cabPROTECT

Data security during label printing

The responsible handling of data and the manipulation-free operation of all cab printing systems are key concerns for us. We have defined safety standards for our devices which I would like to present to you here.

Mario Hiss
Strategic Product Management, cab

Industry 4.0, with a focus on information and communication technologies, is driving intelligent labeling forward. Our customers' printing systems operate autonomously without the need for additional equipment. In networks, they communicate with system controls, host computers or systems for planning and managing resources. Process networks are interconnected inhouse, across locations or transnationally. The resulting advantages are undisputed. However, for the IT managers of a company, this also results in new requirements.

Especially the connection to an ERP software and thus to master data can be critical in case of insufficient security. Think of manipulation possibilities, for example, infections via the Internet, the infiltration of malware via removable media and external hardware into a system, remote maintenance access, but also human error. Solutions for these tasks are, today more than ever, an integral part of our product development.

cabPROTECT

cabPROTECT Security Standards

System password

cab printing systems are delivered open, without restrictions. With the help of a password the access to a system can be restricted and an assessable security level for network participants can be achieved. A system password makes sense especially, if authorizations or encryptions are assigned for device-internal or network settings. These could, without protection, easily be changed or deleted.

External Access

cab printing systems provide remote access via http, SOAP WebService, FTP, VNC or OPC UA for configuration, usability and monitoring. For each service a separate password protected access is factory set up in the device. Changes require the knowledge of the → **System password** (if such a password has been assigned for the access to the cab printing system).

- **http-Service** allows to configure, set parameters and operate a cab printing system with a common browser from a PC or any other network connected device. The service can be accessed by entering the IP address of the printing system. The access is password protected.

- **WebServices** enable services and functions via a defined interface and protocols and enable the interaction of individual machines. Communication with the WebService can be done from different platforms and with different programming languages. The cab WebService uses the standard SOAP. Communication partners have to authenticate each other via a password. The http authentication methods Basic (user name, password) and Digest (user name, password, random string) are supported.

- **FTP-Service:** The transfer of data in a network via the File Transfer Protocol is done in several parts: FTPprint enables printing, FTPcard enables access to a USB stick, a SD card or the internal system memory IFFS, FTPadmin enables the installation of firmware. Each access requires the authentication via a password.

- **VNC-Service** allows to transfer the control panel of a cab printing system (server) to the screen of another participant in the network (client). The activities of the client at a keyboard or mouse are displayed on the server. VNC is platform independent. The access via VNC to a cab printing system is authenticated by a password.

- **OPC UA** is the interface standard in Industry 4.0. It is independent of manufacturer or system supplier, operating system or programming languages and represents the secure communication of field devices in a network or via the Internet. Machines communicate among themselves or with a PC.
cab printing systems have an OPC UA server and an OPC UA client integrated in the firmware.
The server allows the configuration and monitoring of the system. Dynamic print data can be prepared via a defined programming interface. With the client data fields from other OPC UA capable machines can be read and placed on a label. When accessing without a password, write and read rights can be assigned individually. Anonymous access can be switched off and access can be protected by a password.

cabPROTECT

Import / Export of System Settings

In order to save device configurations or transfer them to other devices after commissioning, cab printing systems allow the import and export of this configuration via → **WebDAV** to a network, to a USB stick, SD card or to the internal IFFS device memory. For saving and loading a password can be defined. Entering or editing this password requires the knowledge of the → **System password** (if such a password has been assigned to access the cab printing system).

WebDAV

The firmware of cab printing systems supports the transfer protocol WebDAV. This allows the integration of virtual memories into a cab device via network. The internet storage becomes available as a drive and thus accessible everywhere. The setup of the WebDAV client is done once at the cab printing system. For setup the access data must be known and a user account must be created on the system. Entering or editing these data requires the knowledge of the → **System password** (if such an account has been assigned for the access to the cab printing system).

TLS-Certificate

cab printing systems offer the possibility to transfer data between a participant in the network (client) and a server encrypted by a TLS certificate. TLS is the further development of the SSL protocol and is recognized as even more secure, flexible and efficient. In the standard version a certificate required for this kind of data transfer is factory installed on cab printing systems. This certificate can be overwritten by an own signed certificate at any time. It can be read in via USB stick, SD card or a → **WebDAV** network connection.
The certificate contains identification information that can be used to identify yourself to a server or client in order to release the data transfer. The use of the certificate as well as its selection requires the knowledge of the → **System password** (if such a certificate has been assigned for the access to the cab printing system).
If TLS is activated, the system automatically switches to this encrypted method when using the network services HTTP/HTTPS and FTP/FTPS.

Authentication to IEEE 802.1X

cab printing systems support the IEEE 802.1X network standard. By this, such printers can be authorized securely in a network. Subscribers logging in the network are checked and approved automatically by an authentication server. Similar to a WLAN key, data interchange is granted or denied depending on the agreed authentication information. EAP-PEAP, EAP-TLS and EAP-TTLS authentication standards are provided.

WLAN

Wireless data transmission offers advantages, especially for extensive installation areas or for location-independent, mobile applications. Installation costs are reduced, the application gains flexibility. Encrypted transmission prevents the unauthorized interception of data and its manipulated forwarding. cab printing systems use the methods WPA2 (mainly in smaller networks), WPA2 Enterprise (larger networks) and WPA3 to encrypt the data exchange. Encryption is done according to the generally recognized very secure AES standard. Participants of the WLAN network must authenticate themselves before they are allowed to access resources in the network. To do this, the access point (station that receives and sends data) interrogates the authentication server. The authentication between the participant and the receiving station is done via the WLAN key, a secret string of characters. Changing this key requires the knowledge of the → **System password** (if such a key has been assigned to access the cab printing system). cab printing systems with configured WLAN can be used as hotspot and thus be configured, controlled and monitored from mobile devices. The access requires the password protection described at → **External access.**

cabPROTECT

Firmware Update

Whenever the firmware is updated, the new file is first checked for completeness, damage, correspondence to the corresponding printing system and correct code sequences. Only if the update has been completed without errors, the new version of this firmware is activated on the cab printing system. In future, every cab firmware package shall calculate and publish a mathematical algorithm consisting of letters and numbers. The correspondence of this MD5 checksum with a value transmitted when downloading the firmware guarantees digital integrity and the authenticity of this file. To ensure that no unauthorized updates are performed on the printing system it is recommended to disable access to external storage media as well as → **USB interfaces** and to protect the FTP admin area with a password.

External Memory Devices

cab printing systems support USB mass storage and SD cards. These are usually only used for data transfer and storage, if the printing system is not integrated in a network. To ensure that no unauthorized data or malware can be transferred to the printing system via these channels, the external storage media can be switched off at the cab printing system. This also prevents the unauthorized storage of data from the printing system to external storage media.

USB-Interfaces

cab printing systems have USB interfaces on the back of the device and in the area of the control panel. They are used to configure the printing system with print data, layouts or firmware. They also support the input of print data via keyboard or readers, the control of the system via USB or a Windows driver. For 100 percent prevention against unauthorized access, e.g. a USB mass storage device or → **cab Service Key**, the USB interfaces of cab printing systems can be locked.

cab Service Key

If a password has been assigned for access to a cab printing system, but has been forgotten or lost, all settings can be made via a cab service key. cab hands out these keys only to authorized and registered persons. The service key is plugged into one of the → **USB interfaces** at the cab printing system (make sure that this interface is not locked.) It must be removed from the system after finishing the service work and stored safely. If the USB interfaces of the device are locked and therefore access is not possible, it is possible to send the cab printing system to the nearest cab factory for activation. Otherwise the CPU in the device has to be replaced. This has to be requested from cab.

cabPROTECT compact

www.cab.de/en/cabprotect

Do you have any question? info@cab.de