Certificate

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

Deutsche Telekom AG
Products & Innovation
T-Online-Allee 1
64295 Darmstadt, Germany

to confirm that its IT system

Developer Garden App Monitor

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 until 2015-10-31.

Security SQ9545.13
TÜViT®
2013 Trusted Site
Voluntary Validation
© TÜViT - Member of TÜV NORD GROUP

15
Certificate-Registration-No.:
TUVIT-SQ9545.13

Essen, 2013-10-17

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 product certification system:

- German document: ”Zertifizierungsschema für TÜViT Trusted-Zertifikate der Zertifizierungsstelle TÜV Informationstechnik GmbH“, version 1.0 as of 2010-05-18, TÜV Informationstechnik GmbH

Evaluation Report

- German document: ”Sicherheitstechnische Qualifizierung Developer Garden App Monitor der Deutsche Telekom AG“, version 1.1 as of 2013-10-07, TÜV Informationstechnik GmbH.

Evaluation Requirements

- German document: ”Sicherheitstechnische Qualifizierung (SQ)® der TÜV Informationstechnik GmbH“, version 10.0 as of 2011-03-21, 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 “Developer Garden App Monitor” of Deutsche Telekom AG. 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 Trustworthy Path

- The transfer of the collected data by the IT system and the access to the web interface to retrieve the data (dashboard) is performed via trustworthy paths which protect the integrity and confidentiality of the transmitted data.
- The administration of the server in the back-end is done by authorized persons and is performed over trustworthy paths which protect the integrity and confidentiality of the transmitted data.

2 Authentication and Access Control

- The web interface to retrieve the data (dashboard) is protected against unauthenticated access.
- The web interface to retrieve the data (dashboard) protects the prepared and aggregated data of the IT system against unauthorized access.
- The access to collected unprepared data of the IT system (raw data) is neither possible via the Web interface to retrieve the data (dashboard) nor via the web service.
- The components in the back-end have no known exploitable vulnerabilities.

3 Data Flow Control

- The systems in the back-end are protected by a multi-tier firewall installation against attacks from the Internet.
- The network separation in the back-end does not allow a direct connection from insecure networks into the protected network and vice versa.
- The firewall installation of the back-end allows only the mandatory connection links to operate the system.
- Both the web service to record the data and the web interface to retrieve the data (dashboard) validate the input data set and implement the character encoding. The web service processes exclusively only the defined data.

4 Logging

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

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