TÜVIT

Certificate

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

Telekom Deutschland GmbH
Landgrabenweg 151
53227 Bonn, Germany

Certificate validity:
2022-11-25 – 2024-11-25

to confirm that its IT system

Customer centre

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 9560.22 and consists of 4 pages.

Essen, 2022-11-25

Dr. Christoph Sutter, Head of Certification Body

To Certificate

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

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, Customer centre”, version 1.1 as of 2022-11-02, 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
- System-specific security requirements (see below)

The Evaluation Requirements are summarized at the end.

Evaluation target

The evaluation target is the IT system “Customer centre” of Telekom Deutschland 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 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 Customer Centre uniquely identifies and authenticates end users with sufficient strength to withstand common attacks.

2 Access control and session management

Data, services and functions that require protection are protected from unauthorised access by the Customer Centre.

Session data used by the Customer Centre is securely generated, managed and deleted to ensure confidentiality.

3 Data security and transport security

No confidential information is disclosed by the Customer Centre via the internal network structure.

Communication as well as access to the Customer Centre takes place via secure connections, which protect the integrity and confidentiality of the transmitted data according to the current state of the art (BSI TR-02102-2).

The access data are securely stored by the Customer Centre so that their confidentiality and integrity are guaranteed.

4 Privacy by Design and Privacy by Default

The Customer Centre only stores personal data that is necessary for the processes of the end customers. Personal data that is no longer required is deleted.

The processing of personal data is carried out in a fair and transparent manner for the data subject with data protection-friendly default settings based on an understandable as well as comprehensible information basis about the data processing.

5 System hardening

The components and interfaces accessible from the Internet have no know Authentication & Access Control

6 Logging

Within the scope of logging, security-relevant events are recorded and evaluated.

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 system 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