Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

RWE Effizienz GmbH
Freistuhl 7
44137 Dortmund

für das Hausautomatisierungsprodukt

SmartHome Controller, Version 1.0

die Erfüllung aller Anforderungen der Kriterien

Sicherheitstechnische Qualifizierung (SQ)®, 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 6 Seiten.

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

Security PQ6118.11 TÜViT® 2011 Trusted Product
Voluntary Validation

Zertifikat-Registrier-Nr.:
TUVIT-PQ6118.11

Essen, 10.03.2011

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

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

Zertifizierungssystem

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

- „RWE SmartHome Controller“, Version 1.2 vom 24.02.2011, TÜViT GmbH

Prüfanforderungen

- „Sicherheitstechnische Qualifizierung (SQ)® der TÜV Informationstechnik GmbH“, Version 9.0 vom 01.10.2006, TÜViT GmbH
- Produktspezifische Sicherheitsanforderungen (siehe unten)

Prüfgegenstand

Gegenstand der Prüfung ist das Hausautomatisierungsprodukt „SmartHome Controller“, Version 1.0 der RWE Effizienz GmbH bestehend aus Software und zugehöriger Hardware. Der SmartHome Controller (SHC) steuert über Funk direkt die angeschlossenen Aktoren Heizkörperthermostat und Zwischenstecker sowie den Sensor Wandsender. Zudem können die Aktoren und Sensoren über Regeln und Profile gesteuert werden, die auf dem SHC hinterlegt werden. Die Konfiguration des SHC und die manuelle Steuerung der Aktoren erfolgt über die Software Control/Configuration Node und kann über das Internet oder über das lokale Netzwerk am SHC vorgenommen werden. Der SHC kann mit Software-Updates aktualisiert werden.

Die überprüften Sicherheitsmerkmale des Produkts sind im Abschnitt „Produktspezifische Sicherheitsanforderungen“ aufgeführt.

Prüfergebnis

- Die anwendbaren Anforderungen für die Sicherheits-technische Qualifizierung sind erfüllt.
- Die produktspezifischen Sicherheitsanforderungen sind erfüllt.
- Die im Prüfbericht genannten Anmerkungen und Auflagen sind zu beachten.

Produktspezifische Sicherheitsanforderungen

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

1 Vertrauenswürdiger Pfad

- Die Inbetriebnahme des SHC erfolgt über einen vertrauenswürdigen Pfad, der die Integrität und Vertraulichkeit der übertragenen Daten schützt.
- Die Kommunikation zwischen lokalem Control/Configuration Node und dem SHC im lokalen Netzwerk erfolgt über einen vertrauenswürdigen Pfad, der die Integrität und Vertraulichkeit der übertragenen Daten schützt.
- Die Kommunikation zwischen SHC und den Sensoren und Aktoren erfolgt über einen vertrauenswürdigen Pfad, der die Integrität und Vertraulichkeit der übertragenen Daten schützt.

2 Authentisierung

- Der SHC verwendet Authentisierungsverfahren, die die Verbindung zwischen SHC und Backend sowie Verbindungen aus dem lokalen Netzwerk schützen.

3 Zugriffskontrolle

- Nach erfolgreicher Inbetriebnahme des SHC ist dieser gegen unautorisierte, lokale Schalt- und Konfigurationsvorgänge geschützt.
- Daten, die im SHC gespeichert werden, sind gegen unautorisierte Zugriffe geschützt.
- Die Zertifikate und Schlüssel zur Authentisierung und Verschlüsselung werden geschützt gespeichert und sind gegen unberechtigte Zugriffe geschützt.
- Die Ansteuerung von Sensoren und Aktoren ist gegen unautorisierte Schalt- und Konfigurationsvorgänge geschützt.
- Die unautorisierte Kopplung von SHC und Sensoren oder Aktoren wird verhindert.
- Die unautorisierte Änderung einer eingerichteten Zuordnung von SHC und Sensor oder Aktor wird verhindert.

4 Änderungsmanagement

- Es wird nur von RWE geprüfte und abgenommene, vertrauenswürdige Software in den SHC eingespielt und installiert.
- Für den Control/Configuration Node wird ausschließlich von RWE geprüfte und abgenommene, vertrauenswürdige Software verwendet und verteilt.

5 Datenflusskontrolle

- Der SHC und die Control/Configuration Nodes im lokalen Netzwerk des Kunden stellen ausschließlich Verbindungen zu Systemen von RWE her. Der Verbindungsaufbau wird aus dem lokalen Netzwerk des Kunden initiiert.
- Auf dem SHC stehen nur die betrieblich notwendigen Netzwerkdienste zur Verfügung.

6 Protokollierung

- Sicherheitsrelevante Ereignisse werden vom SHC protokolliert.

Zusammenfassung der Anforderungen für die Sicherheitstechnische Qualifizierung (SQ)®, 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

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 Risikograde 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.