Certificate

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

Ärzteversorgung Westfalen-Lippe
Scharnhorststraße 44
48151 Münster, Germany

to confirm that its IT System

MiPor

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 and consists of 5 pages.

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

Security TÜViT® 2019 Trusted Site

Certificate ID: 9559.19

Zertifikat gültig bis 2021-07-02

Essen, 2019-07-02

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

- German document: “Sicherheitstechnische Qualifizierung MiPor”, version 1.2 as of 2019-06-17, 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
- system-specific security requirements (see below)

The Evaluation Requirements are summarized at the end.

Evaluation Target

The target of evaluation is the Internet portal solution “Mitglieder-Portal” (MiPor) of “Ärzteversorgung Westfalen-Lippe”. MiPor offers its registered customers to view and alter their saved personal data. Further information regarding the target of evaluation 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 Authentication & Access Control

- Data, services and functions are protected against unautorized access.
- Access data is processed and saved by the web application in a secure way to ensure the confidentiality and integrity of access data.

2 Session Management

- Session information is generated, used and deleted by the web application in a secure way to ensure the confidentiality and integrity of session data.
- Session information is processed by the web application in a confidential way.

3 Validation of Input/Output Data

- Before processing input and output data are validated by the web application to prevent processing and providing of malicious data. All used data (e. g. forwarded to browser or database) will be checked by the web application.

- Validation of input and output data is processed server-sided.

4 Data Security

- Confidential information of internal structures is not disclosed by the web application.
- Transmission of confidential data as well as access to the web application is processed by using secure connections to ensure the confidentiality and integrity.
- Caching of confidential data is avoided.
- Confidential data (e. g. access information) is saved encrypted. Used crypto algorithms are in accordance with the state of the art.

5 Application Logic

- Only operational necessary functions are provided by the web application. They cannot be used abusively (e. g. for code exploitation).

6 System Hardening

- Components and server processes reachable from the Internet have no known exploitable vulnerabilities.

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 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 / 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
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