05	SDI, STORAGE_REMOTE	n.a.[56]
SDI_UDT_06	SDI	Pass
SDI_UDT_07	SDI	Pass
5.3.2.2 Export des Archivs (SDI_EXP)		

46 n.a. wegen Profil SM_AGG
47 Siehe Kapitel 8.2.1
48 Siehe Kapitel 8.2.1
49 n.a. wegen Profil SM_REMOTE
50 n.a. wegen Profil STORAGE_REMOTE
51 n.a. wegen Profil SM_AGG
52 n.a. wegen Profil SM_AGG
53 n.a. wegen Profil NO_MULTI_CLIENT
54 n.a. wegen Profil NO_TIME_SYNC
55 n.a. wegen Profil SM_REMOTE
56 n.a. wegen Profil STORAGE_REMOTE

Testcase ID	Profile	Verdict
SDI_EXP_01	SDI	Pass
SDI_EXP_02	SDI	Pass
SDI_EXP_03	SDI	Pass
SDI_EXP_04	SDI	n.a.[57]
SDI_EXP_05	SDI	Pass
SDI_EXP_06	SDI	Pass
SDI_EXP_07	SDI	Pass
SDI_EXP_08	SDI	Pass
SDI_EXP_09	SDI	n.a.[58]
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
SDI_EXP_15	SDI	Pass
SDI_EXP_16	SDI	Pass
SDI_EXP_17	SDI	Pass
SDI_EXP_18	SDI	Pass
SDI_EXP_19	SDI	n.a.[59]
SDI_EXP_20	SDI	Pass
SDI_EXP_21	SDI	Pass
SDI_EXP_22	SDI	Pass
SDI_EXP_23	SDI	Pass
SDI_EXP_24	SDI	Pass
SDI_EXP_25	SDI	Pass
SDI_EXP_26	SDI	Pass
SDI_EXP_27	SDI	Pass
SDI_EXP_28	SDI	Pass
SDI_EXP_29	SDI	Pass
SDI_EXP_30	SDI	Pass
SDI_EXP_31	SDI	Pass
SDI_EXP_32	SDI	Pass
SDI_EXP_33	SDI	Pass
SDI_EXP_34	SDI	Pass
SDI_EXP_35	SDI	Pass
SDI_EXP_36	SDI	n.a.[60]
SDI_EXP_37	SDI	Pass
SDI_EXP_38	SDI	Pass
SDI_EXP_39	SDI	Pass

57 Siehe Kapitel 8.2.1
59 Siehe Kapitel 8.2.1
58 Siehe Kapitel 8.2.1
60 Siehe Kapitel 8.2.1

Testcase ID	Profile	Verdict
SDI_EXP_40	SDI	Pass
SDI_EXP_41	SDI	Pass
SDI_EXP_42	SDI	n.a.[61]
5.3.2.3 Zertifikatsabruf (SDI_EXC)		
SDI_EXC_01	SDI	Pass
5.3.2.4 Wiederherstellen durch ein Backup (SDI_RFB)		
SDI_RFB_01	SDI_RESTORE	n.a.[62]
SDI_RFB_02	SDI_RESTORE	n.a.[63]
SDI_RFB_03	SDI_RESTORE, STORAGE_REMOTE	n.a.[64]
SDI_RFB_04	SDI_RESTORE	n.a.[65]
SDI_RFB_05	SDI_RESTORE	n.a.[66]
5.3.2.5 Lesen einer Log-Nachricht (SDI_RLM)		
SDI_RLM_01	SDI, SM_NOAGG	Pass
SDI_RLM_02	SDI, SM_AGG	n.a.[67]
SDI_RLM_03	SDI, SM_REMOTE	n.a.[68]
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	Pass
SDI_INI_02	SDI	Pass
SDI_INI_03	SDI	Pass
SDI_INI_04	SDI	Pass
SDI_INI_05	SDI	Pass
5.3.2.8 Außerbetriebnahme des Sicherheitsmoduls (SDI_DSE)		
SDI_DSE_01	SDI	Pass
SDI_DSE_02	SDI	Pass
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)		

61 Siehe Kapitel 8.2.1
62 n.a. wegen Profil SDI_RESTORE
63 n.a. wegen Profil SDI_RESTORE
64 n.a. wegen Profil STORAGE_REMOTE
65 n.a. wegen Profil SDI_RESTORE
66 n.a. wegen Profil SDI_RESTORE
67 n.a. wegen Profil SM_AGG
68 n.a. wegen Profil SM_REMOTE

Testcase ID	Profile	Verdict
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, SM_MULTI	Pass
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.[69]
SDI_DSD_04	SDI	Pass
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
SDI_AUT_04	SDI	Pass
SDI_AUT_05	SDI	Pass
SDI_AUT_06	SDI, SM_REMOTE	n.a.[70]
SDI_AUT_07	SDI, STORAGE_REMOTE	n.a.[71]
5.3.2.16 Abmeldung von Benutzern der TSE (SDI_LGO)		
SDI_LGO_01	SDI	Pass
SDI_LGO_02	SDI	Pass
SDI_LGO_03	SDI	Pass
SDI_LGO_04	SDI	Pass
SDI_LGO_05	SDI, SM_REMOTE	n.a.[72]
SDI_LGO_06	SDI, STORAGE_REMOTE	n.a.[73]
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, SM_REMOTE	n.a.[74]
SDI_UBU_06	SDI, STORAGE_REMOTE	n.a.[75]
5.3.3 Prüfungen für herstellerspezifische Einbindungsschnittstellen (CI)		
5.3.3.1 Aktualisierung der Zeit innerhalb des Sicherheitsmoduls (CI_UDT)		

69 n.a. wegen Profil STORAGE_REMOTE
70 n.a. wegen Profil SM_REMOTE
71 n.a. wegen Profil STORAGE_REMOTE
72 n.a. wegen Profil SM_REMOTE
73 n.a. wegen Profil STORAGE_REMOTE
74 n.a. wegen Profil SM_REMOTE
75 n.a. wegen Profil STORAGE_REMOTE

Testcase ID	Profile	Verdict
CI_UDT_01	CUSTOM_INTEGRATION_INTERFACE, SM_BASIC	n.a.[76]
CI_UDT_02	CUSTOM_INTEGRATION_INTERFACE, SM_REMOTE	n.a.[77]
CI_UDT_03	CUSTOM_INTEGRATION_INTERFACE, STORAGE_REMOTE	n.a.[78]
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.[79]
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.[80]
EXP_LOG_10	SM_AGG	n.a.[81]
EXP_LOG_11	SM_NOAGG	Pass
EXP_LOG_12	SM_AGG	n.a.[82]
EXP_LOG_13	SM_BASIC	n.a.[83]
EXP_LOG_14	SM_BASIC	Pass
EXP_LOG_15	SM_BASIC	Pass
EXP_LOG_16	SM_BASIC	Pass
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	-	Pass
SM_ARCH_02	-	Pass

76 n.a. wegen Profil CUSTOM_INTEGRATION_INTERFACE
77 n.a. wegen Profil SM_REMOTE
78 n.a. wegen Profil STORAGE_REMOTE
79 Siehe Kapitel 8.2.2
80 n.a. wegen Profil SM_AGG
81 n.a. wegen Profil SM_AGG
82 n.a. wegen Profil SM_AGG
83 Siehe Kapitel 8.2.2

Testcase ID	Profile	Verdict
SM_ARCH_03	-	Pass
SM_ARCH_04	-	Pass
SM_ARCH_05	-	Pass
SM_ARCH_06	-	n.a.[84]
SM_ARCH_07	-	n.a.[85]
SM_ARCH_08	-	n.a.[86]
SM_ARCH_09	-	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
EXP_LOG_20_M	-	Pass
EXP_LOG_20_N	-	Pass
EXP_LOG_20_O	-	Pass
EXP_LOG_20_P	-	Pass
EXP_LOG_20_Q	-	Pass
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	-	Pass

84 n.a. wegen Einzellösung (TSE enthält nur genau ein SMAERS und genau ein CSP)
85 n.a. wegen Einzellösung (TSE enthält nur genau ein SMAERS und genau ein CSP)
86 n.a. wegen Einzellösung (TSE enthält nur genau ein SMAERS und genau ein CSP)

Testcase ID	Profile	Verdict
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	-	Pass
EXP_LOG_21_Q	-	Pass
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	-	Pass
EXP_LOG_22_I	-	Pass
EXP_LOG_22_J	-	Pass
EXP_LOG_22_K	-	Pass
EXP_LOG_22_L	-	Pass
EXP_LOG_22_M	-	Pass
EXP_LOG_22_N	-	Pass
EXP_LOG_22_O	-	Pass
EXP_LOG_22_P	-	Pass
EXP_LOG_22_Q	-	Pass
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	-	n.a.[87]
EXP_LOG_24	-	n.a.[88]
EXP_LOG_25	-	n.a.[89]
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		

87 n.a. wegen Profil SM_REMOTE
88 n.a. wegen Profil SM_REMOTE
89 n.a. wegen Profil SM_REMOTE

Testcase ID	Profile	Verdict
SM_TME_12	-	n.a.[90]
SM_TME_13	-	n.a.[91]
2.2.6 Ergänzung zur Außerbetriebnahme des Sicherheitsmoduls der Technischen Sicherheitseinrichtung		
II_DSE_08	-	Pass
II_DSE_09	-	Pass
2.2.7 Ergänzung zu Prüfungen der Herstellerdokumentation		
DOC_PAR_01	-	Pass
DOC_DLY_01	-	Pass

8.2 Festgestellte Abweichungen

Im Rahmen der Konformitätsprüfung wurden für den Prüfgegenstand keine Abweichungen von den Prüfgrundlagen festgestellt.

8.2.1 Referenz

Einige Testfälle der Prüfgrundlage zielen auf speziellen Variablen, in Form einer Referenz auf einen Speicherbereich, hin (Pointer). Wird diese Referenz der Funktion nicht korrekt übergeben, so können fehlerhafte Parameter übergeben oder fehlerhafte Werte zurückgesendet werden. Verwendet die Implementierung der Schnittstelle jedoch andere Variablentypen, so erfolgt keine Fehlermeldung.

Der Prüfgegenstand verwendet jedoch keine Referenzen (Pointer), sondern eine „Struktur“ (struct). Hierbei treten keine Fehler durch fehlerhafte oder fehlende Referenzen auf.

Einige Testfälle sind daher nicht anwendbar. Es liegt keine Abweichung seitens des Prüfgegenstands vor.

8.2.2 Beschreibung gesetzt

Einige Testfälle der Prüfgrundlage verlangen als Eingabeparameter beim Initialisieren der TSE eine Beschreibung (Description). Der Prüfgegenstand verwendet jedoch spezifikationsgerecht eigene, unveränderbare Beschreibungen, so dass diese Testfälle fehlschlagen.

Die Testfälle sind daher nicht anwendbar. Es liegt keine Abweichung seitens des Prüfgegenstands vor.

90 n.a. da keine Stellen der Zeitführung im CSP
91 n.a. wegen Profil NO_TIME_SYNC

9 Ergebnis der Konformitätsprüfung

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

TÜV Informationstechnik GmbH
Prüfbericht BSI TR-03153
BSI-K-TR-0482
cryptovision TSE v2
Prüfbericht Version 5
Erstellungsdatum: 20. April 2023

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;
- alle relevanten Testfälle gemäß [BSI TR-03153-TS-KuA] 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-0482-2023 vom 15. Mai 2023 bestätigt.

Das Zertifikat nach Technischen Richtlinien ist gültig bis zum 14. Mai 2031.

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) vom 10. September 2021, Bundesgesetzblatt I, S. 1359

VB-Produkte.PD Verfahrensbeschreibung zur Zertifizierung von Produkten, Prozessen und Dienstleistungen, Version 3.2 vom 28. Oktober 2022

TR-Produkte.PD Zertifizierung von Produkten, Prozessen und Dienstleistungen: Programm Technische Richtlinien, Version 2.2 vom 31. Januar 2023

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 vom 23. Februar 2021

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