



cabPROTECT

Data security in label printing

Modern manufacture sees marking systems work autonomous, interact among each other, with host computers or a plant control unit. Data security is a key issue. The integration of components, their administration and authentication are sensitive tasks demanded from the corporate IT. cab systems developed for printing and applying labels provide proper features by default, fairly protecting your data in a network.



Permissions can be assigned to users and restricted by passwords.



Firmware updates are verified for integrity before installation.



Access to network services (HTTP, FTP, VNC, OPC UA etc.) is possible only for users with authorization. Network services can be switched on or off.



Network protocols can be encrypted using TLS/SSL. To connect securely in a network, a certificate as required is installed in the device ex factory.



Wireless interfaces (WLAN, Bluetooth) can be switched on or off. WPA2, WPA2 Enterprise and WPA3 levels of security are supported.



Printers in a network can be authorized securely. IEEE 802.1X network standard is supported.



USB slots can be locked and access to external storage media be denied.



All the current cab printing systems are based on the same electronics and firmware. The printer language is the same, so are interfaces and memory. Any further developed operating system or driver is available immediately on every device. Resets to default settings are PIN-protected.

Do you have questions? info@cab.de