TÜVIT

Certificate

TÜVIT
TÜV NORD GROUP
Security
Trusted Product
2024
tuvit.de ID: 6148.24

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

symmedia GmbH
Turnerstraße 27
33602 Bielefeld, Germany

Certificate validity:
2024-01-18 – 2026-01-18

to confirm that its remote service portal software

symmedia SP/1, Version 12

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 6148.24 and consists of 5 pages.

Essen, 2024-01-18

Dr. Christoph Sutter, Head of Certification Body

To Certificate

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

TÜV®

TÜVNORDGROUP

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, symmedia SP/1, Version 12”, Version 1.0 as of 2024-01-12, 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
- Product-specific security requirements (see below)

The evaluation requirements are summarized at the end.

Evaluation target

Evaluation target is the remote service portal software “symmedia SP/1, Version 12” of symmedia GmbH. 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 product-specific security requirements are fulfilled.

The 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 Identification & Authentication

The IT product must identify and authenticate the user uniquely. The authentication data must be strong enough to resist sufficiently long against current attacks. The IT product must detect faked authentication data and must prevent their unauthorised use. This is valid for the following relations:

Users and systems:

- Operator to site control server,
- Service technician to site control server,
- Service technician to central server.

Systems and systems:

- Site control server to central server.

2 Access Control

The IT product must provide functionalities that allow restricting users' access privileges. A user must not be able to extend his access privilege with reasonable effort.

3 Encrypted communication channel/path

Communication via insecure networks must be performed via a trustworthy channel/path that ensures the confidentiality of the transmitted data. This is valid for the communication between

- Central server and site control server,
- Service technician and site control server and
- Service technician and central server.

4 Data Flow Control

The IT product must ensure that only connections needed for operation are possible. This is valid for the connections between

- Site control server and central server and
- Service technician and central server.

5 Logging

Security-relevant events must be logged. The Prologging (a log procedure that provides log entries with hashes) makes the manipulation of the log entries more difficult in comparison to the standard log procedure.

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

1 Technical Security Requirements (as of SEAL-1)

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 (as of SEAL-3)

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 (as of SEAL-3)

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 (as of SEAL-2)

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 evaluation 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				
		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
	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 product