TÜVIT

Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH
bescheinigt hiermit dem Unternehmen

All-INKL.COM – Neue Medien Münnich
Hauptstraße 68
02742 Friedersdorf

Zertifikatsgültigkeit:
17.11.2023 – 17.11.2025

für das IT-System

KAS Passwort-Manager

die Erfüllung aller Anforderungen der Kriterien

Sicherheitstechnische Qualifizierung (SQ)
Version 10.0
Security Assurance Level SEAL-3

der TÜV Informationstechnik GmbH. Die Anforderungen sind in der Anlage zum Zertifikat zusammenfassend aufgelistet.

Die Anlage ist Bestandteil des Zertifikats mit der ID 9563.23 und besteht aus 4 Seiten.

Essen, 17.11.2023

Dr. Christoph Sutter, Leiter Zertifizierungsstelle

Zum Zertifikat

TÜV Informationstechnik GmbH
Am TÜV 1 ▪ 45307 Essen
tuvit.de

TÜVNORDGROUP

Zertifizierungsprogramm

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH führt Zertifizierungen auf Basis des folgenden Zertifizierungsprogramms durch:

- „Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 1.1 vom 01.03.2020, TÜV Informationstechnik GmbH

Evaluierungsbericht

- „Evaluierungsbericht – Sicherheitstechnische Qualifizierung, KAS Passwort-Manager“, Version 1.0 vom 31.08.2023, TÜV Informationstechnik GmbH

Evaluierungsanforderungen

- „Trusted Site Security / Trusted Product Security, Sicherheitstechnische Qualifizierung (SQ) Anforderungskatalog der Version 10.0“, Dokumentationsversion 2.9 vom 11.11.2022, TÜV Informationstechnik GmbH
- Systemspezifische Sicherheitsanforderungen (siehe unten)

Die Evaluierungsanforderungen sind am Ende zusammenfassend aufgeführt.

Zertifikatsgegenstand

Zertifikatsgegenstand ist das IT-System „KAS Passwort-Manager“ der All-INKL.COM – Neue Medien Münnich. Dieser wird im Evaluierungsbericht detailliert beschrieben.

Evaluierungsergebnis

Die anwendbaren Anforderungen für die Sicherheitstechnische Qualifizierung nach Security Assurance Level SEAL-3 sind erfüllt.

Die systemspezifischen Sicherheitsanforderungen sind erfüllt.

Die im Evaluierungsbericht genannten Empfehlungen sind zu beachten.

Systemspezifische Sicherheitsanforderungen

Die folgenden systemspezifischen Sicherheitsanforderungen lagen der Zertifizierung zugrunde und wurden überprüft:

1 Identifizierung und Authentifizierung

Das Kunden Administrationssystem (KAS) identifiziert und authentisiert den Kunden eindeutig und hinreichend stark, um gängigen Angriffen standzuhalten.

2 Zugriffskontrolle

Der Zugriff auf Funktionen und sensible Daten des KAS Passwort-Managers durch unbefugte Personen wird verhindert.

3 Passwortmanagement

Die vom KAS Passwort-Manager verwalteten Kundenpasswörter sind mit dem MasterKey verschlüsselt. Der MasterKey wird mit dem Masterpasswort verschlüsselt. Das Masterpasswort wird vom Kunden festgelegt und dient zur Anmeldung am Kunden Administrationssystem (KAS). Erfolgt die Anmeldung am KAS per Deep-Link steht das Masterpasswort nicht zur Verfügung und somit ist die Entschlüsselung des MasterKeys nicht möglich. Das Masterpasswort wird nicht dauerhaft gespeichert, sondern nur im Moment des Logins zur Authentifizierung sowie zur Entschlüsselung des MasterKeys verwendet.

4 Transportverschlüsselung

Alle zum Zwecke der Authentisierung abgeleitete Sicherheitsmerkmale werden im Rahmen des Session-Managements zwischen dem Webbrowser des Kunden und dem Web Frontend des KAS Passwort-Managers gemäß den empfohlenen Algorithmen der BSI TR-02102-2 mittels TLSv1.2 (oder höher) verschlüsselt übertragen.

Zusammenfassung der Evaluierungsanforderungen für die Sicherheitstechnische Qualifizierung (SQ), Version 10.0

1 Technische Sicherheitsanforderungen

Die technischen Sicherheitsanforderungen müssen dokumentiert, widerspruchsfrei und überprüfbar sein. Die Spezifikation muss in Anlehnung an ISO/IEC 17007 erfolgen. Des Weiteren müssen die technischen Sicherheitsanforderungen im Rahmen einer individuellen Bedrohungs- und Risikoanalyse hergeleitet sein, sie müssen aus bereits definierten Schutzprofilen hergeleitet sein, oder sie müssen konform zu veröffentlichten Sicherheitsanforderungen anerkannter Autoritäten oder Gremien der IT-Sicherheit sein. Weiterhin müssen sie für den Einsatzzweck des IT-Systems angemessen sein und geltenden Sicherheitsansprüchen genügen.

2 Architektur und Design

Das IT-System muss sinnvoll und verständlich strukturiert sein. Seine Komplexität darf keinen Einfluss auf die Sicherheit haben. Die Härtungs- und Schutzmaßnahmen müssen angemessen und wirkungsvoll sein. Es darf keine konzeptionellen Schwachstellen enthalten, mit deren Hilfe sicherheitsrelevante Komponenten umgangen oder deaktiviert werden können.

3 Installation und Betrieb (ab SEAL-4)

Die vorhandenen Überwachungsmaßnahmen müssen wirkungsvoll sein. Die überwachten Ereignisse müssen geeignet sein, Sicherheitsvorfälle zuverlässig und zeitnah zu erkennen. Die Administration erfolgt über einen vertrauenswürdigen Pfad hinsichtlich Vertraulichkeit und Integrität. Die Dokumentation muss verständlich und nachvollziehbar sein. Sie muss den berechtigten Personen bekannt und jederzeit frei zugänglich sein.

4 Schwachstellenanalyse und Penetrationstests

Die Sicherheitsmaßnahmen des IT-Systems müssen einer Überprüfung durch Penetrationstests standhalten. Es darf nicht möglich sein, Sicherheitsmaßnahmen zu brechen oder zu umgehen. Das IT-System muss sicher konfiguriert sein, darf keine ausnutzbaren Schwachstellen haben und muss alle definierten technischen Sicherheitsanforderungen erfüllen.

5 Änderungsmanagement (ab SEAL-5)

Das Patch-Management muss dokumentiert und für das IT-System geeignet sein. Das Vorgehen bei Änderungen am IT-System muss klar definiert und geeignet sein. Die beteiligten Personen müssen damit vertraut sein. Verantwortlichkeiten müssen eindeutig geregelt sein. Änderungen dürfen nicht zu einer Reduzierung des erreichten Sicherheitsniveaus führen.

Security Assurance Level

Die folgende Tabelle zeigt die für den Security Assurance Level anwendbaren Evaluierungskriterien für IT-Systeme. Eine Zertifizierung eines IT-Systems ist möglich ab Level SEAL-3.

		Security Assurance Level				
		SEAL-1	SEAL-2	SEAL-3	SEAL-4	SEAL-5
Evaluierungskriterien	Technische Sicherheits-anforderungen	X	X	X	X	X
	Architektur und Design			X	X	X
	Installation und Betrieb				X	X
	Schwachstellenanalyse und Penetrationstests		X	X	X	X
	Änderungsmanagement					X

Tabelle: Evaluierungskriterien und Security Assurance Level für IT-Systeme