Certificate

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

e-netz Südhessen GmbH & Co. KG
Dornheimer Weg 24
64293 Darmstadt, Germany

to confirm that its IT system

Querverbundleitstelle Darmstadt

fulfils all requirements of the criteria

Security Qualification (SQ), Version 10.0
Security Assurance Level SEAL-5

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 2016-06-30.

Security SQ9550.14 TÜViT® 2014 Trusted Site

Voluntary Validation

Certificate-Registration-No.:
TUVIT-SQ9550.14

Essen, 2014-07-17

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: "Querverbundleitstelle Darmstadt der e-netz Südhessen GmbH & Co. KG", version 1.2 as of 2014-07-10, 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 "Querverbundleitstelle (QVL) Darmstadt" of the operator "e-netz Südhessen 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) with Security Assurance Level SEAL-5 of IT systems 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 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