Zertifikat

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

thyssenkrupp Elevator Innovation GmbH
Thyssenkrupp Allee 1
45143 Essen, Germany

to confirm that its IT product

MaxBox HV02.00

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 this certificate.

The appendix is part of the certificate and consists of 6 pages.

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

Security TÜViT® 2019 Trusted Product

Certificate ID: 6135.19

Certificate valid until 2021-04-30

Essen, 2019-04-10

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH
Member of TÜV NORD GROUP
Langemarckstr. 20
45141 Essen, Germany
www.tuvit.de

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 1.0 as of 2015-08-24, TÜV Informationstechnik GmbH

Evaluation Report

- "Evaluation Report Security Qualification MaxBox HV02.00 of thyssenkrupp Elevator Innovation GmbH", version 1.0 as of 2019-03-26, TÜV Informationstechnik GmbH.

Evaluation Requirements

- "Security Qualification (SQ) from TÜV Informationstechnik GmbH", version 10.0 as of 2011-03-21, TÜV Informationstechnik GmbH, see current Requirement Catalog: Trusted Site Security/Trusted Product Security, Security Qualification (SQ) Requirements Catalog for version 10.0, documentation version 2.7 as of 2019-01-07, 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 MaxBox HV02.00 of thyssenkrupp Elevator Innovation GmbH. It is detailed in the evaluation report.

Evaluation Result

- All applicable evaluation requirements for the security qualification with Security Assurance Level SEAL-3 are fulfilled.
- The product-specific security requirements are fulfilled.

The MaxBox must be installed and operated in a secure operating environment that provides physical access protection. The requirements for a secure operating environment are defined by the manufacturer in the operating instructions MAX (version 04/2017 as of 2017-04-13, thyssenkrupp Elevator AG) as well as in MAX-Security Concept (version 14 as of 2019-02-27, thyssenkrupp Elevator AG).

The notes and recommendations of the evaluation report have to be regarded.

Product-specific security requirements

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

1 Authentication

The MaxBox uses secure authentication techniques, which distinctly identify the communication participants. Services provided by the MaxBox can only be used after successful authentication.

2 Trustworthy Path

The communication between the MaxBox and the backend services is established over a trustworthy path, which ensures the integrity and the confidentiality of the transferred data.

3 Access Control

The data, services and functions of the MaxBox are protected from unauthorized access over the network interface and mobile network in orderly commissioned state.

4 Change Management

The MaxBox-Update mechanism only accepts authentic and trustworthy software updates from the manufacturer.

5 System Hardening

The MaxBox provides only network services that are required for the destined operation.

6 Logging

The MaxBox logs security relevant events.

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