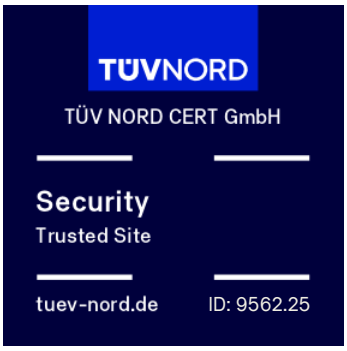
Zertifikat



Die Zertifizierungsstelle der TÜV NORD CERT GmbH
bescheinigt hiermit dem Unternehmen

DTVP Deutsches Vergabeportal GmbH
Unter den Linden 24
10117 Berlin

Zertifikatsgültigkeit:
25.02.2025 – 25.02.2027

für das IT-System

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

die Erfüllung aller Anforderungen der Kriterien

Sicherheitstechnische Qualifizierung (SQ)
Version 10.0
Security Assurance Level SEAL-4

der TÜV NORD CERT GmbH. Die Anforderungen sind in der Anlage zum Zertifikat zusammenfassend aufgelistet.

Die Anlage ist Bestandteil des Zertifikats mit der ID 9562.25 und besteht aus 4 Seiten.

Essen, 25.02.2025

Zertifizierungsstelle der TÜV NORD CERT GmbH

Zum Zertifikat

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

Zertifizierungsprogramm

Die Zertifizierungsstelle der TÜV NORD CERT GmbH führt Zertifizierungen auf Basis des folgenden Zertifizierungsprogramms durch:

- „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

Evaluierungsbericht

- „Evaluierungsbericht – Sicherheitstechnische Qualifizierung, DTVP Deutsches Vergabeportal (VMP-Satellit, VMP-Zentrale) Version 9.6“, 1.1 vom 29.01.2025, TÜV Informationstechnik GmbH

Evaluierungsanforderungen

- „Trusted Site Security / Trusted Product Security, Sicherheitstechnische Qualifizierung (SQ) Anforderungskatalog der Version 10.0“, Dokumentationsversion 2.9 vom 11.11.2022, TÜV Informationstechnik GmbH
- Produktspezifische Sicherheitsanforderungen (siehe unten)

Die Evaluierungsanforderungen sind am Ende zusammenfassend aufgeführt.

Zertifizierungsgegenstand

Zertifizierungsgegenstand ist „DTVP Deutsches Vergabeportal (VMP-Satellit, VMP-Zentrale) Version 9.6“ der DTVP Deutsches Vergabeportal GmbH. Dieser wird im Evaluierungsbericht detailliert beschrieben.

Evaluierungsergebnis

- Die anwendbaren Anforderungen für die Sicherheitstechnische Qualifizierung nach Security Assurance Level SEAL-4 sind erfüllt.
- Die produktspezifischen Sicherheitsanforderungen sind erfüllt.

Die im Evaluierungsbericht genannten Empfehlungen sind zu beachten.

Systemspezifische Sicherheitsanforderungen

Die folgenden systemspezifischen Sicherheitsanforderungen lagen der Zertifizierung zugrunde und wurden überprüft:

1. Zugriffskontrolle

Schützenswerte Daten, Dienste und Funktionen der Module VMP-Zentrale und VMP-Satelliten werden im Berechtigungskonzept definiert und sind vor unbefugten Zugriffen geschützt.

2. Datensicherheit und Transportsicherheit

Die Kommunikation sowie der Zugriff auf die Module VMP-Satelliten sowie VMP-Zentrale erfolgt über gesicherte Verbindungen, welche die Integrität und Vertraulichkeit der übertragenen Daten nach dem aktuellen Stand der Technik (BSI TR-02102-2) schützen.

Zugangsdaten werden gemäß dem Stand der Technik (BSI TR-02102-1) gehasht und damit nicht im Klartext gespeichert.

Abgegebene Angebote, Teilnahmeanträge und Interessensbekundungen werden verschlüsselt gespeichert und können erst nach Ablauf der Angebotsfrist und Durchführung des 4-Augen-Logins entschlüsselt und geöffnet werden.

Der Zugriff auf Informationen zu beschränkten Verfahren (Vergabeunterlagen, Kommunikationsnachrichten) ist nur nach einer Registrierung (Teilnahme am Verfahren) möglich.

3. Validierung von Ein- und Ausgabedaten

Alle Ein- und Ausgabedaten werden von den Modulen VMP-Satelliten und VMP-Zentrale vor der Verarbeitung gemäß dem Stand der Technik (gemäß OWASP ASVS Version 4) validiert. Dabei werden Daten von und zu allen Systemkomponenten (z. B. Browser oder Datenbank) serverseitig validiert.

4. Anwendungslogik

Die angebotenen Funktionen der VMP-Satelliten und VMP-Zentrale können nicht dazu verwendet werden, um die definierten Aufgabenabläufe zu umgehen.

5. Systemhärtung

Die VMP-Satelliten und VMP-Zentrale bieten nur betrieblich erforderliche Dienste auf Netzwerkebene an. Die aus dem Internet erreichbaren Komponenten und Schnittstellen der Module weisen keine bekannten, ausnutzbaren Schwachstellen auf.

6. Protokollierung

Im Rahmen der Protokollierung werden sicherheitsrelevante Traffic-Ereignisse und die Auslastung der Systeme erfasst und ausgewertet.

Zusammenfassung der Evaluierungsanforderungen für die Sicherheitstechnische Qualifizierung (SQ), Version 10.0

1 Technische Sicherheitsanforderungen (ab SEAL-1)

Die technischen Sicherheitsanforderungen müssen dokumentiert, widerspruchsfrei und überprüfbar sein. Die Spezifikation muss in Anlehnung an ISO/IEC 17007 erfolgen. Des Weiteren müssen die technischen Sicherheitsanforderungen im Rahmen einer individuellen Bedrohungs- und Risikoanalyse hergeleitet sein, sie müssen aus bereits definierten Schutzprofilen hergeleitet sein, oder sie müssen konform zu veröffentlichten Sicherheitsanforderungen anerkannter Autoritäten oder Gremien der IT-Sicherheit sein. Weiterhin müssen sie für den Einsatzzweck des IT-Systems angemessen sein und geltenden Sicherheitsansprüchen genügen.

2 Schwachstellenanalyse und Penetrationstests (ab SEAL-2)

Die Sicherheitsmaßnahmen des IT-Systems müssen einer Überprüfung durch Penetrationstests standhalten. Es darf nicht möglich sein, Sicherheitsmaßnahmen zu brechen oder zu umgehen. Das IT-System muss sicher konfiguriert sein, darf keine ausnutzbaren Schwachstellen haben und muss alle definierten technischen Sicherheitsanforderungen erfüllen.

3 Architektur und Design (ab SEAL-3)

Das IT-System muss sinnvoll und verständlich strukturiert sein. Seine Komplexität darf keinen Einfluss auf die Sicherheit haben. Die Härtungs- und Schutzmaßnahmen müssen angemessen und wirkungsvoll sein. Es darf keine konzeptionellen Schwachstellen enthalten, mit deren Hilfe sicherheitsrelevante Komponenten umgangen oder deaktiviert werden können.

4 Installation und Betrieb (ab SEAL-4)

Die vorhandenen Überwachungsmaßnahmen müssen wirkungsvoll sein. Die überwachten Ereignisse müssen geeignet sein, Sicherheitsvorfälle zuverlässig und zeitnah zu erkennen. Die Administration erfolgt über einen vertrauenswürdigen Pfad hinsichtlich Vertraulichkeit und Integrität. Die Dokumentation muss verständlich und nachvollziehbar sein. Sie muss den berechtigten Personen bekannt und jederzeit frei zugänglich sein.

5 Änderungsmanagement (ab SEAL-5)

Das Patch-Management muss dokumentiert und für das IT-System geeignet sein. Das Vorgehen bei Änderungen am IT-System muss klar definiert und geeignet sein. Die beteiligten Personen müssen damit vertraut sein. Verantwortlichkeiten müssen eindeutig geregelt sein. Änderungen dürfen nicht zu einer Reduzierung des erreichten Sicherheitsniveaus führen.

Security Assurance Level

Die folgende Tabelle zeigt die für den Security Assurance Level anwendbaren Evaluierungskriterien für IT-Systeme. Eine Zertifizierung eines IT-Systems ist möglich ab Level SEAL-3.

		Security Assurance Level				
		SEAL-1	SEAL-2	SEAL-3	SEAL-4	SEAL-5
Evaluierungskriterien	Technische Sicherheits-anforderungen	X	X	X	X	X
	Schwachstellenanalyse und Penetrationstests		X	X	X	X
	Architektur und Design			X	X	X
	Installation und Betrieb				X	X
	Änderungsmanagement					X

Tabelle: Evaluierungskriterien und Security Assurance Level für IT-Systeme