Certificate

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

innogy SE
Flamingoweg 1
44139 Dortmund, Germany

to confirm that its IT System

innogy eOperate (software solutions for electromobility)

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 6 pages.

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

Security
TÜViT®
2017
Trusted Site
Certificate ID: 9553.17
© TÜViT – TÜV NORD GROUP – www.tuvit.de

18
Zertifikat gültig bis
30.11.2018

Essen, 2017-04-04

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 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, innogy eOperate (Softwarelösungen für Elektromobilität) der innogy SE", version 1.2 as of 2017-04-04, 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 "innogy eOperate (software solutions for electromobility)" of innogy SE.

This target consists of the following components:

- 3 from the Internet accessible web portals,
- 10 from the Internet accessible web services,
- 8 internal back end systems,
- 2 security gateways

and following components that are not part of the certification:

- Physical infrastructure (charging stations, infrastructure providers and service providers),
- Technical infrastructure (business partners, service providers and their end customers).

The detailed descriptions are documented 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 and Access Control

The IT System uniquely identifies and authenticates internal and external communication partners (e. g. e-mobility charging stations, VPN termination units of external partners) sufficiently strong to withstand common attacks.

Sensitive data services and functions are protected by the IT System effectively against unauthorized access.

2 Management of clients and User Sessions (Session Management)

The IT System enables effective separation of client-specific data. The functions offered can not be misused, a client can not access data from other clients.

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

3 Validation of Input and Output Data

All input and output data of the external components connected via the Internet are validated before processing, so that no malicious data are processed and output. The validation of all input and output data is implemented on the server side.

4 Data Security

The transmission of sensitive data over insecure networks (e. g. the Internet) is done via secure connections, which ensure the integrity and confidentiality of the transmitted data.

5 Data Flow Control

The IT System ensures that only operationally necessary connections from untrusted networks (e. g. Internet) are possible.

6 System Hardening

The server components and server processes of the IT system 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