

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH
bescheinigt hiermit dem Unternehmen

innogy SE
Flamingoweg 1
44139 Dortmund

für das IT-System

**innogy eOperate (Softwarelösungen
für Elektromobilität)**

die Erfüllung aller Anforderungen der Kriterien

**Sicherheitstechnische Qualifizierung
(SQ)[®], Version 10.0**
Security Assurance Level SEAL-3

der TÜV Informationstechnik GmbH. Die Prüfanforderungen sind in
der Anlage zum Zertifikat zusammenfassend aufgelistet.

Die Anlage ist Bestandteil des Zertifikats und besteht aus 6 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.



Certificate ID: 9553.17

© TÜVIT - TÜV NORD GROUP - www.tuvit.de

18
Zertifikat gültig bis
30.11.2018

Essen, 04.04.2017

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Langemarckstraße 20
45141 Essen
www.tuvit.de

Zertifikat

Zertifizierungssystem

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH führt Zertifizierungen auf Basis des folgenden Produktzertifizierungsprogramms durch:

- „Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 1.0 vom 24.08.2015, TÜV Informationstechnik GmbH

Prüfbericht

- „Sicherheitstechnische Qualifizierung, innogy eOperate (Softwarelösungen für Elektromobilität) der innogy SE“, Version 1.2 vom 04.04.2017, TÜV Informationstechnik GmbH

Prüfanforderungen

- „Sicherheitstechnische Qualifizierung (SQ) der TÜV Informationstechnik GmbH“, Version 10.0 vom 21.03.2011, TÜV Informationstechnik GmbH
- Systemspezifische Sicherheitsanforderungen (siehe unten)

Die Prüfanforderungen sind am Ende zusammenfassend aufgeführt.

Prüfgegenstand

Gegenstand der Prüfung ist das IT-System „innogy eOperate (Softwarelösungen für Elektromobilität)“ der innogy SE.

Der Prüfgegenstand besteht aus folgenden Komponenten:

- 3 aus dem Internet erreichbare Webportale,
- 10 aus dem Internet erreichbare Webservices,
- 8 interne Systeme im Backend,
- 2 Sicherheitsgateways

und folgenden nicht zur Zertifizierung gehörenden Komponenten:

- Physikalische Ladeinfrastruktur (Ladesäulen, Infrastruktur der Betreiber und Serviceprovider),
- Technische Infrastruktur (Geschäftspartner, Serviceprovider und deren Endkunden).

Detaillierte Beschreibungen sind im Prüfbericht dokumentiert.

Prüfergebnis

- Die anwendbaren Anforderungen für die Sicherheitstechnische Qualifizierung nach Security Assurance Level SEAL-3 für IT-Systeme sind erfüllt.
- Der Prüfgegenstand erfüllt die systemspezifischen Sicherheitsanforderungen.

Die im Prüfbericht genannten Empfehlungen sind zu beachten.

Systemspezifische Sicherheitsanforderungen

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

1 Authentifizierung und Zugriffskontrolle

Das IT-System identifiziert und authentifiziert externe und interne Kommunikationspartner (z. B. E-Mobility-Ladesäulen, VPN-Terminierungseinheiten von externen Partnern) eindeutig und hinreichend stark, um gängigen Angriffen standzuhalten.

Schützenswerte Daten, Dienste und Funktionen werden von dem IT-System wirksam vor unbefugten Zugriffen geschützt.

2 Verwaltung von Mandanten und Benutzersitzungen (Session Management)

Das IT-System ermöglicht die effektive Trennung der mandantenspezifischen Daten. Die angebotenen Funktionen können nicht missbräuchlich verwendet werden, ein Mandant kann nicht auf Daten anderer Mandanten zugreifen.

Die von dem IT-System verwendeten Sitzungsinformationen werden sicher generiert, verwaltet und gelöscht, so dass die Vertraulichkeit und die Integrität der Sitzungsdaten gewährleistet wird.

3 Validierungen von Ein- und Ausgabedaten

Alle Ein- und Ausgabedaten der externen über das Internet angeschlossenen Komponenten werden vor der Verarbeitung validiert, so dass keine schadhaften Daten verarbeitet und ausgegeben werden. Dabei wird die Validierung aller Ein- und Ausgabedaten serverseitig umgesetzt.

4 Datensicherheit

Die Übertragung schützenswerter Daten über unsichere Netze (z. B. Internet) erfolgt über gesicherte Verbindungen, welche die Integrität und die Vertraulichkeit der übertragenen Daten sicherstellt.

5 Datenflusskontrolle

Das IT-System stellt sicher, dass nur betrieblich notwendige Verbindungen aus unsicheren Netzen (z. B. Internet) möglich sind.

6 Systemhärtung

Die vom Internet erreichbaren Systemkomponenten und Serverprozesse des IT-Systems weisen keine bekannten ausnutzbaren Schwachstellen auf.

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

1 Technische Sicherheitsanforderungen

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 Architektur und Design

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.

3 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.

4 Schwachstellenanalyse und Penetrationstests

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.

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 Prüfkriterien 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
Prüfkriterien					
Technische Sicherheitsanforderungen	X	X	X	X	X
Architektur und Design			X	X	X
Installation und Betrieb				X	X
Schwachstellenanalyse und Penetrationstests		X	X	X	X
Änderungsmanagement					X

Tabelle: Prüfkriterien und Security Assurance Level für IT-Systeme