

Zertifikat

Die Zertifizierungsstelle der TÜV NORD CERT GmbH
bescheinigt hiermit dem Unternehmen

Ärzteversorgung Westfalen-Lippe
Am Mittelhafen 30
48155 Münster

für das IT-System

ÄVWL-Portal, 1.0

die Erfüllung aller Anforderungen der Kriterien

Sicherheitstechnische Qualifizierung (SQ)
Version 10.0
Security Assurance Level SEAL-3

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

Die Anlage ist Bestandteil des Zertifikats mit der ID 9565.25 und besteht aus 4 Seiten.

Essen, 05.06.2025

Zertifizierungsstelle der TÜV NORD CERT GmbH

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

TÜV®



Zertifikatsgültigkeit:
05.06.2025 – 05.06.2027

Zum Zertifikat



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, ÄVWL-Portal, 1.0“, 1.1 vom 05.06.2025, 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 „ÄVWL-Portal, 1.0“ der Ärzteversorgung Westfalen-Lippe. Dieser wird im Evaluierungsbericht detailliert beschrieben.

Evaluierungsergebnis

- Die anwendbaren Anforderungen für die Sicherheitstechnische Qualifizierung nach Security Assurance Level SEAL-3 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. Authentisierung und Zugriffskontrolle

Schützenswerte Daten, Dienste und Funktionen werden von der Webanwendung wirksam vor unbefugten Zugriffen geschützt.

Die Zugangsdaten werden von der Webanwendung sicher geändert, verarbeitet und gespeichert, so dass die Vertraulichkeit und Integrität der Zugangsdaten geschützt wird.

2. Verwaltung von Benutzersitzungen (Session Management)

Die von der Webanwendung verwendeten Sitzungsinformationen werden sicher generiert, verwaltet und gelöscht, so dass die Vertraulichkeit und Integrität der Sitzungsdaten geschützt wird.

Die Sitzungsinformationen werden von der Webanwendung vertraulich behandelt.

3. Validierung von Ein- und Ausgabedaten

Alle Ein- und Ausgabedaten werden von der Webanwendung vor der Verarbeitung validiert, so dass keine schadhaften Daten von der Webanwendung verarbeitet und ausgegeben werden. Dabei werden Daten von und zu allen Systemkomponenten (z. B. Browser oder Datenbank) von der Webanwendung geprüft.

Die Validierung aller Ein- und Ausgabedaten wird serverseitig umgesetzt.

4. Datensicherheit

Von der Webanwendung werden keine vertraulichen Informationen über die interne Struktur der Anwendung preisgegeben.

Die Übertragung vertrauenswürdiger Daten sowie der Zugriff auf die Webanwendung erfolgt über gesicherte Verbindungen, welche die Integrität und Vertraulichkeit schützen.

Die Zwischenspeicherung sensibler Daten wird vermieden.

Vertrauliche Daten (z. B. Zugangsdaten) werden verschlüsselt gespeichert. Dabei werden Algorithmen verwendet, die dem Stand der Technik (gemäß BSI TR-02102) entsprechen.

5. Anwendungslogik

Die Webanwendung bietet nur betrieblich notwendige Funktionen an. Die angebotenen Funktionen der Webanwendung können nicht missbräuchlich verwendet werden (z. B. Ausbrechen aus einem definierten Ablauf).

6. Systemhärtung

Die vom Internet erreichbaren Komponenten und Serverprozesse weisen keine bekannten, ausnutzbaren Schwachstellen auf.

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 Härtings- 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 Sicherheitsanforderungen	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