Certificate

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

HID Global GmbH
611 Center Ridge Drive
Austin TX 78753, USA

to confirm that its IT product

Physical Access Control Credential, Seos, FW releases 1.1.27 & 1.1.28

fulfils all requirements of the criteria

Security Qualification (SQ), Version 10.0
Security Assurance Level SEAL-5

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

The appendix is part of the certificate and consists of 5 pages.

The certificate is valid only in conjunction with the evaluation report.

Security TÜViT® 2022 Trusted Product

Certificate ID: 6145.22

Certificate validity:
2022-09-19 – 2024-07-17

Essen, 2022-09-19

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Am TÜV 1
45307 Essen, Germany
www.tuvit.de

TO CERTIFICATE

Certification Scheme

The certification body of TÜV Informationstechnik GmbH performs its certification on the basis of 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

- "Evaluation Report Security Qualification Trusted Product Security Evaluation Scheme, Physical Access Control Credential, Seos, FW releases 1.1.27 & 1.1.28", version 2, Revision A as of 2022-08-18, TÜV Informationstechnik GmbH

Evaluation Requirements

- "Trusted Site Security / Trusted Product Security, Security Qualification (SQ) Requirements Catalog for version 10.0", document version 2.8 as of 2020-03-16, TÜV Informationstechnik GmbH
- product-specific security requirements (see below)

The Evaluation Requirements are summarized at the end.

Evaluation Target

The target of evaluation is the IT product "Physical Access Control Credential, Seos, FW releases 1.1.27 & 1.1.28" of HID Global GmbH. The IT product is an access control credential with a security controller (secure element) with Seos core operating system. The Seos core operating system allows read and write access to data based on strong authentication. The IT product is

targeted to be embedded in an access control systems. It is detailed in the evaluation report.

Evaluation Result

- All applicable evaluation requirements for the security qualification with Security Assurance Level SEAL-5 are fulfilled.
- The product-specific security requirements are fulfilled.

Product-specific security requirements

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

1 Identification & Authentication

The IT product must enforce a unique identification and authentication of its users. In addition, the IT product must identify and authenticate itself to the user.

2 Trusted Path

To protect the integrity and confidentiality of transmitted data, the IT product must establish a trusted path between itself and the authorized user.

3 Access Control

The IT product must implement measures to ensure that only authorized users have access to their memory (read, modify, add, or remove data).

4 Generation of Random Numbers

The IT product must support the generation of random numbers that are suitable for the usage in cryptographic algorithms.

5 Attack Resistance

The IT product must be resistant against known attacks on smart cards. This also covers the implementation of cryptographically strong algorithms as well as measures against physical and logical attacks.

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

3 Development Process

Development of the IT product must follow a defined development life cycle taking into account at least the phases

of planning, analysis, design, implementation, testing, deployment and maintenance. The maintenance phase of the development life cycle must consider and eliminate vulnerabilities that allow bypassing or disabling security-relevant components. As part of the testing phase of the development life cycle tests with respect to security functionality of the IT product must be considered.

4 Operating Instructions (as of SEAL-4)

The documentation consisting of security requirements for the operating environment of the product, manuals for installation and administration as well as manuals for the end user must be clearly understandable and comprehensible. The documentation must be known to authorized person and always be readily accessible.

5 Vulnerability Assessment and Penetration Testing

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

6 Source Code Analysis (as of SEAL-4)

The source code must not contain vulnerabilities, errors or inconsistencies, such as e. g. undocumented commands, parameters and test functions.

7 Change Management (as of SEAL-5)

Patch management must be completely documented and suitable for the IT product. The procedure for amendments of the IT product must be clearly defined and appropriate for the

IT product. Persons involved must be familiar with it and responsibilities must be clearly defined. Amendments of the IT product 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 products having successfully passed the evaluation and reaching an overall level of at least SEAL-3.

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

Table: Evaluation Criteria and Security Assurance Level of IT products