

The certification body of TÜV Informationstechnik GmbH  
hereby awards this certificate to the company

**KDVZ Citkomm  
Griesenbraucker Straße 4  
58640 Iserlohn, Germany**

to confirm that its VPN-Gateway

**iWAN-Gateway, Version 2**

fulfils all requirements of the product specific document

**Security Qualification (SQ),  
Version 9.0**

of TÜV Informationstechnik GmbH. The requirements are  
summarized in the appendix to this certificate. The appendix is  
part of the certificate and consists of 7 pages.

The certificate is valid only in conjunction with the corresponding  
evaluation report until 2013-04-30.



© 2011 TÜVIT GmbH - Member of TÜV NORD Group

Certificate-Registration-No.:  
TUVIT-PQ6119.11

13

Essen, 2011-04-05

Joachim Faulhaber  
Deputy of Certification Body

**TÜV Informationstechnik GmbH**  
Member of TÜV NORD Group  
Langemarckstr. 20  
45141 Essen, Germany  
www.certuvit.de

Certificate

## **Certification System**

The certification body of TÜV Informationstechnik GmbH performs its certification on the basis of the following product certification system:

- German document: “Zertifizierungsschema für TÜViT Trusted-Zertifikate der Zertifizierungsstelle TÜV Informationstechnik GmbH“, version 1.0 as of 2010-05-18, TÜViT GmbH

## **Evaluation Report**

- German document: “Prüfbericht Sicherheitstechnische Qualifizierung (Nachprüfung) des iWAN-Gateways, Version 2, der KDVZ Citkomm“, version 1.0 as of 2011-03-10, TÜViT GmbH

## **Evaluation Requirements**

- German document “Sicherheitstechnische Qualifizierung (SQ)<sup>®</sup> der TÜV Informationstechnik GmbH“, version 9.0 as of 2006-10-01, TÜViT GmbH
- Product-specific security requirements (see below)

## **Evaluation Target**

The target of the evaluation, iWAN-Gateway, Version 2, is a VPN-Gateway with firewall functionality and consists of following components:

- iWAN-baseGate, Release 2,  
for connection of a single customer LAN to a Virtual Private Network (VPN)
- iWAN-easyGate, Release 2,  
for connection of further distributed IT components of the customer LAN

each with network interfaces for LAN and Internet connections and an ISDN backup interface.

The product “iWAN-Home“ is not included in the evaluation target.

## **Evaluation Result**

- The evaluation target fulfils all applicable evaluation requirements of the “Security Qualification (SQ)”.
- The evaluation target fulfils the product-specific security requirements.

## **Product-specific security requirements**

The certification is based on the following product-specific security requirements, whose fulfilment was assessed.

### **1 Identification and Authentication**

- Unambiguous identification and authentication for users and also the administration of the iWAN-Gateways themselves by the administrators of the KDVZ is performed by means of a trustworthy path, which protects the integrity and confidentiality of the data which is transferred.
- Establishment of a VPN between the iWAN-Gateways is based on unambiguous and successful identification and authentication of the participating iWAN-Gateways as termination endpoints.
- Failed authentication attempts at the iWAN-Gateways, in particular for the administrative area, are saved as logging information.

## **2 Access control**

- The iWAN-Gateway protects itself against attacks known at the time of the assessment. Such attacks include those
  - from the Internet,
  - from the established VPN and
  - from further local networks connected to the iWAN-Gateway.
- Only the software and services which are absolutely necessary for operation are present on the iWAN-Gateway that is used.

## **3 Data flow control**

- The firewall architecture of the iWAN-Gateway is implemented in several stages in order to protect the local network structure. Therefore direct connection from the Internet into the network to be protected and vice versa is not possible.
- The standard rule set of the iWAN-Gateway ensures that
  - all connections that are not explicitly permitted are blocked (White List) and
  - the filter rules are free of logical inconsistencies and are consistently laid down in the order in which they are worked through.
- The packet filter with Stateful Packet Inspection supports at least a separate filtering of incoming and outgoing packets at each network interface by transferring on or refusing packets based on:
  - the source IP and target IP address of individual

- computers or partial networks,
- the source and target ports for TCP and UDP packets,
- the ICMP subtype,
- the TCP flags (URG, ACK, PSH, RST, SYN, FIN),
- the connection status in the case of connection-orientated protocols (e. g. TCP).
- At least the following actions are supported for each filter rule:
  - Onward transfer of the packet ("Allow"),
  - Refusal of the packet ("Deny & Drop"),
  - Refusal of the packet and report to the sender ("Deny & Reject").

#### **4 Transmission security**

- The confidentiality of the data traffic within the VPN between the iWAN-Gateways is ensured by means of suitable encryption methods.

#### **5 Logging**

- Logging of the:
  - IP address (Receiver/User)
  - Port number (Service)
  - Time and date for each packet

of the source and target system is possible for each established or refused VPN connection of the iWAN-Gateway.

- The iWAN-Gateway offers the possibility of sending all

logging information to a configurable central location at the KDVZ via a trustworthy path which protects the integrity and confidentiality of the transferred data.

- If a logging component is not present, the iWAN-Gateway offers the possibility of issuing a warning to the administrators of the KDVZ.
- The activities of the administrators at the iWAN-Gateways are technically recorded as logging information in a manner which is secure against manipulation.

## **6 Change management**

- The integrity of the software packages, configuration files and update packages (e. g. security updates) is ensured by the KDVZ by means of suitable mechanisms before the update process of the iWAN-Gateways. It is ensured by the KDVZ that only packages that have been checked are installed.

## **Summary of the requirements for the Security Qualification (SQ), version 9.0**

### **1 Technical security requirements**

Technical security requirements are defined based on recognized criteria, specifications or standards. The technical security requirements are free of internal contradictions and satisfy accepted security requirements.

### **2 Documentation of the architecture**

For the qualification of the IT product and its application environment or of the IT system, appropriate descriptions of all necessary components are available. From these, the mutual utilization relationships and data flows as well as the fulfillment of security requirements can be recognized.

### **3 User, administration and other operational documents**

Suitable manuals for installation, administration and usage are available. These particularly include notes on configuration of necessary system and product components as well as environmental measures and personnel responsibilities which satisfy the security requirements.

### **4 Security of the components used**

All sub-components that implement security functionalities could be classified as trustworthy based on previously performed formal evaluations and/or publicly accessible information.

### **5 Means of system management**

Suitable configuration facilities as well as appropriate monitoring and logging guarantee the secure operational state. Tools used for system management are subject to the same security requirements as the IT product/IT system itself.

### **6 Tests and inspections**

Comprehensive penetration testing and technical vulnerability analyses have been performed during testing. The vulnerabilities determined during testing and analyses have been rated according to their risk potential.

### **7 Change management**

A concept for the planning and implementation of new configurations and the import of updates exists in order to adequately evaluate risks and their effects as well as to guarantee maintenance of the intended protective level. The concept describes the way in which changes may take

place and how the documentation is adapted where necessary.

## **8 IT systems: operational environment**

Suitable operational conditions exist. The personnel responsibilities and environmental conditions satisfy the security claim of the IT system.

## **9 Security analyses**

In a final analysis documented in the evaluation report the results of the previously listed evaluation aspects are compared to the security requirements. The result is that all security requirements have been met and the resulting residual risks are bearable.