Certificate

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

Agfa HealthCare GmbH
Konrad-Zuse-Platz 1 - 3
53227 Bonn, Germany

to confirm that its IT system

IMPAX/web.Access

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® 2018 Trusted Site

Certificate ID: 9557.18

Zertifikat gültig bis 30.09.2020

Essen, 2018-09-24

Dr. Christoph Sutter
Head of Certification Body

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

Certification System

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

- 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 IMPAX/web.Access der Agfa HealthCare GmbH", version 1.0 as of 2018-09-06, TÜV Informationstechnik GmbH.

Evaluation Requirements

- German document: "Sicherheitstechnische Qualifizierung (SQ) der TÜV Informationstechnik GmbH", version 10.0 as of 2018-01-15, TÜV Informationstechnik GmbH
- System-specific Security Requirements (see below)

The Evaluation Requirements are listed at the end.

Evaluation Target

- The target of evaluation is the IT system "IMPAX/-web.Access" of Agfa HealthCare 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 were the basis of the certification and have been checked.

1 Authentication and Access Control

- The web application protects data, services, and functions with restricted access effectively against unauthorized access.
- The data is changed, processed and stored by the web application in a secure manner, that confidentiality and integrity of the data are protected.

2 Management of User Sessions (Session Management)

- The session information used by the web application is generated, managed and deleted in a secure manner, that confidentiality and integrity of the session data are protected.
- The session information is confidentially treated by the web application.

3 Validation of Input and Output Data

- All input and output data are validated before being processed by the web application, so that no malicious data is processed and displayed by the web application. In this process the data from and to all system components (e. g. browser or database) are examined by the web application.

- Validation of all input and output data is implemented on the server side.

4 Data Security

- No confidential information about the internal structure of the application will be revealed by the web application.
- The transfer of trusted data and the access to the web application is carried out via secure connections.
- The temporary storage of sensitive data is avoided.
- Confidential data (e. g. login data) is stored encrypted by using algorithms that are state-of-the-art.

5 Application Logic

- The web application offers only operationally necessary functions. The functions offered by the web application can't be misused (e. g. breaking out of a defined sequence).

6 System Hardening

- The server components and processes accessible 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 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 / 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 for IT systems