



Zertifikat

Die Zertifizierungsstelle der
TÜV Informationstechnik GmbH bescheinigt hiermit,
dass die Web-Applikation

Visual Web
Version 2.3 Build 135_8
der
primion Technology AG

Steinbeisstraße 2-4
72510 Stetten a. k. M.

die Anforderungen zur Vergabe des Prüfzeichens Trusted Product Security
der TÜViT GmbH erfüllt.

Prüfgrundlage sind die in "Security Qualification (SQ)[®] and Certification of Trustworthy
IT Systems and Products" Version 9.0, Stand Februar 2006, dargelegten Anforderungen
zusammen mit den "Bewertungskriterien für sichere Web Applikationen (SWA)",
Version 1.0, Stand Februar 2006.

Die Erfüllung der Anforderungen ist in den Berichten
"Validierungsgrundlage für die Web-Applikation Visual Web", Version 1.0, 03.03.2006 und
"Validierungsergebnisse für die Web-Applikation Visual Web", Version 1.0, 03.03.2006
der TÜV Informationstechnik GmbH dokumentiert.

Eine Übersicht der Anforderungen wird umseitig wiedergegeben.

Dieses Zertifikat ist längstens gültig bis zum 31.03.2007.
Es berechtigt zur Nutzung des Prüfzeichens



Gültig bis

Voluntary Validation

© 2006 TÜVIT GmbH - Member of TÜV NORD Group

Zertifikat-Registrier-Nr.: TUVIT-PQ6103.06

Essen, 03.03.2006 gez. Dr. Gruschwitz

Zertifizierungsstelle

Kriterien für Sichere Web-Applikationen (SWA), Version 1.0

Die **Kriterien für Sichere Web-Applikationen (SWA)** bestehen aus den folgenden Sicherheits- und Qualitätsanforderungen, die für das jeweilige Produkt auf Basis der *Security Qualification (SQ)[®] of Trustworthy IT Systems and Products, Version 9.0, Stand Februar 2006* überprüft werden:

1. Sicherheitsanforderungen

Die Web-Applikation verfügt mindestens über folgende Sicherheitseigenschaften:

- Identifikation und Authentisierung

Die Web-Applikation muss den Benutzer eindeutig identifizieren und authentifizieren. Die Authentisierungsdaten müssen hinreichend stark sein, um gängigen Angriffen ausreichend lange standzuhalten. Des Weiteren müssen vorgetäuschte Authentisierungsdaten von der Web-Applikation erkannt und deren Missbrauch verhindert werden.

- Zugriffskontrolle

Die Web-Applikation muss Funktionen bereitstellen, die es ermöglicht, Benutzerrechte einzuschränken. Einem Benutzer darf es mit vertretbarem Aufwand nicht möglich sein, seine Rechte unbefugt zu erweitern.

- Vertrauenswürdiger Kanal zum Web-Browser des Benutzers

Die Web-Applikation muss Funktionen zum Aufbau eines vertrauenswürdigen Kanals zum Web-Browsers des Benutzers bereitstellen, der die Vertraulichkeit und Integrität der übertragenen Daten sicherstellt.

2. Qualitätsanforderungen

Die Web-Applikation verfügt mindestens über folgende Qualitätseigenschaften:

- Unterstützung mehrerer Benutzer gleichzeitig

Die Web-Applikation kann zuverlässig mehrere Benutzer gleichzeitig bedienen.

- Unterstützung von Browsern verschiedener Hersteller

Die Web-Applikation arbeitet fehlerfrei mit Browsern unterschiedlicher Hersteller zusammen.

- Online-Hilfe für die Benutzung der Web-Applikation

Eine Online-Hilfe mit Erläuterungen zu allen wichtigen Funktionen der Web-Applikation steht dem Benutzer zur Verfügung.

- Keine Software-Installation durch den Benutzer

In der Standard-Konfiguration der Web-Applikation ist außer der Installation auf dem Server keine weitere Installation von Software notwendig.

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 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.