Zertifikat

Die Zertifizierungsstelle der
TÜV Informationstechnik GmbH bescheinigt hiermit
dem

Rechenzentrum der Finanzverwaltung

Roßstraße 131
40476 Düsseldorf

die

Sicherheitstechnische Qualifizierung

für die

ELSTER Clearingstelle in Düsseldorf

Der Umfang der in der Qualifizierung einbezogenen System-Teile und die mit der Installation verfolgten Sicherheitsziele sind im Dokument "*RZF D SQ, Version 1.12*" spezifiziert. Die Qualifizierung wurde auf der Grundlage der Anforderungen der Spezifikation SQ, Version 8.2 von der TÜV Informationstechnik GmbH durchgeführt.

Dieses Zertifikat gilt nur in Verbindung mit dem Qualifizierungsbericht *RZF D SQ, Version 1.12* vom 13.02.2002 sofern die Maßgaben für die Installation eingehalten werden.

Dieses Zertifikat berechtigt zur Nutzung des Prüfzeichens

Security SQ9518.02 2002 Trusted Site
Voluntary Validation

© 2001 TÜViT GmbH - ein Unternehmen der RWTÜV-Gruppe -

Zertifikat-Registrier-Nr.:TUVIT-SQ9518.02

Essen, 14.02.2002 **gez. Dr. Gruschwitz**

Zertifizierungsstelle

TÜV Informationstechnik GmbH - Ein Unternehmen der RWTÜV-Gruppe
Am Technologiepark 1 · 45307 Essen

Zusammenfassung der Anforderungen für die Sicherheitstechnische Qualifizierung (SQ), Version 8.2

1 Technische Sicherheitsanforderungen und Vorgaben

Es liegen technische Sicherheitsanforderungen vor, die die Sicherheitspolitik und die Bedrohungen darlegen. Die Informationen zu den technischen Sicherheitsanforderungen weisen keine inhaltlichen Widersprüche auf.

2 Systemdokumentation

Eine Darstellung der statischen Systemstruktur, die mindestens die Zerlegung bis auf die Ebene von Hauptsubsystemen darlegt, liegt vor. Die Zerlegung eines Subsystems ist in dieser Darstellung bis auf Komponenten verfeinert, wenn dies als sicherheitsspezifisch erkannt wurde. Die Nutzungsbeziehungen und Datenflüsse zwischen den identifizierten Subsystemen sind dargelegt.

3 Sicherheit der verwendeten Komponenten

Für alle Komponenten und Subsysteme der Zerlegung sind funktionale Spezifikationen erkennbar. Darlegungen der externen Schnittstellen der Installation liegen vor. Die Sicherheitsanforderungen von sicherheitsspezifischen Subsystemen sind erkennbar. Für wesentliche sicherheitsspezifische Subsysteme liegen Darlegungen der Sicherheitsanforderungen vor.

4 Benutzer-, Administrations- und sonstige Betriebsdokumentation

Handbücher zur IT-Installation sowie zu den sicherheitsspezifischen und kritischen Subsystemen liegen vor.

5 Mittel des Systemmanagement

Ein Konfigurationsmanagement der sicherheitsspezifischen Komponenten ist vorhanden und ein Monitoring ist möglich.

6 Verfahren und technische Mittel des Änderungsmanagement

Ein Security Maintenance-Plan liegt vor. Dieser legt dar, in welcher Weise Dokumentation und Sicherheitsanalysen bei Änderungen an der IT-Installation regelmäßig zumindest nachträglich angepasst werden. In dieses Verfahren sind mindestens die Dokumentation der IT-Installation (Zerlegung) und die technischen Sicherheitsanforderungen eingeschlossen.

7 Tests und Inspektionen

Durch eine Inspektion an der Installation sind die sicherheitsspezifischen Komponenten identifiziert und ihr Vorhandensein in der angenommenen Version vollständig bestätigt worden. Der Betreiber hat für die Prüfer erkennbare Nachweise über vollständig erfolgreiche Tests aller definierten Sicherheitsfunktionen vorgelegt.

8 Operationelle Anforderungen

Geeignete operationelle Bedingungen, die eine einwandfreie Funktionsweise des zu untersuchenden Systems unterstützen, liegen vor. Die personellen Verantwortlichkeiten und die räumlichen Gegebenheiten gewährleisten den fachkundigen Einsatz und die Zugangssicherheit der Installation.

9 Sicherheitsanalysen

Die Prüfer haben qualifizierte Aussagen zu den Schwachstellen der Installation abgegeben. Resultierende Aussagen über die Klassifizierung der Subsysteme und die Wirksamkeit der Sicherheitsfunktionen liegen vor.