

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH  
bescheinigt hiermit dem Unternehmen

**RWE Effizienz GmbH**  
**Freistuhl 7**  
**44137 Dortmund**

für den Webshop

**RWE SmartHome Shop**

die Erfüllung aller Anforderungen der Kriterien

**Sicherheitstechnische Qualifizierung**  
**(SQ)<sup>®</sup>, Version 9.0**

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

Die Anlage ist Bestandteil des Zertifikats und besteht aus 5 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem zugehörigen  
Prüfbericht und ist bis zum 31.03.2013 gültig.



Zertifikat-Registrier-Nr.:  
TUVIT-SQ9541.11

13

Essen, 13.05.2011

Joachim Faulhaber  
Stellv. Leiter Zertifizierungsstelle

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

Zertifikat

## Zertifizierungssystem

**TÜV**<sup>®</sup>

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH führt Zertifizierungen auf Basis des folgenden Produkt-Zertifizierungssystems durch:

- „Zertifizierungsschema für TÜViT Trusted-Zertifikate der Zertifizierungsstelle TÜV Informationstechnik GmbH“, Version 1.0 vom 18.05.2010, TÜViT GmbH

## Prüfbericht

- „SmartHome-Lösung – Auflagenprüfung – Sicherheitstechnische Qualifizierung (SQ)<sup>®</sup> des RWE SmartHome Webshops der RWE Effizienz GmbH“, Version 1.1 vom 07.04.2011, TÜViT GmbH
- „SmartHome-Lösung – Sicherheitstechnische Qualifizierung (SQ)<sup>®</sup> des RWE SmartHome Webshops der RWE Effizienz GmbH“, Version 1.1 vom 17.01.2011, TÜViT GmbH

## Prüfanforderungen

- „Sicherheitstechnische Qualifizierung (SQ)<sup>®</sup> der TÜV Informationstechnik GmbH“, Version 9.0 vom 01.10.2006, TÜViT GmbH
- Systemspezifische Sicherheitsanforderungen (siehe unten)

## Prüfgegenstand

Gegenstand der Prüfung ist der Webshop „RWE SmartHome Shop“ der RWE Effizienz GmbH. Der Webshop besteht aus der Webanwendung und seiner Systemumgebung. Der RWE SmartHome Shop ist die zentrale Vertriebsplattform für die RWE-Kunden. Untersucht werden ausschließlich die unten aufgeführten systemspezifischen Sicherheitsanforderungen auf Basis der SQ<sup>®</sup>. Weitere Eigenschaften des Webshops sind nicht

Gegenstand der Zertifizierung.

**TÜV**<sup>®</sup>

## **Prüfergebnis**

- Die anwendbaren Anforderungen für die Sicherheitstechnische Qualifizierung sind erfüllt.
- Die systemspezifischen Sicherheitsanforderungen sind erfüllt.

## **Systemspezifische Sicherheitsanforderungen**

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

### **1 Sicherheitsfunktionen der Systemumgebung**

- Die Systemkomponenten der Webanwendung, die aus dem Internet erreichbar sind, enthalten keine zum Zeitpunkt der technischen Untersuchung bekannten, ausnutzbaren Schwachstellen.
- Administrative Tätigkeiten erfolgen über vertrauenswürdige Pfade, die die Integrität und Vertraulichkeit der Daten sichern. Die entsprechenden Schnittstellen sind aus dem Internet nicht erreichbar.
- Für die Betriebssysteme und Serverprozesse ist ein Protokollierungskonzept umgesetzt.
- Die Webanwendung wird durch eine Firewall-Installation geschützt.

### **2 Sicherheitsfunktionen der Webanwendung**

- Die Webanwendung verwendet sichere Authentisierungsmerkmale. Diese Authentisierungsmerkmale werden bei der Authentifizierung durch die Webanwendung auf sichere Weise geprüft.

- Die Webanwendung implementiert oder nutzt ein sicheres Session Management, das geeignet ist, die Sitzungen der Benutzer zu separieren.
- Es sind wirksame Zugriffskontrollen umgesetzt, die einen unautorisierten Zugriff auf URL, Geschäftsfunktionen, Daten, Services und Dateien schützen.
- Die Validierung der Eingabedaten ist umgesetzt.
- Die Anwendung setzt eine Ausgabekodierung um.
- Die Fehlerbehandlung und die Protokollierungsfunktionalitäten der Anwendung sind geeignet, um sicherheitsrelevante Ereignisse (z. B. Angriffsversuche) zu identifizieren. Sie geben keine vertraulichen Informationen preis.
- Die Anwendung nutzt sichere Einstellungen für die HTTP-Kommunikation, so dass die Datenübertragung abgesichert ist. Darüber hinaus werden die Daten über HTTPS-Verbindungen übertragen, die mittels SSL/TLS gesichert sind.
- Die Sicherheitskonfiguration der Webanwendung wird vor unautorisierten Änderungen geschützt.

## **Zusammenfassung der Anforderungen für die Sicherheitstechnische Qualifizierung (SQ)<sup>®</sup>, Version 9.0**

### **1 Technische Sicherheitsanforderungen**

Basierend auf anerkannten Kriterien, Spezifikationen oder Normen sind Sicherheitsanforderungen definiert. Diese weisen keine inhaltlichen Widersprüche auf und genügen geltenden Sicherheitsansprüchen.

## **2 Dokumentation der Architektur**

**TÜV**<sup>®</sup>

Für die Qualifizierung des IT-Produkts und seiner Einsatzumgebung bzw. des IT-Systems liegen für die Untersuchung angemessene Beschreibungen aller notwendigen Komponenten vor. Aus diesen sind die gegenseitigen Nutzungsbeziehungen und Datenflüsse sowie die Erfüllung der Sicherheitsanforderungen erkennbar.

## **3 Benutzer-, Administrations- und sonstige Betriebsdokumente**

Geeignete Handbücher zur Installation, Administration und Benutzung liegen vor. Diese enthalten insbesondere Hinweise zur Konfiguration der notwendigen System- bzw. Produktkomponenten sowie zu den räumlichen Maßnahmen und zu personellen Verantwortlichkeiten, die den Sicherheitsanforderungen genügen.

## **4 Sicherheit der verwendeten Komponenten**

Für alle Teilkomponenten, die Sicherheitsfunktionalitäten realisieren, konnte anhand von bereits durchgeführten formalen Evaluationen und/oder öffentlich zugänglichen Informationen nachvollzogen werden, dass sie als vertrauenswürdig eingestuft werden können.

## **5 Mittel des Systemmanagement**

Es existieren geeignete Konfigurationsmöglichkeiten sowie ein angemessenes Monitoring und Logging, die den sicheren Betriebszustand gewährleisten. Dafür eingesetzte Werkzeuge unterliegen denselben Sicherheitsanforderungen, wie das IT-Produkt / das IT-System selbst.

## **6 Tests und Inspektionen**

Umfangreiche Penetrationstests und technische Schwachstellenanalysen sind bei der Prüfung durchgeführt worden. Die bei den Tests und Analysen ermittelten Schwachstellen sind entsprechend ihres Risikogrades bewertet worden.

## **7 Änderungsmanagement**

Für die Planung und Durchführung von Neukonfigurationen sowie das Einspielen von Updates liegt ein Konzept vor, um Risiken und deren Auswirkungen adäquat bewerten zu können sowie die Erhaltung des angestrebten Schutzniveaus zu gewährleisten. Dieses legt dar, in welcher Weise Änderungen stattfinden dürfen und wie ggf. die Dokumentation angepasst wird.

## **8 IT-Systeme: Operationelle Umgebung**

Es liegen geeignete operationelle Bedingungen vor. Die personellen Verantwortlichkeiten und räumlichen Gegebenheiten genügen dem Sicherheitsanspruch des IT-Systems.

## **9 Sicherheitsanalysen**

Die Ergebnisse der vorher genannten Bewertungsaspekte sind im Rahmen einer abschließenden Analyse den Sicherheitsanforderungen gegenübergestellt und in einem Prüfbericht dokumentiert. Das Ergebnis ist, dass sämtliche Sicherheitsanforderungen erfüllt und die resultierenden Restrisiken tragbar sind.