



# Zertifikat

Die Zertifizierungsstelle der  
TÜV Informationstechnik GmbH bescheinigt hiermit  
der

**Siemens Enterprise Communications GmbH & Co. KG**

Hofmannstraße 51  
81379 München

die

**Sicherheitstechnische Qualifizierung**

für den

**Remote Service basierend auf SIRA**

**Secured Infrastructure for Remote Access**

Der Umfang der in der Qualifizierung einbezogenen System-Teile und die mit der Installation verfolgten Sicherheitsziele sind im Qualifizierungsbericht spezifiziert. Die Qualifizierung wurde auf der Grundlage der Anforderungen der Spezifikation SQ, Version 9.0 von der TÜV Informationstechnik GmbH durchgeführt.

Dieses Zertifikat gilt nur in Verbindung mit dem Qualifizierungsbericht SQ Siemens, Version 1.0 vom 28.02.2007 sofern die Maßgaben für die Installation eingehalten werden.

Dieses Zertifikat berechtigt zur Nutzung des Prüfzeichens



**Voluntary Validation**

© 2007 TÜVIT GmbH - Member of TÜV NORD Group

Zertifikat-Registrier-Nr.:TUVIT-SQ9532.07

Essen, 28.02.2007 **gez. Dr. Sutter**

Zertifizierungsstelle

TÜV Informationstechnik GmbH - Unternehmensgruppe TÜV NORD  
Langemarckstraße 20 45141 Essen

**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 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.