Certificate

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

SLA Software Logistik Artland GmbH
Friedrichstraße 30
49610 Quakenbrück, Germany

to confirm that its IT system

Meat Integrity Solution (MIS)

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 2017-02-28.

Security SQ9546.15 TÜViT® 2015 Trusted Site

Voluntary Validation

© TÜViT - Member of TÜV NORD GROUP

Certificate-Registration-No.:
TUVIT-SQ9546.15

Essen, 2015-02-25

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: "Sicherheitstechnische Qualifizierung Meat Integrity Solution (MIS) der SLA Software Logistik Artland GmbH", version 1.2 as of 2015-01-30, 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 "Meat Integrity Solution (MIS)" of SLA Software Logistik Artland GmbH. SLA sells the IT system for acquisition and processing of measurement data collected in slaughterhouse under the meat processing. The measurement data are signed, stored, processed by a web portal and made available. The evaluation report contains a detailed description of the IT system.

Evaluation Result

- All applicable evaluation requirements for the security qualification with Security Assurance Level SEAL-5 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 Trusted path

- The communication between the SLA MIS Connector and connected components is protected by trusted paths that ensure the integrity and confidentiality of the data.
- The communication between the SLA MIS Connector and the MIS database is protected by trusted paths that ensure the integrity and confidentiality of the data.
- Communication between the MIS system and the central MIS platform is protected by trusted paths that ensure the integrity and confidentiality of the data.
- At the date of investigation, system components of the web application accessible from the internet do not contain any know exploitable vulnerabilities.
- Administrative activities are protected by trusted paths that ensure the integrity and confidentiality of the data.

2 Authentication

- To protect the connections within the MIS system only secure authentication methods are used.

- The web application uses secure authentication features.
- The authentication features are checked during authentication by the web application in a secure manner.

3 Access control

- After successful commissioning, the MIS system is protected against unauthorized local switching and configuration operations.
- Data stored within the MIS system is protected against unauthorized access and changes.
- The certificates and keys for authentication and encryption are stored securely and protected against unauthorized access.
- Unauthorized coupling of components to the SLA MIS Connector is prevented.
- Unauthorized modification of existing mappings between components and the SLA MIS Connector is prevented.
- Session management implemented / used within the web application is suitable to separate user sessions securely.
- Effective access controls are implemented to prevent unauthorized access to URL, business functions, data, services, and files.
- The security configuration of the web application is protected against unauthorized changes.

4 Change management

- Fully tested and approved software is loaded and installed on the MIS system by the SLA exclusively.

5 Data flow control

- The MIS system established only connections to the slaughterhouse IT system or the central MIS platform.

- Within the MIS system, only the operationally necessary network services are available.
- Unauthorized access to the MIS database is prevented by appropriate measures.
- Communication with the web application is established via trusted paths.
- The web application processes only defined data.
- The web application is protected by a firewall installation and allows only communication links mandatory for operation.

6 Logging

- Security incidents within the MIS system are recorded and assessed.
- The error handling and logging functionality of the web application are suitable to identify security incidents (e. g. attempted attacks).
- No confidential information about error handling is revealed to unauthorized persons.
- A logging concept for operating systems and server processes is implemented for collection and assessment of security incidents.

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