Certificate

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

Verteilnetzbetreiber (VNB) Rhein-Main-Neckar GmbH & Co. KG
Frankfurter Str. 100
64293 Darmstadt, Germany

to confirm that its IT-System

Querverbundleitstelle Darmstadt

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 6 pages.

The certificate is valid only in conjunction with the evaluation report until 2014-06-30.

Security SQ9544.12 TÜViT® 2012 Trusted Site
Voluntary Validation
© TÜViT - Member of TÜV NORD Group

Certificate-Registration-No.:
TUVIT-SQ9544.12

Essen, 2012-06-11

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 Informationstechnik GmbH“, version 1.0 as of 2010-05-18, TÜViT GmbH

Evaluation Report

- German document: “Querverbundleitstelle Darmstadt des Verteilnetzbetreiber (VNB) Rhein-Main-Neckar GmbH & Co. KG“, version 1.2 as of 2012-06-04, 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 evaluation is the IT system “Querverbundleitstelle (QVL) Darmstadt” of the operator “Verteilnetzbetreiber (VNB) Rhein-Main-Neckar GmbH & Co. KG”. The laterally integrated control centre (“Querverbundleitstelle”) consists of three parts: two control centres in Darmstadt and the systems that are necessary for the connection of the interconnected control centre in Aschaffenburg of Aschaffenburger Versorgungs-GmbH (AVG).

Examined were exclusively the beyond mentioned system-specific security requirements on the basis of the SQ®. Further properties of the IT systems are not target of the certification.

Evaluation Result

- All applicable evaluation requirements for the security qualification (SQ) are fulfilled.
- System-specific security requirements are fulfilled.
- The recommendations of the evaluation report have to be regarded.

System-specific security requirements

The certification is based on the following system-specific security requirements of the document

- "White Paper Requirements for Secure Control and Telecommunication Systems", version 1.0 as of 2008-06-10, Bundesverband der Energie- und Wasserwirtschaft e. V.

that have been checked in the evaluation.

1 General Requirement and Housekeeping

The area General Requirement and Housekeeping is divided into sub-area General with the sub-items:

- Secure System Architecture
- Contact Person
- Patching and Patch Management
- Provision of Security Patches for all System Components
- Third Party Support
- Encryption of Sensitive Data during Storage and Transmission
- Cryptographic standards

- Internal and External Software and Security Tests and related Documentation
- Secure Standard Configuration, Installation and Start-Up
- Integrity Checks

and the sub-area Documentation with the sub-items:

- Design Documentation, Specification of Security Relevant System Components and Implementation Characteristics
- Administrator and User Documentation
- Documentation of Security Parameters and Security Log Events or Warnings
- Documentation of Requirements and Assumptions needed for Secure System Operation

2 Base System

The area Base System is divided into the sub-areas:

- System Hardening
- Anti Virus Software
- Autonomous User Authentication

3 Network / Communication

The area Network / Communication is divided into the sub-area Secure Network Design and Communication Standards with the sub-items:

- Deployed Communication Technologies and Network Protocols
- Secure Network Design
- Documentation of Network Design and Configuration

and the sub-area Secure Maintenance Processes and Remote Access with the sub-items:

- Secure Remote Access
- Maintenance Processes
- Wireless Technologies: Assessment and Security Requirements

4 Backup, Recovery and Disaster Recovery

The area Backup, Recovery and Disaster Recovery is divided into the sub-areas:

- Backup: Concept, Method, Documentation, Test
- Disaster Recovery

The additional security requirements of areas "Application" and "Development, Testing and Rollout" contained in the White Paper are not relevant for system testing. They are not part of the certification.

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.