Bundesamt
für Sicherheit in der
Informationstechnik

Zertifikat

nach Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik

BSI-K-TR-0524-2024

D-TRUST Web-Dienst für TSE
Version 3.1

der	D-Trust GmbH
Konformität zu:	**BSI TR-03153** – Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme
gültig bis:	25. Februar 2032

Die Konformität des Prüfgegenstands D-TRUST Web-Dienst für TSE, Version 3.1 zur Technischen Richtlinie BSI TR-03153 wurde von einem gemäß DIN ISO/IEC 17025 anerkannten Prüflaboratorium 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-0524-2024. 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 26. Februar 2024
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag

Sandro Amendola
Direktor

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87, 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-0524-2024

D-TRUST Web-Dienst für TSE

Version 3.1

der

D-Trust GmbH

Kommandantenstraße 15, 10969 Berlin

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87, 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 einem vom BSI anerkannten Prüflaboratorium 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 BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) vom 2. September 2019, Bundesgesetzblatt Teil I, S. 1365, [BMIBGebV]
- Verfahrensbeschreibung zur Zertifizierung von Produkten und Dienstleistungen, Version 3.2 vom 28.10.2022, [VB-Produkte.PD]
- Zertifizierung von Produkte, Prozessen und Dinestleistungen: Programm Technische Richtlinien (TR), Version 2.2 vom 31.01.2023, [TR-Produkte.PD]

3 Hinweise für den Antragsteller

1. Das vom BSI erteilte Zertifikat nach Technischen Richtlinien BSI-K-TR-0524-2024 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 Fehler: Verweis nicht gefunden 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 des Prüflaboratoriums, 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

D-Trust GmbH
Kommandantenstraße 15
10969 Berlin

Deutschland

Ansprechpartner:

Toni Habich (t.habich@d-trust.net)
Joris Minolla (j.minolla@d-trust.net)

mit Antragsdatum 24. Februar 2022 (Eingangsdatum BSI: 16. März 2022) beim BSI eine Re-Zertifizierung nach Technischen Richtlinien beantragt.

Vorherige Zertifizierungen erfolgten unter folgenden Zertifizierungs-IDs:

BSI-K-TR-0474-2021

BSI-K-TR-0442-2021

BSI-K-TR-0369-2020

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]
>
> **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 Prüflaboratorium

Mit der Durchführung der Konformitätsprüfung wurde folgendes, vom BSI gemäß DIN ISO/IEC 17025 anerkanntes Prüflaboratorium 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:

D-TRUST Web-Dienst für TSE, Version 3.1

Bei dem Prüfgegenstand handelt es sich um eine softwarebasierte Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme gemäß Kassensicherungsverordnung [KassenSichV]. Sie besteht aus einer lokalen Client Komponente, die die SMAERS Anwendung [PP_SMAERS] einschließlich des Package Trusted Channel implementiert und einer Server Komponente, die remote im Rechenzentrum der D-Trust GmbH die CSP Dienste gemäß [PP-CSPL] bereitstellt.

Wesentliche Bestandteile des Prüfgegenstands sind der TSS Client Desktop sowie der Remote CSP Service.

Beim TSS Client Desktop handelt es sich um Softwarebibliotheken, die in der operativen Umgebung des Steuerpflichtigen betrieben wird.

Der Remote CSP Service wird von der D-Trust (dem Trust Center der Bundesdruckerei) betrieben. Er wird von den TSS Clients aufgerufen, um u.a. Signaturen über die zu signierenden Daten zu erzeugen.

Die Verbindung zwischen TSS Client und Remote CSP Service erfolgt durch einen Trusted Channel über das Internet.

7.2 Komponenten des Prüfgegenstands

Die einzelnen Komponenten des Prüfgegenstands sowie deren zertifizierte Versionsstände sind in den Tabelle Fehler: Verweis nicht gefunden-6 festgeschrieben.

7.2.1 TSS Client Version 1.4.3

Die Komponenten des TSS Client Desktops sind in Tabelle 1 identifiziert.

Tabelle 1: Komponenten des TSS Client Desktop Version 1.4.3

Nr	JAR File	SHA-256 Hash
1	smaers-1.4.3-1856182.jar	1039 29c4 6244 8272 2daf bf81 274e ec65 68e9 d2fb 68ea b61f 3832 9da7 db0c 9f88
2	tss-client-1.4.3-1856182.jar	eae2 e74c 916e 9e4e dd11 c576 c989 06b7 12ef 20ca aaf4 bab1 1b71 d47f cd0b 2cf7

Tabelle 2: Unterstützende Komponenten von TSS Client und SMAERS Version 1.4.3

Nr	JAR File	SHA-256 Hash	SMAERS	TSS Client
1	annotations-13.0.jar	ace2 a10d c8e2 d5fd 3492 5eca c03e 4988 b2c0 f851 650c 94b8 cef4 9ba1 bd11 1478	x	
2	bcpkix-jdk15on-1.70.jar	e5b9 cb82 1df5 7f70 b059 3358 e89c 0e8d 7266 515d a9d0 88af 6c64 6f63 d433 c07c	x	
3	bcprov-jdk15on-1.70.jar	8f3c 20e3 e2d5 65d2 6f33 e8d4 857a 37d0 d7f8 ac39 b62a 7026 496f cab1 bdac 30d4	x	
4	commons-compress-1.22.jar	53d0 4a0e fc72 23ba ecaa 303b d5d2 98eb 0600 e6b8 2b40 76f9 cecd 558b 97ba 760b		x
5	HikariCP-3.4.5.jar	8b73 2f94 7057 0d4a 841d c1ef 6c82 6b58 6978 b25b a830 712f f1fa 59de 275d fa61		x
6	jackson-annotations-2.14.1.jar	d255 b4b8 63ff 8ec7 14a8 f96f a55c 3462 1d43 dbb8 2b82 d3f5 7476 496a 4c09 e1e7	x	
7	jackson-core-2.14.1.jar	0114 187e 296b 34c9 31c1 bf9e 5a84 152b 62bf ab7d 182f 5623 f398 2dc2 da35 e526	x	
8	jackson-databind-2.14.1.jar	423a 0c80 6de4 b3fa 5eb4 a286 9830 5e3a 3777 c731 e1bc fa1b 2f3a 3760 c7b6 e773	x	
9	kotlin-stdlib-1.8.0.jar	c77b ef87 7464 0b9f b9d6 e217 459f f220 dae5 9878 beb7 d2e4 b430 506f effc 654e	x	x
10	kotlin-stdlib-common-1.8.0.jar	78ef 93b5 9e60 3cc0 fe51 def9 bd4c 037b 07cb ace3 b3b7 806d 1a49 0a42 bc1f 4cb2	x	x
11	kotlin-stdlib-jdk7-1.8.0.jar	4c88 9d1d 9803 f5f2 eb6c 1592 a6b7 e623 69ac 7660 c9ee e15a ba16 fec0 5916 3666	x	x
12	kotlin-stdlib-jdk8-1.8.0.jar	05b6 2804 441b 0c9a 1920 b6b7 d5cf 7329 a4e2 4b62 5847 8e32 b1f0 46ca 0190 0946	x	x
13	logging-interceptor-4.10.0.jar	273b a218 636c 34f7 a091 c059 d159 6005 43e0 3ea8 beef 2c5f c565 25b4 7396 160e	x	x
14	okhttp-4.10.0.jar	7580 f14f a169 1206 e370 81ad 3f92 063b 1603 b328 da0b b316 f2fe f02e 0562 e7ec		x
15	okio-jvm-3.0.0.jar	7580 f14f a169 1206 e370 81ad 3f92 063b 1603 b328 da0b b316 f2fe f02e 0562 e7ec		x
16	shared.jvmJar-jvm-1.4.3-1856182.jar	0da0 b26a 3c4d 7f39 bd8e e17f 2ada 6ae3 5ae6 02a8 0740 e771 39e7 5790 9d40 ed4	x	x
17	slf4j-api-1.7.31.jar	cda8 62aa 6968 3ac0 72ee 2afd 0b93 d070 ceab 291e f5b8 57d3 18b2 4c15 95b3 6b8a	x	x
18	sqlite-jdbc-3.41.2.2.jar	0cda b410 947e 04b6 743d f99c f154 3267 ddd1 0735 7d6f 7694 8d14 5be5 90fd 497d		x

7.2.2 TSS Client Version 1.3.4

Anstelle des TSS Client Version 1.4.3 kann der Prüfgegenstand auch in Verbindung mit dem TSS Client Desktop Version 1.3.4 betrieben werden.

Die zugehörigen Komponenten sind in den Tabellen 3 und 4 identifiziert.

Tabelle 3: Komponenten des TSS Client Desktop Version 1.3.4

Nr	JAR File	SHA-256 Hash
1	smaers-1.3.3-400793-hotfix_3.0.0.jar	cb22 3be3 a1d9 cf79 2617 9242 0604 4886 701d 3f0d 439a 0b01 bcbb 4814 d5ca e707
2	tss-client-1.3.4-400793-hotfix_3.0.0.jar	c470 cd2f ace1 297b 777f 5a22 be8a c430 d0b9 69dd b29c 84b8 82b1 338d d78f 69ac

Tabelle 4: Unterstützende Komponenten von TSS Client und SMAERS Version 1.3.4

Nr	JAR File	SHA-256 Hash	SMAERS	TSS Client
1	annotations-13.0.jar	ace2 a10d c8e2 d5fd 3492 5eca c03e 4988 b2c0 f851 650c 94b8 cef4 9ba1 bd11 1478	x	
2	bcpkix-jdk15to18-1.68.jar	5f8f 2f8f b99f 8aa8 98ae 442b 694e 6ebf c70e a66b 91ac 97da 0381 1a4f acd7 c060	x	
3	bcprov-jdk15to18-1.68.jar	f147 f23d 7ea0 f364 8e44 0952 11c4 e63c e8c0 719f 2a68 f681 5705 75fc a45b 539c	x	
4	commons-compress-1.20.jar	0aeb 625c 948c 697e a7b2 0515 6e11 2363 b59e d5e2 5512 12cd 4e46 0bdb 72c7 c06e		x
5	HikariCP-3.4.5.jar	8b73 2f94 7057 0d4a 841d c1ef 6c82 6b58 6978 b25b a830 712f f1fa 59de 275d fa61		x
6	jackson-annotations-2.12.3.jar	05da 0a25 bb44 a217 880a 299a 1a1e 0a30 1d19 4b56 56a9 a077 76b7 7a88 f326 e7e9	x	
7	jackson-core-2.12.3.jar	baef 34fb ce04 1d54 f3af 3ff4 fc91 7ed8 b43e d2a6 fa30 e0a6 abfd 9a2b 2c3f 71e0	x	
8	jackson-databind-2.12.3.jar	94d9 7306 2c2f da3d ff2c 9a85 eafc e572 0482 1cce 9085 a993 7769 3dbc 9fb8 da23	x	
9	kotlin-stdlib-1.5.20.jar	80cd 79c2 6aac 46d7 2d78 2de1 ecb3 2606 1e93 c6e6 88d9 94b4 8627 ffd6 68ba 63a8	x	x
10	kotlin-stdlib-common-1.5.20.jar	9819 5298 04bf 9296 e385 3acd 5ae8 24df 95d8 f8c6 1309 e776 8b7c ae5c a136 1d36	x	x
11	kotlin-stdlib-jdk7-1.5.20.jar	b110 f6d2 0204 3030 99af 0d5f 2c84 6ac6 0bc6 ae56 63ef 5f22 e726 ca46 2735 9d06	x	x
12	kotlin-stdlib-jdk8-1.5.20.jar	a7e9 cffe 569c 43eb 8f0f e313 9978 b094 3fe9 2abc c513 f7cf 0454 4f27 97f8 d38a	x	x
13	logging-interceptor-4.9.1.jar	08ae 52d4 e7ab 4dde 8f94 970b beb1 545b 5193 4d4b 3f08 02f6 e816 b052 2902 fa9d	x	x
14	okhttp-4.9.1.jar	6afd d8f3 5f4e b60d f965 c290 fa3a cf29 443f a986 5451 13d0 729b 8461 f657 1f8f		x
15	okio-jvm-2.8.0.jar	4496 b06e 7398 2fcd d8a5 393f 46e5 df2c e2fa 4465 df58 9545 4cac 68a3 2f09 bbc8		x
16	shared.jar	6d2d 19f9 b91b 793f 5940 3078 f1e9 4dbf baee b43d a5d1 9d4f 9169 c194 bc68 8dde	x	x

Nr	JAR File	SHA-256 Hash	SMAERS	TSS Client
17	slf4j-api-1.7.31.jar	cda8 62aa 6968 3ac0 72ee 2afd 0b93 d070 ceab 291e f5b8 57d3 18b2 4c15 95b3 6b8a	x	x
18	sqlite-jdbc-3.34.0.jar	6059 79c9 4e7f e004 37f1 e10d cfa6 57a2 3f12 5c8e b4d2 f0ec 17e3 f846 1389 4cc3		x

7.2.3 CSP-L Version 1.4.1

Auf Serverseite implementieren die in Tabelle 5 und 6 identifizierten Komponenten den CSP Service des Prüfgegenstands.

Tabelle 5: Komponenten des CSP-L Version 1.4.1

Nr	JAR File	SHA-256 Hash
1	server.csp.csplight.application-1.4.1-1856182-jar-with-dependencies.jar	f1f2 7366 c592 f427 9073 d5e2 6135 3797 0932 3668 bf61 1ef9 0fd8 0d41 d2f2 8645

Tabelle 6: Unterstützende Komponenten des CSP-L Version 1.4.1

Nr	Softwarekomponente	Liefergegenstand / Bezeichnung	SHA-256 Hash
1	AccessController	accesscontrol-1.4.0-1856182.zip	85e8 5ddf 476c 7a68 3da0 d9a8 4c28 7db2 c8eb b4c7 a487 6ff8 f969 f7ba 5514 342f
2	Control-Application	controlapp-1.4.0-1856182.zip	5c77 8b88 274f 6bdc 48cb d484 6d70 2838 cc34 6af6 c220 7e50 3582 02aa 165a 3684
3	Cloudmanagement und TSE Management	cloudmanagement-cmi-1.4.1-1856182.zip	1545 6fc1 7601 0453 d358 1845 978e fe28 1ea6 ed49 6497 cfd1 c716 2082 0c51 39ba
		cloudmanagement-tmi-1.4.0-1856182.zip	ff1d 83f1 53ce 072a 9d8a 1876 9798 4f2e 6ece d2bb 0462 5978 7639 da5c 9f28 2a08
4	DB	MySQL Datenbank Version 8.1.0	n.a.

7.3 Ablaufumgebungen des Prüfgegenstands

Die Ablaufumgebung des Prüfgegenstands besteht also sowohl auf Client- als auch auf Server-Seite aus einer Java Virtual Machine (JVM).

Als Java Runtime Environment sind folgende Versionen zulässig:

- Azul Zulu Community Java 17 für TSS Client Version 1.4.3
- Azul Zulu Community Java 8 für TSS Client Version 1.3.4

Auf Server-Seite kommt ausschließlich das Betriebssystem Red Hat Enterprise Linux 8 (RHEL 8) zum Einsatz.

Auf Client-Seite kann die JVM auf unterschiedlichen Betriebssystemen (z.B. Windows, Linux, macOS) ausgeführt werden.

Ein TR-konformer Betrieb der TSS Client Desktop Komponente ist ausschließlich für die nachfolgend genannten Betriebssysteme auf einer Hardware, welche die Mindestanforderungen gemäß Tabelle 7 erfüllt, zulässig.

Darüber hinaus sind die Vorgaben der Herstellerdokumente [INT_ANF] und [NUTZ_BED] zu berücksichtigen.

Tabelle 7: Ablaufumgebungen TSS Client Desktop

Nr	Umgebung von TSS Client & SMAERS	TSS Client v1.4.3	TSS Client v1.3.4
1	**Red Hat Enterprise Linux 7 x64** 2 x Intel® Xeon® @2.10 GHz, 2 GB RAM	x	x
2	**Red Hat Enterprise Linux 8 x64** 2 x Intel® Xeon® @2.10 GHz, 2 GB RAM	x	x
3	**CentOS Linux 7 x64** 2 x Intel® Xeon® @2.10 GHz, 2 GB RAM		x
4	**CentOS Linux 8 x64** 1 x Intel® Xeon® @2.10 GHz, 2 GB RAM	x	
5	**CentOS Linux 9 x64** 2 x Intel® Xeon® @2.10 GHz, 2 GB RAM	x	
6	**Rocky Linux 9.1 LTS x64** 1 x Intel® Xeon® @2.10 GHz, 2 GB RAM	x	x
7	**Suse Linux Enterprise Server 12 x64** 2 x Intel® Xeon® @2.10 GHz, 2 GB RAM	x	x
8	**Suse Linux Enterprise Server 15 x64** 1 x Intel® Xeon® @2.10 GHz, 1 GB RAM	x	x
9	**Ubuntu 18.04 LTS x64** 2 x Intel® Xeon® @2.10 GHz, 1 GB RAM	x	x
10	**Ubuntu 20.04 ARM x64** 4 x ARM Cortex-A72 @1,5 GHz, 4 GB RAM	x	
11	**Ubuntu 22.04.2 LTS x64** 1 x Intel® Xeon® @2.10 GHz, 1 GB RAM	x	x
12	**Debian Linux 11 x64** 2 x Intel® Xeon® @2.10 GHz, 1 GB RAM	x	
13	**Flatcar OS (3033.3.10) x64** 2 x Intel® Xeon® @2.10 GHz, 4 GB RAM	x	
14	**Windows POSReady 7 x64** 3 x Intel® Xeon® @2.10 GHz, 8 GB RAM	x	x
15	**Windows 10 x64 Pro** 1 x Intel® Xeon® @2.10 GHz, 8 GB RAM	x	x
16	**Windows 10 IoT Enterprise x64** 1 x Intel® Xeon® @2.10 GHz, 1 GB RAM	x	
17	**Windows 11 x64 Pro** 2 x Intel® Xeon® @2.10 GHz, 4 GB RAM	x	
18	**Windows Server 2012 R2 x64**	x	x

Nr	Umgebung von TSS Client & SMAERS	TSS Client v1.4.3	TSS Client v1.3.4
	2 x Intel® Xeon® @2.10 GHz, 4 GB RAM		
19	**Windows Server 2016 x64** 1 x Intel® Xeon® @2.10 GHz, 2 GB RAM	x	x
20	**Windows Server 2019x64** 1 x Intel® Xeon® @2.10 GHz, 2 GB RAM	x	x
21	**macOS 13 (Ventura) für Intel x64** 1 x Intel® Xeon® @3.20 GHz, 4 GB RAM	x	x
22	**Rocky Linux 9.2 LTS x64** 1 x Intel® Xeon® @2.10 GHz, 2 GB RAM	x	x

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 8: 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	No
aggregiert Aktualisierungen (Updates) und sichert diese zusammengefasst ab (signiert)	SM_AGG	Yes
kann mehrere Transaktionen parallel verwalten	SM_MULTI	Yes (500)
besitzt eine herstellerspezifische Einbindungsschnittstelle und setzt den Export-Teil der Einheitlichen Digitalen Schnittstelle um	CUSTOM_INTEGRATION_INTERFACE	Yes
implementiert alle Funktionen der Einheitlichen Digitalen Schnittstelle gemäß BSI TR-03153	SDI	No
implementiert die optionale Funktion restoreFromBackup der Einheitlichen Digitalen Schnittstelle gemäß	SDI_RESTORE	No

BSI TR-03153		
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
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 9: Verwendeter Signaturalgorithmus

Verwendete Kryptofunktionen	Angaben des Antragstellers
Signaturalgorithmus	ECDSA
Parameter zum Signaturalgorithmus (inkl. Hashfunktion und Schlüssellängen	SHA384withPLAIN-ECDSA, 384 Bit, secp384r1

Tabelle 10: Zusätzliche Angaben

Gegenstand	Angaben des Antragstellers
Größe des internen Speichers des Sicherheitsmoduls	4GB Entsprechend den Systemmindestanforderungen wird diese Größe vom System des Steuerpflichtigen, auf dem das SMAERS-Modul installiert ist, erwartet.
Zeitlicher Abstand in dem das Sicherheitsmodul die intern verwaltete Zeit in seinem nichtflüchtigen Speicher speichert	Im Remote CSP wird die verwaltete Systemzeit batteriegepuffert geführt.
Welche Zeitformate werden von der TSE unterstützt ?	UNIX Time
Maximale Anzahl von Clients, die die TSE gleichzeitig zur Absicherung von Transaktionen nutzen können	500
Maximale Anzahl der parallel geöffneten Transaktionen, die das Sicherheitsmodul verwalten kann	500

7.5 Mitgeltende Zertifizierungen

Die vom Sicherheitsmodul des Prüfgegenstands genutzte Public-Key-Infrastruktur (PKI) verfügt über folgende mitgeltende Zertifizierung[1]:

Zertifikat nach Technischen Richtlinien
BSI-K-TR-0545-2023 des BSI
vom 03. April 2023
gültig bis 02. April 2026
D-Trust GmbH
Scope: D-Trust Device PKI

Hinweis: Die Gültigkeit der Zertifizierung des Prüfgegenstands ist abhängig von der Gültigkeit der mitgeltenden Zertifizierungen. Verlieren diese ihre Gültigkeit, wird damit auch das Zertifikat des Prüfgegenstands (BSI-K-TR-0524-2024) ungültig.

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

1 Siehe hierzu auch Pfüffall SM_PKI_01

8 Konformitätsprüfung

Die Konformitätsprüfung wurde im Zeitraum April 2023 bis Februar 2024 vom beauftragten Prüflaboratorium durchgeführt.

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

8.1 Ergebnisse der Konformitätsprüfung

Tabelle 11 enthält die Zusammenfassung der durchgeführten Prüffälle.

Tabelle 11: 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	Pass
STO_FUN_02	SM_NOAGG	n.a.[2]
STO_FUN_03	SM_AGG	Pass
STO_FUN_04	SM_NOAGG	n.a.[3]
STO_FUN_05	SM_AGG	Pass
STO_FUN_06	SM_NOAGG, SM_MULTI	n.a.[4]
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)		

2 n.a. wegen Profil SM_NOAGG
3 n.a. wegen Profil SM_NOAGG
4 n.a. wegen Profil SM_NOAGG

Testcase ID	Profile	Verdict
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	n.a.[6]
SM_CON_02	SM_AGG	Pass
SM_CON_03	SM_NOAGG	n.a.[7]
SM_CON_04	SM_AGG	Pass
SM_CON_05	SM_AGG	Pass
SM_CON_06	SM_NOAGG, SM_MULTI	n.a.[8]
SM_CON_07	SM_AGG, SM_MULTI	Pass
SM_CON_08	SM_NOAGG, SM_MULTI	n.a.[9]
SM_CON_09	SM_AGG, SM_MULTI	Pass
SM_CON_10	SM_AGG, SM_MULTI	Pass
SM_CON_11	SM_AGG, SM_MULTI	Pass
SM_CON_12	SM_NOAGG, SM_MULTI	n.a.[10]
SM_CON_13	SM_BASIC	Pass
SM_CON_14	SM_BASIC	Pass
SM_CON_15	SM_BASIC, SDI	n.a.[11]
SM_CON_16	SM_BASIC, SDI	n.a.[12]
SM_CON_17	SM_BASIC, SDI	n.a.[13]
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

5 n.a. wegen Profil STORAGE_REMOTE
13 n.a. wegen Profil SDI
12 n.a. wegen Profil SDI
11 n.a. wegen Profil SDI
10 n.a. wegen Profil SM_NOAGG
9 n.a. wegen Profil SM_NOAGG
8 n.a. wegen Profil SM_NOAGG
7 n.a. wegen Profil SM_NOAGG
6 n.a. wegen Profil SM_NOAGG

Testcase ID	Profile	Verdict
SM_TME_04	SM_BASIC, NO_TIME_SYNC	n.a.[14]
SM_TME_05	SM_AGG, SM_MULTI	Pass
SM_TME_06	SM_NOAGG, SM_MULTI	n.a.[15]
SM_TME_07	SM_NOAGG	n.a.[16]
SM_TME_08	SM_AGG	Pass
SM_TME_09	SM_BASIC, SDI	n.a.[17]
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	n.a.[20]
SM_SIG_02	SM_AGG	Pass
SM_SIG_03	SM_NOAGG, SM_MULTI	n.a.[21]
SM_SIG_04	SM_AGG	Pass
SM_SIG_05	SM_BASIC	Pass
SM_SIG_06	SM_NOAGG	n.a.[22]
SM_SIG_07	SM_AGG	Pass
SM_SIG_08	SM_BASIC, SDI	n.a.[23]
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

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

Testcase ID	Profile	Verdict
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.[24]
SM_KRY_04	SM_BASIC	Pass
5.2.6 Prüfungen der PKI von Sicherheitsmodulen (SM_PKI)		
SM_PKI_01	SM_BASIC	Pass[25]
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.[26]
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.[27]

24 Testcase nicht verpflichtend gemäß [BSI TR-03153-TS-ERG]
27 n.a. wegen Profil STORAGE_REMOTE
26 n.a. wegen Profil SM_REMOTE
25 Die verwendete PKI vefügt über eine Zertifizierung nach BSI TR-03145-1 (siehe Kapitel

Testcase ID	Profile	Verdict
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	n.a.[28]
II_INI_04	SM_BASIC	n.a.[29]
II_INI_05	SM_BASIC	n.a.[30]
II_INI_06	SM_BASIC	Pass
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.[31]
II_INI_14	SM_BASIC, STORAGE_REMOTE	n.a.[32]
5.3.1.3 Außerbetriebnahme des Sicherheitsmoduls (II_DSE)		
II_DSE_01	SM_BASIC	Fail[33]
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.[34]

28 Das Feld "description" ist nicht vom Hersteller vorbesetzt.
34 n.a. wegen Profil SM_REMOTE
33 Siehe Kapitel 8.2.2
32 n.a. wegen Profil STORAGE_REMOTE
31 n.a. wegen Profil SM_REMOTE
30 Das Feld "description" ist nicht vom Hersteller vorbesetzt.
29 Das Feld "description" ist nicht vom Hersteller vorbesetzt.

Testcase ID	Profile	Verdict
II_DSE_07	SM_BASIC, STORAGE_REMOTE	n.a.[35]
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.[36]
II_STA_04	SM_BASIC	n.a.[37]
II_STA_05	SM_BASIC	n.a.[38]
II_STA_06	SM_BASIC, SM_REMOTE	n.a.[39]
II_STA_07	SM_BASIC, STORAGE_REMOTE	n.a.[40]
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.[41]
II_UPD_02	SM_NOAGG	n.a.[42]
II_UPD_03	SM_AGG	Pass
II_UPD_04	SM_NOAGG	n.a.[43]
II_UPD_05	SM_BASIC, SM_REMOTE	n.a.[44]
II_UPD_06	SM_BASIC, STORAGE_REMOTE	n.a.[45]
II_UPD_07	SM_AGG, STORAGE_REMOTE	n.a.[46]
II_UPD_08	SM_BASIC, SM_NOAGG	n.a.[47]
II_UPD_09	SM_BASIC, SM_AGG	Pass
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

35 n.a. wegen Profil STORAGE_REMOTE
36 Dieser Test ist mit der D-TRUST TSS-Client Lib (Java API) nicht durchführbar, da der Zeitpunkt des Vorgangbeginns nicht über einen "output" Parameter zurückgegeben wird, sondern als "member" der Resultklasse "StartTransactionResult“.
37 Dieser Test ist mit der D-TRUST TSS-Client Lib (Java API) nicht durchführbar, da der Signaturzähler nicht über einen "output" Parameter zurückgegeben wird, sondern als "member" der Resultklasse "StartTransactionResult".
38 Dieser Test ist mit der D-TRUST TSS-Client Lib (Java API) nicht durchführbar, da die Serialnumber nicht über einen "output" Parameter zurückgegeben wird, sondern als "member" der Resultklasse "StartTransactionResult".
39 n.a. wegen Profil SM_REMOTE
40 n.a. wegen Profil STORAGE_REMOTE
41 n.a. wegen Profil SM_NOAGG
42 n.a. wegen Profil SM_NOAGG
43 n.a. wegen Profil SM_NOAGG
44 n.a. wegen Profil SM_REMOTE
45 n.a. wegen Profil STORAGE_REMOTE
46 n.a. wegen Profil STORAGE_REMOTE
47 n.a. wegen Profil SM_NOAGG

Testcase ID	Profile	Verdict
II_FIN_02	SM_BASIC	Pass
II_FIN_03	SM_BASIC	n.a.[48]
II_FIN_04	SM_BASIC	n.a.[49]
II_FIN_05	SM_BASIC, SM_REMOTE	n.a.[50]
II_FIN_06	SM_BASIC, STORAGE_REMOTE	n.a.[51]
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	n.a.[52]
II_MCU_02	MULTI_CLIENT, SM_AGG	Pass
II_MCU_03	MULTI_CLIENT, SM_NOAGG	n.a.[53]
II_MCU_04	MULTI_CLIENT, SM_AGG	Pass
II_MCU_05	MULTI_CLIENT, SM_BASIC	Pass
II_MCU_06	NO_MULTI_CLIENT, SM_BASIC	n.a.[54]
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.[55]
SDI_UDT_02	SDI, TIME_SYNC	n.a.[55]
SDI_UDT_03	SDI, NO_TIME_SYNC	n.a.[55]
SDI_UDT_04	SDI, SM_REMOTE	n.a.[55]
SDI_UDT_05	SDI, STORAGE_REMOTE	n.a.[55]
SDI_UDT_06	SDI	n.a.[55]
SDI_UDT_07	SDI	n.a.[55]
5.3.2.2 Export des Archivs (SDI_EXP)		
SDI_EXP_01	SDI	n.a.[55]
SDI_EXP_02	SDI	n.a.[55]
SDI_EXP_03	SDI	n.a.[55]
SDI_EXP_04	SDI	n.a.[55]
SDI_EXP_05	SDI	n.a.[55]
SDI_EXP_06	SDI	n.a.[55]
SDI_EXP_07	SDI	n.a.[55]
SDI_EXP_08	SDI	n.a.[55]

48 Dieser Test ist mit der D-TRUST TSS-Client Lib (Java API) nicht durchführbar, da der Zeitpunkt des Vorgangbeginns nicht über einen "output" Parameter zurückgegeben wird, sondern als "member" der Resultklasse "FinishTransactionResult".
49 Dieser Test ist mit der D-TRUST TSS-Client Lib (Java API) nicht durchführbar, da der Signaturzähler nicht über einen "output" Parameter zurückgegeben wird, sondern als "member" der Resultklasse "FinishTransactionResult".
50 n.a. wegen Profil SM_REMOTE
51 n.a. wegen Profil STORAGE_REMOTE
52 n.a. wegen Profil SM_NOAGG
53 n.a. wegen Profil SM_NOAGG
54 n.a. wegen Profil NO_MULTI_CLIENT
55 n.a. wegen Profil SDI

Testcase ID	Profile	Verdict
SDI_EXP_09	SDI	n.a.[55]
SDI_EXP_10	SDI	n.a.[55]
SDI_EXP_11	SDI	n.a.[55]
SDI_EXP_12	SDI	n.a.[55]
SDI_EXP_13	SDI	n.a.[55]
SDI_EXP_14	SDI	n.a.[55]
SDI_EXP_15	SDI	n.a.[55]
SDI_EXP_16	SDI	n.a.[55]
SDI_EXP_17	SDI	n.a.[55]
SDI_EXP_18	SDI	n.a.[55]
SDI_EXP_19	SDI	n.a.[55]
SDI_EXP_20	SDI	n.a.[55]
SDI_EXP_21	SDI	n.a.[55]
SDI_EXP_22	SDI	n.a.[55]
SDI_EXP_23	SDI	n.a.[55]
SDI_EXP_24	SDI	n.a.[55]
SDI_EXP_25	SDI	n.a.[55]
SDI_EXP_26	SDI	n.a.[55]
SDI_EXP_27	SDI	n.a.[55]
SDI_EXP_28	SDI	n.a.[55]
SDI_EXP_29	SDI	n.a.[55]
SDI_EXP_30	SDI	n.a.[55]
SDI_EXP_31	SDI	n.a.[55]
SDI_EXP_32	SDI	n.a.[55]
SDI_EXP_33	SDI	n.a.[55]
SDI_EXP_34	SDI	n.a.[55]
SDI_EXP_35	SDI	n.a.[55]
SDI_EXP_36	SDI	n.a.[55]
SDI_EXP_37	SDI	n.a.[55]
SDI_EXP_38	SDI	n.a.[55]
SDI_EXP_39	SDI	n.a.[55]
SDI_EXP_40	SDI	n.a.[55]
SDI_EXP_41	SDI	n.a.[55]
SDI_EXP_42	SDI	n.a.[55]
5.3.2.3 Zertifikatsabruf (SDI_EXC)		
SDI_EXC_01	SDI	n.a.[55]
5.3.2.4 Wiederherstellen durch ein Backup (SDI_RFB)		
SDI_RFB_01	SDI_RESTORE	n.a.[55]
SDI_RFB_02	SDI_RESTORE	n.a.[55]
SDI_RFB_03	SDI_RESTORE, STORAGE_REMOTE	n.a.[55]
SDI_RFB_04	SDI_RESTORE	n.a.[55]
SDI_RFB_05	SDI_RESTORE	n.a.[55]

Testcase ID	Profile	Verdict
5.3.2.5 Lesen einer Log-Nachricht (SDI_RLM)		
SDI_RLM_01	SDI, SM_NOAGG	n.a.[55]
SDI_RLM_02	SDI, SM_AGG	n.a.[55]
SDI_RLM_03	SDI, SM_REMOTE	n.a.[55]
5.3.2.6 Export von Seriennummern (SDI_ESN)		
SDI_ESN_01	SDI	n.a.[55]
SDI_ESN_02	SDI	n.a.[55]
SDI_ESN_03	SDI	n.a.[55]
5.3.2.7 Initialisierung der Sicherheitseinrichtung (SDI_INI)		
SDI_INI_01	SDI	n.a.[55]
SDI_INI_02	SDI	n.a.[55]
SDI_INI_03	SDI	n.a.[55]
SDI_INI_04	SDI	n.a.[55]
SDI_INI_05	SDI	n.a.[55]
5.3.2.8 Außerbetriebnahme des Sicherheitsmoduls (SDI_DSE)		
SDI_DSE_01	SDI	n.a.[55]
SDI_DSE_02	SDI	n.a.[55]
SDI_DSE_03	SDI	n.a.[55]
5.3.2.9 Abfrage der maximalen Anzahl von simultanen Clients der TSE (SDI_MNC)		
SDI_MNC_01	SDI, MULTI_CLIENT	n.a.[55]
5.3.2.10 Abfrage der aktuellen Anzahl von Clients der TSE (SDI_CNC)		
SDI_CNC_01	SDI, MULTI_CLIENT	n.a.[55]
SDI_CNC_02	SDI, MULTI_CLIENT	n.a.[55]
SDI_CNC_03	SDI, MULTI_CLIENT	n.a.[55]
SDI_CNC_04	SDI, MULTI_CLIENT	n.a.[55]
5.3.2.11 Abfrage der maximalen Anzahl von parallelen Transaktionen (SDI_MNT)		
SDI_MNT_01	SDI, SM_MULTI	n.a.[55]
5.2.3.12 Abfrage aktuelle Anzahl parallel geöffneter Transaktionen (SDI_CNT)		
SDI_CNT_01	SDI, SM_MULTI	n.a.[55]
SDI_CNT_02	SDI, SM_MULTI	n.a.[55]
SDI_CNT_03	SDI, SM_MULTI	n.a.[55]
SDI_CNT_04	SDI, SM_MULTI	n.a.[55]
5.3.2.13 Abfrage unterstützte Varianten der Aktualisierungen von Transaktionen (SDI_UTV)		
SDI_UTV_01	SDI	n.a.[55]
5.3.2.14 Löschen von gespeicherten Daten im Speichermedium (SDI_DSD)		
SDI_DSD_01	SDI_DELETE	Pass
SDI_DSD_02	SDI_DELETE	Fail[56]
SDI_DSD_03	SDI_DELETE, STORAGE_REMOTE	n.a.[57]
SDI_DSD_04	SDI	n.a.[57]
SDI_DSD_05	SDI	n.a.[57]
5.3.2.15 Authentifizierung von Benutzern der TSE (SDI_AUT)		

56 Sieh hierzu Kapitel 8.2.1
57 n.a. wegen Profil SDI

Testcase ID	Profile	Verdict
SDI_AUT_01	SDI	n.a.[57]
SDI_AUT_02	SDI	n.a.[57]
SDI_AUT_03	SDI	n.a.[57]
SDI_AUT_04	SDI	n.a.[57]
SDI_AUT_05	SDI	n.a.[57]
SDI_AUT_06	SDI, SM_REMOTE	n.a.[57]
SDI_AUT_07	SDI, STORAGE_REMOTE	n.a.[57]
5.3.2.16 Abmeldung von Benutzern der TSE (SDI_LGO)		
SDI_LGO_01	SDI	n.a.[57]
SDI_LGO_02	SDI	n.a.[57]
SDI_LGO_03	SDI	n.a.[57]
SDI_LGO_04	SDI	n.a.[57]
SDI_LGO_05	SDI, SM_REMOTE	n.a.[57]
SDI_LGO_06	SDI, STORAGE_REMOTE	n.a.[57]
5.3.2.17 Entsperren von Benutzern(SDI_UBU)		
SDI_UBU_01	SDI	n.a.[57]
SDI_UBU_02	SDI	n.a.[57]
SDI_UBU_03	SDI	n.a.[57]
SDI_UBU_04	SDI	n.a.[57]
SDI_UBU_05	SDI, SM_REMOTE	n.a.[57]
SDI_UBU_06	SDI, STORAGE_REMOTE	n.a.[57]
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.[58]
CI_UDT_03	CUSTOM_INTEGRATION_INTERFACE, STORAGE_REMOTE	n.a.[59]
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	n.a.[60]
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	n.a.[61]
EXP_LOG_04	SM_BASIC, SDI	n.a.[62]

58 n.a. wegen Profil SM_REMOTE
59 n.a. wegen Profil STORAGE_REMOTE
60 Das Feld „description“ ist nicht vom Hersteller vorbesetzt.
61 n.a. wegen Profil SDI
62 n.a. wegen Profil SDI

Testcase ID	Profile	Verdict
EXP_LOG_05	SM_BASIC	Pass
EXP_LOG_06	SM_BASIC	Pass
EXP_LOG_07	SM_NOAGG	n.a.[63]
EXP_LOG_08	SM_NOAGG	n.a.[64]
EXP_LOG_09	SM_AGG	Pass
EXP_LOG_10	SM_AGG	Pass
EXP_LOG_11	SM_NOAGG	n.a.[65]
EXP_LOG_12	SM_AGG	Pass
EXP_LOG_13	SM_BASIC	Pass
EXP_LOG_14	SM_BASIC	n.a.[66]
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
SM_ARCH_03	-	Pass
SM_ARCH_04	-	Pass
SM_ARCH_05	-	Pass
SM_ARCH_06	-	Pass
SM_ARCH_07	-	Pass
SM_ARCH_08	-	Pass
SM_ARCH_09	-	Pass
2.2 Ergänzende Testfälle zu Log-Nachrichten		
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	-	n.a.[67]

63 n.a. wegen Profil SM_NOAGG
64 n.a. wegen Profil SM_NOAGG
65 n.a. wegen Profil SM_NOAGG
66 Das Feld „description“ ist nicht vom Hersteller vorbesetzt.
67 Das Event „updateDevice“ ist gemäß [BSI TR-03153-TS-KuA] optional und wird durch vom Prüfgegenstand nicht unterstützt.

Testcase ID	Profile	Verdict
EXP_LOG_20_I	-	Pass / Fail[68]
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	-	n.a.[69]
EXP_LOG_20_Q	-	n.a.[70]
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.[71]
EXP_LOG_21_I	-	Pass / Fail[72]
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.[73]
EXP_LOG_21_Q	-	n.a.[74]
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.[75]

68 Siehe Kapitel 8.2.3
69 Das Event „lockTransactionLoging“ ist gemäß [BSI TR-03153-TS-KuA] optional und wird durch vom Prüfgegenstand nicht unterstützt.
70 Das Event „unlockTransactionLoging“ ist gemäß [BSI TR-03153-TS-KuA] optional und wird durch vom Prüfgegenstand nicht unterstützt.
71 Das Event „updateDevice“ ist gemäß [BSI TR-03153-TS-KuA] optional und wird durch vom Prüfgegenstand nicht unterstützt.
72 Siehe Kapitel 8.2.3
73 Das Event „lockTransactionLoging“ ist gemäß [BSI TR-03153-TS-KuA] optional und wird durch vom Prüfgegenstand nicht unterstützt.
74 Das Event „unlockTransactionLoging“ ist gemäß [BSI TR-03153-TS-KuA] optional und wird durch vom Prüfgegenstand nicht unterstützt.

Testcase ID	Profile	Verdict
EXP_LOG_22_I	-	Pass / Fail[76]
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	-	n.a.[77]
EXP_LOG_22_Q	-	n.a.[78]
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	-	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

8.2.1 Name der Fehlermeldung ErrorUnexportedStoredData

Festgestellte Abweichung: Der Prüfgegenstand liefert im Prüffall SDI_DSD_02 nicht wie verlangt den Fehlercode „ErrorUnexportedStoredData“, sondern „ErrorLogMessagesNotExported“.

75 Das Event „updateDevice“ ist gemäß [BSI TR-03153-TS-KuA] optional und wird durch vom Prüfgegenstand nicht unterstützt.
76 Siehe Kapitel 8.2.3
77 Das Event „lockTransactionLoging“ ist gemäß [BSI TR-03153-TS-KuA] optional und wird durch vom Prüfgegenstand nicht unterstützt.
78 Das Event „unlockTransactionLoging“ ist gemäß [BSI TR-03153-TS-KuA] optional und wird durch vom Prüfgegenstand nicht unterstützt.

Bewertung: Da der Prüfgegenstand das Profil SDI nicht unterstützt ist die Ausgabe des im Prüffall geforderten Fehlercodes nicht relevant.

Erforderliche Maßnahme: -

8.2.2 Aktualisierung der Zeit nach Deaktivierung des Sicherheitsmoduls

Festgestellte Abweichung: Der Prüfgegenstand liefert im Prüffall II_DSE_01 nicht in jedem Fall die nach [BSI TR-03153-TS] erwartete Fehlermeldung zurück, da die Zeit auch zentral im CSP verwaltet wird.

Bewertung: Aus dem Prüffall geht hervor, dass eine Fehlermeldung erzeugt wird. Daher wird dies nicht als Problem angesehen.

Erforderliche Maßnahme: -

8.2.3 Log-Nachricht updateDeviceCompleted

Festgestellte Abweichung: Die konforme Erstellung der Log-Nachricht updateDeviceCompleted konnte im Rahmen der Konformitätsprüfung für Konfigurationen des Prüfgegenstands mit TSS Client v1.3.4 nicht geprüft werden (Prüffälle EXP_LOG_20/21/22_I).

Bewertung: Die Prüffälle EXP_LOG_20/21/22_I wurden für Konfigurationen des Prüfgegenstands mit TSS Client v1.3.4 mit „Fail“ bewertet. Die Prüffälle konnten nicht durchgeführt werden, da zum Zeitpunkt der Konformitätsprüfung ältere Installationen des D-Trust Web-Dienst für TSE mit Version echt kleiner 3.0 aufgrund abgelaufener Code-Signing-Zertifikate nicht mehr lauffähig waren und somit auch kein Update einer älteren Produktversion auf Konfigurationen mit TSS Client v1.3.4 mehr möglich bzw. zu erwarten ist.

Dass eine konforme updateDeviceCompleted Log-Nachricht geschrieben wird, wurde jedoch im vorherigen Zertifizierungsverfahren BSI-K-TR-0474-2021 (D-Trust Web-Dienst für TSE Version 3.0) mit identischem TSS Client v1.3.4 aber älterem CSP-L v1.3.1 nachgewiesen.

Der CSP ist an der Erkennung , dass ein Update durchgeführt wurde, nicht involviert, sondern stellt ausschließlich Signatur, Uhrzeit und Signaturzähler für die Log-Nachricht bereit.

Bei einer Aktualisierung nur des CSP ausgehend von dem unter BSI-K-TR-0474-2021 zertifizierten D-Trust Web-Dienst für TSE Version 3.0 bestehend aus TSS Client v1.3.4 & CSP-L v1.3.1 auf eine Konfiguration des Prüfgegenstands bestehend aus TSS Client v1.3.4 & CSP-L v1.4.1 wird keine updateDeviceCompleted Log-Nachricht erstellt. Dies ist gemäß [BSI TR-03153-TS-KuA] auch nicht verpflichtend.

Dass das Verhalten des Prüfgegenstands für Konfigurationen mit TSS Client v1.3.4 gegenüber der unter BSI-K-TR-0474-2021 zertifizierten Produktversion abweicht ist somit unwahrscheinlich. Um dies jedoch vollständig auszuschließen, wird folgende Maßnahme für den Prüfgegenstand festgelegt.

Erforderliche Maßnahme: Konfigurationen des Prüfgegenstands mit TSS Client v1.3.4 dürfen nur per Erst-Installation und nicht durch Aktualisierung einer älteren Produktversion in Betrieb genommen werden.

Hinweis: Für Konfigurationen des Prüfgegenstands mit TSS Client v1.4.3 konnte die konforme Erstellung der updateDeviceCompleted Log-Nachricht nachgewiesen werden. Die Prüffälle EXP_LOG_20/21/22_I wurden für diese Konfigurationen mit „Pass“ bewertet.

8.2.4 TerminateStaleTransactions

Festgestellte Abweichung: Der Prüfgegenstand bietet bei Betrieb unter Verwendung des TSS Client v1.3.4 die Funktion *terminateStaleTransaction* als Komfortfunktionalität an, mit der die TSE selbstständig „alte“ bzw. „abgestandene“ Transaktionen beenden kann. Eine vollständige Konformität dieser Funktion zu den Anforderungen der [BSI TR-03153] konnte im Rahmen der Konformitätsprüfung nicht nachgewiesen werden.

Bewertung: Zwar wurde das Problem der Belegung des Feldes „processData“ in der Transaction-Log-Message behoben (das Datenfeld ist vorhanden aber leer), jedoch fällt gleichzeitig das Feld „processType“, welches bei einem FinishTransaction-Log zwingend vorhanden sein muss, vollends weg. Auch ist unklar, wie sich die Funktion im Fehlerfall verhält. Ebenso ist unklar, wie sich die Funktion gegenüber aggregierten, nicht-abgesicherten Transaktionsdaten verhält.

Insgesamt ist die Konformität der Funktion daher nicht gegeben und eine Nutzung von *terminateStaleTransactions* würde nicht-konforme Situationen und Lognachrichten produzieren.

Der Antragsteller muss seinen Integratoren die Unzugänglichmachung dieser Funktion für Endkunden vorgeben. Hierzu wurden die Integrationsanforderungen [INT_ANF] um einen entsprechenden Passus ergänzt.

Erforderliche Maßnahme: Verbot der Nutzung der Funktion *terminateStaleTransactions* für den durch die Zertifizierung gedeckten Betrieb bei Verwendung des TSS Client v1.3.4.

Bei bei Verwendung des TSS Client v1.3.4 muss der Integrator sicherstellen, dass diese Funktion durch niemanden, insbesondere nicht die Endkunden, genutzt werden kann.

Bei Verwendung des TSS Client v1.3.4 muss der Antragsteller durch organisatorische Maßnahmen sicherstellen, dass *terminateStaleTransactions* nicht genutzt werden kann.

Hinweis: Die Funktion *terminateStaleTransactions* wurde im TSS Client v1.4.3 entfernt.

8.2.5 Einschränkung des zertifizierten Betriebs auf getestete Ablaufumgebungen

Im Rahmen der Konformitätsprüfung wurde der Prüfgegenstand auf verschiedenen Host-Systemen für die Client-Komponente geprüft. Der Prüfbericht bestätigt die Konformität des Prüfgegenstands für verschiedene Kombinationen aus Hardware, Java Virtual Machine und Betriebssystem.

Die Konformität des Prüfgegenstands kann ausschließlich für die im Rahmen der Konformitätsprüfung geprüften, in Kapitel 7.3 aufgeführten Hardware-Betriebssystem-JVM-Kombinationen bestätigt werden.

Erforderliche Maßnahme: Für einen zertifizierten Betrieb muss die Client-Komponente des Prüfgegenstands mit einer in Kapitel 7.3 aufgeführten Betriebssystem-JVM-Kombination und auf einer Hardware, welche die entsprechenden Mindestanforderungen erfüllt, betrieben werden. Der Betrieb der Server-Komponente (Remote CSP Service) ist ausschließlich auf Red Hat Enterprise Linux 8.9 (Ootpa) zulässig.

8.2.6 Fehlende Logs beim Export bei Abweichungen der Zeit zwischen CSP und SMAERS

Festgestellte Abweichung: Der Prüfgegenstand liefert im Prüffall bei einer Differenz der Uhrzeiten zwischen CSP-L und SMAERS eventuell nicht alle Audit-Log-Nachrichten bei einem Export aus.

Bewertung: Das Problem wird voraussichtlich immer dann bestehen, wenn die SMAERS und CSP-L Komponenten divergierende Uhrzeiten aufweisen. Der Antragsteller weist in [INT_ANF] darauf hin, dass eine Differenz der Uhrzeit zwischen CSP-L und SMAERS zu vermeiden ist. Da die meisten Ereignisse auch in Form eines System-Logs aufgezeichnet werden und die steuerlich relevanten Daten mittels Transaktions-Logs gesichert werden, sind diese laut Prüfbericht von diesem Problem nicht betroffen.

Erforderliche Maßnahme: Bis zur nächsten, zur Re-Zertifizierung vorgelegten Version des Prüfgegenstands eine konforme Behebung dieses Problems nachzuweisen oder es sind in Abstimmung mit der Zertifizierungsstelle weitere Maßnahmen zur Begrenzung des durch diese Abweichung auftretenden Schadenspotentials festzulegen.

8.2.7 Weitere Vorgaben für einen zertifizierten Betrieb

Das Prüflaboratorium weist im Prüfbericht darauf hin, dass für einen zertifizierten Betrieb die Anforderungen einiger Zusatzdokumente einzuhalten sind.

Erforderliche Maßnahme: Für einen zertifizierten Betrieb der Client-Komponente der TSE sind die Vorgaben der folgenden Dokumente einzuhalten:

- D-Trust-TSE-Web Leitlinie zum Schutz von SMAERS durch die Umgebung, Version 6.9 vom 19. August 2021, [D-Trust_US_SMAERS]
- D-Trust-TSE-Web Trust Provisioning, Version 1.9 vom 20. September 2021, [D-Trust_TP_SMAERS]
- D-Trust-TSE-Web Interface Specification TSS Client, Version 1.12.5 vom 17. März 2022, [IS_TSS_Client], bzw. Version 1.11 vom 13. September 2021, [IS_TSS_Client_alt]
- Integrationsanforderungen des D-Trust TSE-Webservices, Version 5.1 vom 20. Februar 2024, [INT_ANF]
- D-Trust-TSE-Web Nutzungsbedingungen, Version 5.1 vom 20. Februar 2024, [NUTZ_BED]

9 Ergebnis der Konformitätsprüfung

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

TÜV-IT
Prüfbericht BSI TR-03153
BSI-K-TR-0524
D-TRUST WEB-Dienst für TSE v3.1
Prüfbericht Version 4
Erstellungsdatum: 20. Februar 2024

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 Prüffälle des Moduls *Storage – Speichermedium (STO)* konnten mit „Pass“ bewertet werden;
- alle relevanten Prüffälle des Moduls *Security Module – Sicherheitsmodul (SM)* konnten mit „Pass“ bewertet werden;
- bei der Durchführung der relevanten Prüffälle des Moduls *Integration Interface – Einbindungsschnittstelle* wurden die Prüffälle SDI_DSD_02[79] und II_DSE_01[80] mit „Fail“ bewertet; alle übrigen relevanten Prüffälle konnten mit „Pass“ bewertet werden;
- alle relevanten Prüffälle des Moduls *Prüfung der Exportdaten gemäß BSI TR-03153* konnten mit „Pass“ bewertet werden;
- bei der Durchführung der relevanten Prüffälle gemäß [BSI TR-03153-TS-KuA] wurden die Prüffälle EXP_Log_20/21/22_I[81] mit „Fail“ bewertet; alle übrigen relevanten Prüffälle konnten mit „Pass“ bewertet werden.

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

79 Siehe Kapitel 8.2.1
80 Siehe Kapitel 8.2.2
81 Siehe Kapitel 8.2.3

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-0524-2024 vom 26. Februar 2024 mit Auflagen bestätigt.

Das Zertifikat nach Technischen Richtlinien ist gültig bis zum 25. Februar 2032 unter der Voraussetzung, dass die in Kapitel 7.5 dieses Konformitätsreports aufgeführten, mitgeltenden Zertifizierungen ihre Gültigkeit behalten.

Aufgrund der im Rahmen der Konformitätsprüfung identifizierten Einschränkungen und Abweichungen von der Prüfgrundlage werden darüber hinaus folgende Auflagen festgelegt:

1. Für einen zertifizierten Betrieb des Prüfgegenstands sind die in Kapitel 8.2 dieses Konformitätsreports aufgeführten, erforderlichen Maßnahmen sind vorzunehmen und einzuhalten.

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 BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) vom 2. September 2019, Bundesgesetzblatt Teil I, S. 1365

VB-Produkte.PD Verfahrensbeschreibung zur Zertifizierung von Produkten und Dienstleistungen, Version 3.2 vom 28.10.2022

TR-Produkte.PD Zertifizierung von Produkte, Prozessen und Dinestleistungen: Programm Technische Richtlinien (TR), Version 2.2 vom 31.01.2023

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

KassenSichV Verordnung zur Bestimmung der technischen Anforderungen an elektronische Aufzeichnungs- und Sicherungssysteme im Geschäftsverkehr (Kassensicherungsverordnung - KassenSichV) vom 26. September 2017, Bundesgesetzblatt I, S3515

INT_ANF D-TRUST-TSE-WEB - Integrationsanforderungen, Version 5.1 vom 20.02.2024

NUTZ_BED D-TRUST-TSE-WEB - Nutzungsbedingungen, Version 5.1 vom 20.02.2024

D-Trust_US_SMAERS D-Trust-TSE-WEB - Leitlinie zum Schutz von SMAERS durch die Umgebung, Version 6.9 vom 19. August 2021

D-Trust_TP_SMAERS D-Trust-TSE-WEB - Trust Provisioning, Version 1.9 vom 20. September 2021

IS_TSS_Client D-TRUST-TSE-WEB, Interface Specification TSS Client,Version 1.12.5 vom 17. März 2022

IS_TSS_Client_alt D-Trust-TSE-Web Interface Specification TSS Client, Version 1.11 vom13. September 2021