Certificate

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

RWE Effizienz GmbH
Freistuhl 7
44137 Dortmund, Germany

to confirm that its firewall and server installation

SmartHome Backend and Webservices

fulfil all requirements of the criteria

Security Qualification (SQ), Version 9.0

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 until 2013-03-31.

Security SQ9540.11 TÜViT® 2011 Trusted Site
Voluntary Validation

Certificate-Registration-No.:
TUVIT-SQ9540.11

Essen, 2011-05-13

Joachim Faulhaber
Deputy Head of Certification Body

TÜV Informationstechnik GmbH
Member of TÜV NORD Group
Langemarckstr. 20
45141 Essen, Germany
www.certuvit.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 Informations-technik GmbH“, version 1.0 as of 2010-05-18, TÜViT GmbH

Evaluation report

- German document: “Auflagenprüfung SmartHome Backend und Webservices“, version 1.1 vom 2011-04-07, TÜViT GmbH
- German document: “Sicherheitstechnische Qualifizierung (SQ)® SmartHome Backend und Webservices“, Version 1.1 vom 02.03.2011, TÜViT GmbH

Evaluation requirements

- German document: “Sicherheitstechnische Qualifizierung (SQ)® der TÜV Informationstechnik GmbH“, version 9.0 as of 2006-10-01, TÜViT GmbH
- System-specific security requirements (see below)

Evaluation Target

The target of the evaluation is the firewall and server installation "SmartHome Backend and Webservices“ of RWE Effizienz GmbH, which is described in detail in the evaluation report.

The "SmartHome Backend and Webservices" target of evaluation forms part of the SmartHome solution of RWE Effizienz GmbH.

- Smarthome Backend and Webservices: The backend contains the services and webservices which are needed to support operation of the SmartHome solution. These include registration of the Smart Home Controller (SHC),

assignment of the SHC to users, storage of the profiles entered into the system, device management and software updates.

The solution consists of the following three further main components, which are however not included in the scope of the certification:

- SmartHome Controller: the SHC directly controls the devices connected to it. The devices can also be controlled via rules and profiles which are stored in the SHC.
- SmartHome Devices: In the current development stage, the devices consist of the actuators for the radiator thermostat and the adapter plug and of the wall transmitter sensor. The actuators can be controlled either through establishment of a time profile or through direct user enquiry via a control/configuration node. It is also possible for sensors and actuators to be directly connected.
- Control and Configuration Node: The Control and Configuration Node is the central user interface which can be employed by the final user to set and adjust the SmartHome solution according to his or her own requirements. Using this interface, (Silverlight application or web-based client) the SHC can be controlled both via the local network and via remote control/configuration nodes and mobile devices.

Evaluation Result

- The applicable evaluation requirements for Security Qualification are fulfilled.
- The system-specific security requirements are fulfilled.

System-specific security requirements

The certification is based on the following system-specific security requirements that have been checked in the evaluation.

1 Trusted path

- The communication between the control and configuration node and the servers in the backend is by means of trusted paths, which protect the integrity and confidentiality of the data which are transferred.
- The servers in the backend are administered by persons authorised by RWE and the administration is via trusted paths which protect the integrity and confidentiality of the data which are transferred.

2 Authentication

- The backend makes use of authentication procedures that protect the connection between the SHC and the backend.
- Incorrect authentication attempts are rejected.

3 Access control

- Configuration and profile data that are stored in the backend are protected against unauthorised access.
- The switching and configuration procedures are protected against manipulation during use of the web services of the backend.
- The components in the backend do not exhibit any known exploitable vulnerabilities.

4 Data flow control

- The systems in the backend are protected against attacks from the Internet by means of a multi-stage firewall installation.

- The network separation in the backend does not allow a direct link from the non-secure network into the network to be protected and vice versa.
- The firewall installation of the backend only permits the communication links that are necessary for operation.
- The internal structure of the backend is concealed.

5 Logging

- Security-related events at the firewall components of the backend are stored on a central logging server and are regularly analysed.
- The system state of the components in the backend is monitored with regard to processes, capacities and load.
- Special configurable log messages of individual system components lead to immediate warning of the system responsibles.

Summary of the requirements for the Security Qualification (SQ), version 9.0

1 Technical security requirements

Technical security requirements are defined based on recognized criteria, specifications or standards. The technical security requirements are free of internal contradictions and satisfy accepted security requirements.

2 Documentation of the architecture

For the qualification of the IT product and its application environment or of the IT system, appropriate descriptions of all necessary components are available. From these, the

mutual utilization relationships and data flows as well as the fulfillment of security requirements can be recognized.

3 User, administration and other operational documents

Suitable manuals for installation, administration and usage are available. These particularly include notes on configuration of necessary system and product components as well as environmental measures and personnel responsibilities which satisfy the security requirements.

4 Security of the components used

All sub-components that implement security functionalities could be classified as trustworthy based on previously performed formal evaluations and/or publicly accessible information.

5 Means of system management

Suitable configuration facilities as well as appropriate monitoring and logging guarantee the secure operational state. Tools used for system management are subject to the same security requirements as the IT product/IT system itself.

6 Tests and inspections

Comprehensive penetration testing and technical vulnerability analyses have been performed during testing. The vulnerabilities determined during testing and analyses have been rated according to their risk potential.

7 Change management

A concept for the planning and implementation of new configurations and the import of updates exists in order to adequately evaluate risks and their effects as well as to guarantee maintenance of the intended protective level. The

concept describes the way in which changes may take place and how the documentation is adapted where necessary.

8 IT systems: operational environment

Suitable operational conditions exist. The personnel responsibilities and environmental conditions satisfy the security claim of the IT system.

9 Security analyses

In a final analysis documented in the evaluation report the results of the previously listed evaluation aspects are compared to the security requirements. The result is that all security requirements have been met and the resulting residual risks are bearable.