TÜVIT

Certificate

The certification body of TÜV Informationstechnik GmbH
hereby awards this certificate to the company

All-INKL.COM – Neue Medien Münnich
Hauptstraße 68
02742 Friedsdorf, Germany

Certificate validity:
2023-11-17 – 2025-11-17

to confirm that its IT system

KAS Passwort-Manager

fulfils all requirements of the criteria

Security Qualification (SQ)
version 10.0
Security Assurance Level SEAL-3

of TÜV Informationstechnik GmbH. The requirements are summarized in the appendix to the certificate.

The appendix is part of the certificate with the ID 9563.23 and consists of 4 pages.

Essen, 2023-11-17

Dr. Christoph Sutter, Head of Certification Body

To Certificate

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

Certification scheme

The certification body of TÜV Informationstechnik GmbH performs its certifications based on the following certification scheme:

- German document: “Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH”, version 1.1 as of 2020-03-01, TÜV Informationstechnik GmbH

Evaluation report

- German document: “Evaluierungsbericht – Sicherheitstechnische Qualifizierung, KAS Passwort-Manager”, version 1.0 as of 2023-08-31, TÜV Informationstechnik GmbH

Evaluation requirements

- “Trusted Site Security / Trusted Product Security, Security Qualification (SQ) Requirements Catalog for version 10.0”, documentation version 2.9 as of 2022-11-11, TÜV Informationstechnik GmbH

- System-specific security requirements (see below)

The evaluation requirements are summarized at the end.

Evaluation target

Evaluation target is the IT system “KAS Passwort-Manager” of All-INKL.COM – Neue Medien Münnich. It is detailed in the evaluation report.

Evaluation result

All applicable evaluation requirements for the security qualification with Security Assurance Level SEAL-3 of IT systems are fulfilled.

The system-specific security requirements are fulfilled.

The recommendations of the evaluation report have to be regarded.

System-specific Security Requirements

The following system-specific security requirements are the basis of the certification and have been checked.

1 Identification and authentication

The web application uniquely identifies and authenticates the client with sufficient strength to withstand common attacks.

2 Access control

Access to functions and sensitive data of the KAS Passwort-Manager by unauthorised persons is prevented.

3 Password management

The customer passwords managed by the KAS Passwort-Manager are encrypted with the MasterKey. The MasterKey is encrypted with the Master Password. The master password is set by the customer and is used to log in to the KAS Portal. If the login to the KAS portal takes place via deep link, the master password is not available and therefore the decryption of the master key is not possible. The master password is not stored permanently, but is only used during login for authentication and decryption of the MasterKey.

4 Transport encryption

All security features derived for the purpose of authentication are encrypted during the session management between the customer's web browser and the web frontend of the KAS Passwort-Manager in accordance with the recommended algorithms of BSI TR-02102-2 using TLSv1.2 (or higher).

Summary of the evaluation requirements for the Security Qualification (SQ), version 10.0

1 Technical Security Requirements

The technical security requirements must be documented, consistent and verifiable. The specification must be made in accordance with ISO / IEC 17007. In addition, technical security requirements must be derived in the framework of an individual threat and risk analysis, they must be derived from previously defined protection profiles, or they must conform to published security requirements of recognized authorities or bodies of IT security. Furthermore, they must be appropriate to the intended use of the IT product and meet applicable security demands.

2 Architecture and Design

The IT system must be structured reasonably and understandable. Its complexity must not have any impact on security. The hardening and protection measures must be adequate and effective. It must not contain any conceptual vulnerability that allows bypassing or disabling security-relevant components.

3 Operating Instructions (as of SEAL-4)

The existing control measures must be effective. The monitored events must be able to identify security incidents promptly and reliably. Administration is performed through a trusted path/channel for confidentiality and integrity. The documentation must be clear and understandable. The documentation must be known to authorized person and always be readily accessible.

4 Vulnerability Assessment and Penetration Testing

The security measures of the IT system must withstand penetration testing. It must not be possible to break or circumvent security measures. The IT system must be configured securely, must meet all of the defined technical security requirements and must not have any exploitable vulnerabilities.

5 Change Management (as of SEAL-5)

Patch management must be completely documented and suitable for the IT system. The procedure for amendments of the IT system must be clearly defined and appropriate for the IT system. Persons involved must be familiar with it and responsibilities must be clearly defined. Amendments of the IT system must not lead to a reduction of the security level achieved.

Security Assurance Level

The following table shows the applicable criteria for the security assurance level. A certificate can be issued for IT systems having successfully passed the evaluation and reaching an overall level of at least SEAL-3.

		Security Assurance Level				
		SEAL-1	SEAL-2	SEAL-3	SEAL-4	SEAL-5
Evaluation Criteria	Technical Security Requirements	X	X	X	X	X
	Architecture and Design			X	X	X
	Operating Instructions				X	X
	Vulnerability Assessment and Penetration Testing		X	X	X	X
	Change Management					X

Table: Evaluation Criteria and Security Assurance Level of IT systems