Bundesamt
für Sicherheit in der
Informationstechnik

Konformitätsreport

BSI-K-TR-0550-2023

RECORDPROOF® - MW

Version 2.1.1

der

timeproof GmbH

Münchnerstr. 33, 82319 Starnberg, Deutschland

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 (sicherheits-) technischen, funktionalen und qualitativen Anforderungen einer TR erfüllt.

Konformitätsprüfungen werden von den vom BSI gemäß DIN ISO/IEC 17025 anerkannten Prüfstellen oder zertifizierten Auditoren für ISO 27001 Audits auf der Basis von IT-Grundschutz gemäß den in der jeweiligen TR definierten Prüfspezifikationen und Tests durchgeführt. Die Konformitätsprüfung eines Prüfgegenstands erfolgt in Übereinstimmung mit den Bestimmungen des entsprechenden BSI-Schemas zur Zertifizierung nach Technischen Richtlinien.

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

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

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

2 Grundlagen des Zertifizierungsverfahrens

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

- BSI-Gesetz – Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009, Bundesgesetzblatt Teil I Nr. 54, S. 2821, [BSIG]
- BSI-Zertifizierungs- und Anerkennungsverordnung – Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSIZertV), vom 17. Dezember 2014, Bundesgesetzblatt Teil I Nr. 61, S. 2231, [BSIZertV]
- Besondere Gebührenverordnung des Bundesministeriums des Inneren, für Bau und Heimat für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (Besondere Gebührenverordnung BMI, BMIBGebV) vom 02. September 2019, Bundesgesetzblatt I, S. 1359, [BMIBGebV]
- Verfahrensbeschreibung zur Zertifizierung von Produkten, Prozessen und Dienstleistungen, VB-Produkte.PD, Version 3.1.1 vom 06.09.2022, [VB-Produkte]
- Zertifizierung von Produkten, Prozessen und Dienstleistungen: Programm Technische Richtlinien (TR), TR-Produkte.PD, Version 2.1 vom 30.08.2022, [TR-Produkte]

3 Hinweise für den Antragsteller

1. Das vom BSI erteilte Zertifikat nach Technischen Richtlinien BSI-K-TR-0550-2023 ist nur in Zusammenhang mit dem vollständigen Konformitätsreport gültig.
2. Die Gültigkeit des Zertifikats erstreckt sich ausschließlich auf die geprüfte Version bzw. Konfiguration des Prüfgegenstands. Alle geprüften Komponenten des Prüfgegenstands und deren Versionsstände sind in Kapitel 7 des Konformitätsreports festgeschrieben.
3. Die Gültigkeit eines Zertifikats nach der Technischen Richtlinie BSI TR-03125 beträgt fünf 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

timeproof GmbH
Münchnerstr. 33

82319 Starnberg

Deutschland

Ansprechpartner:

Herr Olaf Feller (olaf.feller@timeproof.de)

mit Antragsdatum 29. Juni 2022 (Eingangsdatum BSI: 04. Juli 2022) beim BSI eine erstmalige Zertifizierung nach Technischen Richtlinien beantragt.

5 Prüfbereich und Prüfgrundlage

Beantragt wurde eine Zertifizierung nach der Technischen Richtlinie:

BSI TR-03125 – Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR, Preservation of Evidence of Cryptographically Signed Documents)

Die Konformitätsprüfung nach der Technischen Richtlinie BSI TR-03125 erfolgte für den Prüfbereich:

BSI TR-03125 – Beweiswerterhaltung kryptographisch signierter Dokumente

Die Prüfgrundlage für Konformitätsprüfungen in diesen Prüfbereichen bildeten folgende Dokumente:

BSI TR-03125 – Beweiswerterhaltung kryptographisch signierter Dokumente, Version 1.2.2 vom 03.05.2029 [BSI TR-03125]

BSI TR-03125 M.1 – Beweiswerterhaltung kryptographisch signierter Dokumente Anlage M.1: ArchiSafe-Modul, Version 1.2.1 vom 15.03.2018 [BSI TR-03125 M.1]

BSI TR-03125 M.2– Beweiswerterhaltung kryptographisch signierter Dokumente Anlage M.2: Krypto-Modul, Version 1.2.1 vom 15.03.2018 [BSI TR-03125 M.2]

BSI TR-03125 M.3 – Beweiswerterhaltung kryptographisch signierter Dokumente Anlage M.3: ArchiSig-Modul, Version 1.2.1 vom 15.03.2018 [BSI TR-03125 M.3]

BSI TR-03125 B – Beweiswerterhaltung kryptographisch signierter Dokumente Anlage B: Profilierung für Bundesbehörden, Version 1.2.1 vom 15.03.2018 [BSI TR-03125 B]

BSI TR-03125 E – Beweiswerterhaltung kryptographisch signierter Dokumente Anlage E: Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks, Version 1.2.2 vom 02.05.2019 [BSI TR-03125 E]

BSI TR-03125 F – Beweiswerterhaltung kryptographisch signierter Dokumente Anlage F: Formate und Protokolle, Version 1.2.2 vom 02.05.2019 [BSI TR-03125 F]

BSI TR-03125 X– Beweiswerterhaltung kryptographisch signierter Dokumente Anlage Profil XBDP: Profilierung des XAIP mit XBARCH, XDOMEA und PREMIS, Version 1.2.1 vom 15.03.2018 [BSI TR-03125 X]

BSI TR-03125 VR– Beweiswerterhaltung kryptographisch signierter Dokumente Anlage VR: Verification Reports for Selected Data Structures, Version 1.2.1 vom 15.03.2018 [BSI TR-03125 VR]

BSI TR-03125 ERS– Beweiswerterhaltung kryptographisch signierter Dokumente Anlage ERS: Profilierung der Evidence Records gemäß RFC4998 und RFC6283 (Konformitätsstufe 2 – technische Konformität), Version 1.2.1 vom 15.03.2018 [BSI TR-03125 ERS]

BSI TR-03125 APP – Beweiswerterhaltung kryptographisch signierter Dokumente Anlage APP: Profilierung einiger TR-ESOR Assessment Kriterien zur ETSI TS 119511 Prüferleichterung, Version 1.2.2 vom 01.04.2021 [BSI TR-03125 APP]

BSI TR-03125 C.1 – Beweiswerterhaltung kryptographisch signierter Dokumente Anlage C.1: Conformity Test Specification (Level 1 – Functional Conformity), Version 1.2.2 vom 15.03.2021 [BSI TR-03125 C.1]

6 Prüfstelle

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

datenschutz cert GmbH
Konsul-Smidt-Straße 88a
28217 Bremen
Tel.: 0421 69 66 32 50
Fax: 0421 69 66 32 51
office@datenschutz-cert.de

7 Prüfgegenstand

7.1 Beschreibung des Prüfgegenstands

Prüfgegenstand ist das IT-Produkt/-System:

RECORDPROOF® - MW, Version 2.1.1

Bei dem Prüfgegenstand handelt es sich um eine Lösung für eine von Fachverfahren unabhängige, vertrauenswürdige und beweiswerterhaltende Langzeitspeicherung nach den Grundsätzen der Technischen Richtlinie BSI TR-03125 (TR-ESOR).

7.2 Komponenten des Prüfgegenstands

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

Tabelle 1: Komponenten des Prüfgegenstands

Nr.	Typ	Komponente	Datei / Version	Hashwert (SHA256)
1	SW	ArchiSafe	tr-archisafe-0.3.1-SNAPSHOT.jar	2f75aa33d9080afe5d6b447f6382ae4ca4017dd6eabe35471ae1370c3e40225b
2	SW	ArchiSig	tr-archisig-0.3.1-SNAPSHOT.jar	ccf82eee9534064f326c258c646ea6ca687eb4608ef6d4c47fabaff02fb0d4f4
3	SW	Krypto	tr-crypto-s1-0.3.1-SNAPSHOT.jar	30a9b79a95305fa5f44f99e6557d725a9627de8300425d59819508d9572ce03c
			tr-crypto-s3-0.3.1-SNAPSHOT.jar	45056336a8d0b82b0f946c8ca89c6d792dcf58d32625a9c8e9c723126c038a1a
			tr-verify-service-1.0.0-SNAPSHOT.jar	d43b223da676fbeac7941605f6ac2fc6da9600c5770b61c4f990b4b815ab36df
4	SW	Upload/ Download	tr-file-0.3.1-SNAPSHOT.jar	a885704ba891e53c718c72a9dc0c1989e7115970702b1e0f6367a266ac0650db

Der Prüfgegenstand besteht aus vier Java-Applikationen. Hinsichtlich der Referenzarchitektur der BSI TR-03125 realisiert er folgende Module:

ArchiSig Modul

ArchiSafe Modul

Krypto-Modul

Upload/Download Modul

Für den Betrieb des Prüfgegenstands werden darüber hinaus folgende weitere Komponenten benötigt, die nicht Bestandteil des Prüfgegenstands sind und nicht im Rahmen der Konformitätsprüfung geprüft wurden (siehe Tabelle 2):

Tabelle 2: Sonstige Komponenten, nicht zum Prüfgegenstand gehörig

Nr	Identifier	Version	Bemerkung
1	Client Anwendung	n.a.	
2	Langzeitspeicher	n.a.	

Client Anwendungen sind Endanwendungen oder Fachverfahren, die von einem Benutzer bedient werden, um Dokumente zu archivieren. Als Langzeitspeicher, in dem die Archivdaten abgelegt werden, können z. B. ein dateibasiertes Speichersystem oder eine Datenbank verwendet werden.

Fachverfahren sollen die zu speichernden Daten als XAIP bereitstellen und müssen eine definierte Webservice- Schnittstelle bedienen. Für die Konformitätsprüfung wurde Testskripte zur Verfügung gestellt.

7.3 Implementation Conformance Statement

Das Implementation Conformance Statement (ICS) enthält die für die Durchführung der Konformitätsprüfung benötigten Informationen zum Prüfgegenstand, gibt Aufschluss über dessen Funktionalität und definiert den Prüfumfang. Der Umfang der Konformitätsprüfung wird aus den vom Prüfgegenstand umgesetzten Funktionsmodulen der Prüfgrundlage abgeleitet.

Der Prüfgegenstand erhebt Anspruch auf funktionale Konformität zu den Anforderungen der BSI TR-03125 an die Module

ArchiSig

ArchiSafe

Krypto

sowie die Schnittstellen

S.1

S.4

8 Konformitätsprüfung

8.1 Konformitätsprüfung gemäß BSI TR-03125

Die Konformitätsprüfung wurde im Zeitraum November 2021 bis November 2022 von der beauftragten Prüfstelle durchgeführt.

Tabelle 3 enthält eine Übersicht über die im Rahmen der Konformitätsprüfung durchgeführten Prüffälle gemäß [BSI TR-03125 C.1] & [BSI TR-03125 APP] sowie die erzielten Prüfergebnisse. Die vollständigen Prüfergebnisse sind im von der Prüfstelle vorgelegten Prüfbericht enthalten.

Tabelle 3: Prüfumfang gemäß BSI TR-03125, Anhang C.1 & APP

Nr	Prüffall	Verdict
4.1 Tests for all products		
01	A-01	Pass
02	A-02	Pass
03	A-03	Pass
04	A-03.1	Pass
05	A-03.2	Pass
06	A-03.3	Pass
07	A-04	Pass
08	A-05	Pass
09	A-06	Pass
10	A-07	Pass
11	A-08	Pass
12	A-09	Pass
13	A-10	Pass
14	A-11	Pass
15	A-12	Pass
16	A-13	Pass
17	A-14	Pass
18	A-15	Pass
4.2 Module 1 - ArchiSafe-Module		
19	M.1-01	n.a.
20	M.1-02	Pass
21	M.1-03	Pass
22	M.1-04	Pass
23	M.1-05	Pass
24	M.1-06	Pass
25	M.1-07	Pass
26	M.1-08	Pass
27	M.1-09	n.a.
28	M.1-10	Pass
29	M.1-11	Pass
4.3 Module 2 - Crypto-Module		
30	M.2-01	n.a.
31	M.2-02	Pass
32	M.2-03	Pass
33	M.2-04	n.a.
34	M.2-05	Pass
35	M.2-06	Pass
36	M.2-07	n.a.
37	M.2-08	Pass
38	M.2-09	Pass

39	M.2-10	Pass
40	M.2-11	Pass
41	M.2-12	Pass
42	M.2-13	Pass
43	M.2-14	n.a.
44	M.2-15	Pass
45	M.2-16	Pass
46	M.2-17	Pass
47	M.2-18	Pass
48	M.2-19	Pass
49	M.2-20	Pass
50	M.2-21	Pass
4.4 Module 3 - ArchiSig-Module		
51	M.3-01	Pass
52	M.3-02	Pass
53	M.3-03	Pass
54	M.3-04	Pass
55	M.3-05	Pass
56	M.3-06	Pass
57	M.3-07	Pass
58	M.3-08	Pass
59	M.3-09	n.a.
60	M.3-10	Pass
61	M.3-11	Pass
62	M.3-12	Pass
63	M.3-13	Pass
64	M.3-14	Pass
65	M.3-15	Pass
66	M.3-16	Pass
67	M.3-17	Pass

68	M.3-18	Pass
69	M.3-19	Pass
70	M.3-20	n.a.
71	M.3-21	Pass
72	M.3-22	Pass
73	M.3-23	Pass
74	M.3-24	Pass
75	M.3-25	Pass
4.5 Interface functions		
4.5.1 Interface S1		
76	S.1.1-01	Pass
77	S.1.1-02	Pass
4.5.4 Interface S4		
78	S.4.1-01	Pass
79	S.4.1-02	Pass
80	S.4.1-03	n.a.
81	S.4.1-04	Pass
82	S.4.1-05	Pass
83	S.4.1-06	Pass
84	S.4.1-07	Pass
85	S.4.1-08	Pass
86	S.4.1-09	Pass
87	S.4.2-01	Pass
88	S.4.2-02	Pass
89	S.4.2-03	Pass
90	S.4.2-04	Pass
91	S.4.2-05	Pass
92	S.4.2-06	Pass
93	S.4.2-07	Pass
94	S.4.2-08	Pass

95	S.4.2-09	Pass
96	S.4.2-10	Pass
97	S.4.3-01	Pass
98	S.4.3-02	Pass
99	S.4.4-01	Pass
100	S.4.4-02	Pass
101	S.4.4-03	Pass
102	S.4.5-01	Pass
103	S.4.5-02	Pass

104	S.4.5-03	Pass
105	S.4.5-04	Pass
106	S.4.5-05	n.a.
107	S.4.5-06	Pass
108	S.4.6-01	n.a.
109	S.4.7-01	Pass
110	S.4.8-01	Pass
111	S.4.9-01	n.a.

9 Ergebnis der Konformitätsprüfung

Die vollständigen Ergebnisse der Konformitätsprüfung sind in folgenden Prüfberichten enthalten:

[1] Prüfbericht nach TR-03125: RECORDPROOF® - MW, Version 2.1.1
Vorgangs-Nr. BSI-K-TR-0550
Version 1.2
Erstellungsdatum 10.11.2022

[2] Konformitätstest Level 1 von RECORDPROOF® - MW, V2.1.1
Testprotokoll auf der Basis von Annex TR-ESOR-C.1 zu
BSI Technical Guideline 03125
Version 1.1
Erstellungsdatum 10.11.2022

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

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

- im Rahmen der Konformitätsprüfung der Module ArchiSig/ArchiSafe/Krypto sowie der Schnittstellen S.1 und S.4 gemäß BSI TR-03125, Anhang C.1 & APP konnten alle durchgeführten Prüffälle 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-03125 wird vom Bundesamt für Sicherheit in der Informationstechnik für den untersuchten Prüfbereich mit dem Zertifikat nach Technischen Richtlinien BSI-K-TR-0550-2023 vom 03. Februar 2023 bestätigt.

Das Zertifikat nach Technischen Richtlinien BSI-TR-0550-2023 ist befristet gültig bis zum 02. Februar 2028.

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 02. September 2019, Bundesgesetzblatt I, S. 1359
VB-Produkte	Verfahrensbeschreibung zur Zertifizierung von Produkten, Prozessen und Dienstleistungen, VB-Produkte.PD, Version 3.1.1 vom 06.09.2022, Bundesamt für Sicherheit in der Informationstechnik
TR-Produkte	Zertifizierung von Produkten, Prozessen und Dienstleistungen: Programm Technische Richtlinien (TR), TR-Produkte.PD, Version 2.1 vom 30.08.2022, Bundesamt für Sicherheit in der Informationstechnik
BSI TR-03125	BSI TR-03125 – Beweiswerterhaltung kryptographisch signierter Dokumente, Version 1.2.2 vom 03.05.2029
BSI TR-03125 M.1	BSI TR-03125 M.1 – Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage M.1: ArchiSafe-Modul, Version 1.2.1 vom 15.03.2018
BSI TR-03125 M.2	BSI TR-03125 M.2– Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage M.2: Krypto-Modul, Version 1.2.1 vom 15.03.2018
BSI TR-03125 M.3	BSI TR-03125 M.3 – Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage M.3: ArchiSig-Modul, Version 1.2.1 vom 15.03.2018
BSI TR-03125 B	BSI TR-03125 B – Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage B: Profilierung für Bundesbehörden, Version 1.2.1 vom 15.03.2018
BSI TR-03125 E	BSI TR-03125 E – Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage E: Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks,Version 1.2.2 vom 02.05.2019
BSI TR-03125 F	BSI TR-03125 F – Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage F: Formate und Protokolle, Version 1.2.2 vom 02.05.2019
BSI TR-03125 X	BSI TR-03125 X– Beweiswerterhaltung kryptographisch signierter DokumenteAnlage Profil XBDP: Profilierung des XAIP mit XBARCH, XDOMEA und PREMIS, Version 1.2.1 vom 15.03.2018
BSI TR-03125 VR	BSI TR-03125 VR– Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage VR: Verification Reports for Selected Data Structures, Version 1.2.1 vom 15.03.2018
BSI TR-03125 ERS	BSI TR-03125 ERS– Beweiswerterhaltung kryptographisch signierter Dokumente Anlage ERS: Profilierung der Evidence Records gemäß RFC4998 und RFC6283 (Konformitätsstufe 2 – technische Konformität), Version 1.2.1 vom 15.03.2018
BSI TR-03125 APP	BSI TR-03125 APP – Beweiswerterhaltung kryptographisch signierter DokumenteAnlage APP: Profilierung einiger TR-ESOR Assessment Kriterien zur ETSI TS 119511 Prüferleichterung, Version 1.2.2 vom 01.04.2021

BSI TR-03125 C.1 BSI TR-03125 C.1 – Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage C.1: Conformity Test Specification (Level 1 – Functional Conformity), Version 1.2.2 vom 15.03.2021