Certificate

The certification body of TÜV Informationstechnik GmbH
hereby confirms that

Microsoft GmbH

Konrad-Zuse-Str. 1
85716 Unterschleißheim
has passed

Security Qualification

for the

Scalable Enterprise Firewall System Architecture

Built with Microsoft Internet Security and Acceleration Server 2000

The extent of the parts of the installation included in this qualification as well as the considered security objectives are specified in the document *SQ Microsoft, version 1.0.* The qualification was performed by TÜV Informationstechnik GmbH on the basis of the requirements of the specification SQ version 8.3.

This certificate is valid only in conjunction with the SQ evaluation report *SQ Microsoft, version 1.0* of 2003-01-16, provided that the measures for the installation described in the document *Configuration Guide for TÜViT security-related qualification of a trustworthy IT installation built with the Microsoft Internet Security and Acceleration Server 2000, V1.0,* of 2003-01-15 are respected.

This certificate entitles to use the certification mark

Security SQ9521.03 TÜViT 2003 Trusted Site

Voluntary Validation

Certificate Registration No.:
TUVIT-SQ9521.03

Essen, 2003-01-16 **signed by Dr. Gruschwitz**
Certification Body

TÜV Informationstechnik GmbH - Subsidiary of the RWTÜV Group
Am Technologiepark 1 · 45307 Essen

Summary of the requirements for the Security Qualification (SQ), version 8.3

1 Technical security target

Technical security requirements exist which comply to “current security claims”. There are no inconsistencies in content.

2 Documentation of the IT-installation

In the documentation the used elements and relations of the IT installation are explained in a clear and understandable way . The documentation describes the partition into basic subsystems. The relations of use and the data flow between the identified subsystems can be reconstructed.

3 User-, administration-, and further operational documents

Manuals for the IT installation as well as for the security enforcing and critical subsystems exist.

4 Security of utilized components

All components and subsystems with security functions can be regarded as trustworthy. The trustworthiness is verified with the help of conducted formal evaluations and/or public information sources.

5 Means of the system management

Suitable configuration tools of the security enforcing components exist and monitoring these components is possible. All administrative tools are safeguarded as good as the security enforcing subsystems.

6 Tests and inspections

By means of network tests and configuration analyses it has been verified that no known or directly usable vulnerabilities exist on the inspected IT installation.

7 Change management

A concept exists for planning and carrying out changes in order to assess adequately the consequences for security. The concept describes how changes may be performed and how the documentation of the IT installation has to be adapted.

8 Operational requirements

Suitable operational conditions supporting a perfect functioning of the inspected system exist. The personal responsibilities and physical conditions meet the security claims of the IT installation.

9 Security analyses

The evaluators have documented their results in a test report. The result of the inspection is that all security requirements are fulfilled and the remaining risks can be accepted in accordance with the customer.