TÜVNORD

Certificate

TÜVNORD
TÜV NORD CERT GmbH
Security
Trusted Site
tuev-nord.de ID: 9562.25

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

Certificate validity:
2025-02-25 –
2027-02-25

DTVP Deutsches Vergabeportal GmbH
Unter den Linden 24
10117 Berlin

to confirm that its IT system

DTVP Deutsches Vergabeportal
(VMP-Satellit, VMP-Zentrale) Version 9.6

fulfils all requirements of the criteria

Security Qualification (SQ)
Version 10.0
Security Assurance Level SEAL-4

of TÜV NORD CERT GmbH. The requirements are summarized in the appendix to the certificate.

The appendix is part of the certificate with the ID 9562.25 and consists of 4 pages.

Essen, 2025-02-25

Zertifizierungsstelle der TÜV NORD CERT GmbH

To Certificate

TÜV NORD CERT GmbH
Am TÜV 1, 45307 Essen, Germany
tuev-nord-cert.de

TÜV®

Certification scheme

The certification body of TÜV NORD CERT GmbH performs its certifications based on the following certification scheme:

- German document: „Zertifizierungssystem für IT-Zertifikate (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV NORD CERT GmbH“, D503-CP-001, Rev. 00/09.24, TÜV NORD CERT GmbH

Evaluation report

- German document: “Evaluierungsbericht – Sicherheitstechnische Qualifizierung, DTVP Deutsches Vergabeportal (VMP-Satellit, VMP-Zentrale) Version 9.6”, 1.1 as of 2025-01-29, TÜV Informationstechnik GmbH

Evaluation requirements

- “Trusted Site Security / Trusted Product Security, Security Qualification (SQ) Requirements Catalog for version 10.0”, documentation version 2.9 as of 2022-11-11, TÜV Informationstechnik GmbH
- Product-specific security requirements (see below)

The evaluation requirements are summarized at the end.

Evaluation target

Evaluation target is the “DTVP Deutsches Vergabeportal (VMP-Satellit, VMP-Zentrale) Version 9.6” of DTVP Deutsches Vergabeportal GmbH. It is detailed in the evaluation report.

Evaluation result

- All applicable evaluation requirements for the security qualification with Security Assurance Level SEAL-4 are fulfilled.
- The product-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. Access Control

Data, services and functions of the VMP-Center and VMP-Satellite modules that require protection are defined in the authorisation concept and are protected against unauthorised access.

2. Data Security and Transport Security

Communication and access to the VMP-Satellite and VMP-Center modules takes place via secure connections that protect the integrity and confidentiality of the transmitted data in accordance with the current state of the art (BSI TR-02102-2).

Access credentials are hashed in accordance with the state of the art (BSI TR-02102-1) and therefore not stored in plain text.

Submitted tenders, requests to participate and expressions of interest are stored in encrypted form and can only be decrypted and opened after the tender deadline has expired and the for-eyes login has been carried out.

Access to information on restricted procedures (tender documents, communication messages) is only possible after registration (participation in the procedure).

3. Validation of Input and Output Data

All input and output data is validated by the VMP-Satellite and VMP-Center modules prior to processing in accordance with the state of the art (in accordance with OWASP ASVS version 4). Data from and to all system components (e.g. browser or database) are validated on the server side.

4. Business Logic

The functions offered by the VMP-Satellite and VMP-Center cannot be used to bypass the defined task sequences.

5. System Hardening

The VMP-Satellite and VMP-Center only offer operationally required services at network level. The components and interfaces of the modules accessible from the Internet have no known exploitable vulnerabilities.

6. Logging/Monitoring

Security-relevant traffic events and the utilization of the systems are recorded and evaluated as part of the logging process.

Summary of the evaluation requirements for the Security Qualification (SQ), version 10.0

1 Technical Security Requirements (as of SEAL-1)

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 Vulnerability Assessment and Penetration Testing (as of SEAL-2)

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.

3 Architecture and Design (as of SEAL-3)

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.

4 Installation and Operation (as of SEAL-4)

The existing logging and monitoring measures must be effective. The logged and monitored events must be appropriate for detecting security incidents in a reliable and prompt manner. With respect to confidentiality and integrity, the administration is carried out via a trustworthy path. The documentation must be understandable and transparent. It must be known to the authorized individuals and freely accessible at all times.

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				
		SEAL-1	SEAL-2	SEAL-3	SEAL-4	SEAL-5
Evaluation Criteria	Technical Security Requirements	X	X	X	X	X
	Vulnerability Assessment and Penetration Testing		X	X	X	X
	Architecture and Design			X	X	X
	Operating Instructions				X	X
	Change Management					X

Table: Evaluation criteria and Security Assurance Level of IT system