

## Information Security in the TecCom System

When creating the TecCom software and the TecCom infrastructure, the greatest attention is paid to the security of data in the TecCom system. This extends all the way to the interface to each TecCom user. The following describes the existing security measures for TecCom software and providers along with those measures that must be taken by the TecCom business partners (buyers, suppliers).

### Description of TecCom provider security

- The TecCom system provides the TecCom business partners (users, suppliers) with a network that meets the highest requirements for data security in the area of networks.
- The actual log-in to the TECCOM application server is done via a separate password, which the business partners should be changed as often as possible.
- The connection can be made via Internet. All the data traffic is handled with HTTPS. In this way, only encrypted data are transferred (via SSL: secure socket layer). Any accidental or purposeful recording of the data stream can only be made re-usable again with the help of the associated key.
- It is not possible to establish a direct connection between buyer and supplier, supplier to supplier, or buyer to buyer. The entire data traffic is handled via TecCom application servers. The application servers do not provide routing of messages. Instead, the messages are processed, and logical connections are established with the necessary points in the network, depending on the business transactions.
- In the TecCom system, business process data is transported in a special format (TecForm).
- In the application, all passwords are encrypted.
- Access to the databases of the user is encrypted
- Access to the TecCom system from the Internet is protected by a firewall maintained by the operator of the system. In this firewall, only the protocol HTTPS (Port 443) can be used. Via this port (443) and using a filter, only TecForm messages can be received.
- The WIN2003 servers available in the TecCom network are tested regularly using the latest security guidelines in order to ensure early detection of any weak points in the security.
- All TecCom components are operated in security areas (access protection, fire protection, emergency power supply).
- All employees have signed agreements obligating them to comply with the data secrecy provisions of § 5 of the BDSG (Bundesdatenschutzgesetz = German privacy law) and to observe business and official secrets as well. They are informed regularly of any changes.
- The TecCom system operator is certified under ISO 9001.

**TecCom system security can be achieved only if both the TecCom system operator and all business partners observe the following principles:**

### **Measures for Buyers**

- Business partners (buyers) dialing in directly from a PC without their own network should switch off acceptance of external calls at their modem or ISDN adapter. It may be possible to do this in their telephone system. This prevents unauthorized access to the PC from outside. When the connection to the TecCom system is no longer needed, it should be disconnected.
- Business partners (orders) with their own network and router used by numerous PCs to log on to the TecCom system must use an IP-based “extended access list” in the router. This makes it possible to limit data traffic to a single IP address pair.

Connection to the TecCom system is done via an NIC-IP address or an RFC address (including network address conversion) issued by the TecCom system. The system operator provides this address to the user at the time of set-up. The user can reach all TecCom services via this one IP address.

- The user and operator agree to a host name and a password. Using the PPP protocol (with CHAP) the routers involved exchange messages. Data traffic is only possible if the data matches.
- In the router the protocol HTTPS (Port 443) should be implemented. In this way only HTTPS messages are permitted up to the local network. Acceptance of external calls in the router should be disabled except when incoming EDIFACT messages are used, in which case a check of the external caller ID should be implemented. When the connection to the TecCom system is no longer needed, it should be disconnected.

### **Measures for suppliers**

- Business partners (suppliers) with their own network and router used by numerous PCs to log on to the TecCom system must use an IP-based “extended access list” in the router. This makes it possible to limit data traffic to a single IP address pair.

Connection to the TecCom system is done via an NIC-IP address or an RFC address (including network address conversion) issued by the TecCom system. The system operator provides this address to the user at the time of set-up. The user can reach all TecCom services via this one IP address.

- The user and operator agree to a host name and a password. Using the PPP protocol (with CHAP) the routers involved exchange messages. Data traffic is only possible if the data matches.
- In the router only the protocol HTTPS (Port 443) should be implemented. In addition for acceptance of external calls, checking of the CID (caller ID = ISDN telephone number) should be activated. This avoids the possibility that the outgoing call could be taken by an “outsider”. When the connection to the TecCom system is no longer needed, it should be disconnected.
- Business partners with their own firewall should observe the same rules as above. The firewall should use all filtering options.