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 home automation product

SmartHome Controller, Version 1.0

fulfils 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 5 pages.

The certificate is valid only in conjunction with the evaluation report until 2013-03-31.

Security PQ6118.11 TÜViT® 2011 Trusted Product

Voluntary Validation

Certificate-Registration-No.:
TUVIT-PQ6118.11

13

Essen, 2011-03-10

Dr. Christoph Sutter
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: “RWE SmartHome Controller“, version 1.2 as of 2011-02-24, TÜViT GmbH.

Evaluation requirements

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

Evaluation Target

The target of evaluation is the home automation product SmartHome Controller Version 1.0 of the company RWE Effizienz GmbH consisting of software and related hardware. The SmartHome Controller (SHC) directly controls the connected actuators radiator thermostat and adapter plug, as well as the wall transmitter sensor, directly by radio signal. Furthermore, the actuators and sensors can be controlled via rules and profiles which are stored in the SHC.

The configuration of the SHC and the manual control takes place via the software Control/Configuration Node and can be performed via Internet or via the local network at the SHC. The SHC may be updated with software updates.

The verified security characteristics are listed in the chapter "Product-specific security requirements".

Evaluation Result

- All applicable evaluation requirements for the security qualification are fulfilled.
- Product-specific security requirements are fulfilled.
- Requirements and recommendations given in the evaluation report must be applied.

Product-specific security requirements

The following product-specific security requirements are the basis of the certification and have been verified:

1 Trusted path

- The SHC is put into operation via a trusted path which protects the integrity and confidentiality of the data which are transferred.
- The communication between local control/configuration node and the SHC in the local network is implemented via a trusted path, which protects the integrity and confidentiality of the data which are transferred.
- The communication between the SHC and the sensors and actuators is implemented via a trusted path, which protect the integrity and confidentiality of the data which are transferred.

2 Authentication

- The SHC makes use of authentication procedures that secure the connection between SHC and the backend as well as connections from the local network.

3 Access control

- Following successful commissioning of the SHC, the SHC is protected against unauthorised local switching and configuration activities.
- Data that are stored in the SHC are protected against unauthorised access.
- The certificates and keys for authentication and encryption are securely stored and are protected against unauthorised access.
- Triggering of sensors and actuators is protected against unauthorised switching and configuration activities.
- Unauthorised coupling of SHC and sensors or actuators is barred.
- Unauthorised change of a connection of SHC and actuator or sensor is barred.

4 Change management

- Only trustworthy software that has been tested and accepted by RWE is loaded and installed onto the SHC.
- Only trustworthy software that has been tested and accepted by RWE is used and distributed for the Control/Configuration Node.

5 Data flow control

- The SHC and the control/configuration nodes in the local network of the customer only create connections to systems of RWE. The creation of the connection is initiated from the local network of the customer.
- Only the network services which are necessary for operation are available on the SHC.

6 Logging

- Security-relevant events are logged by the SHC.

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.