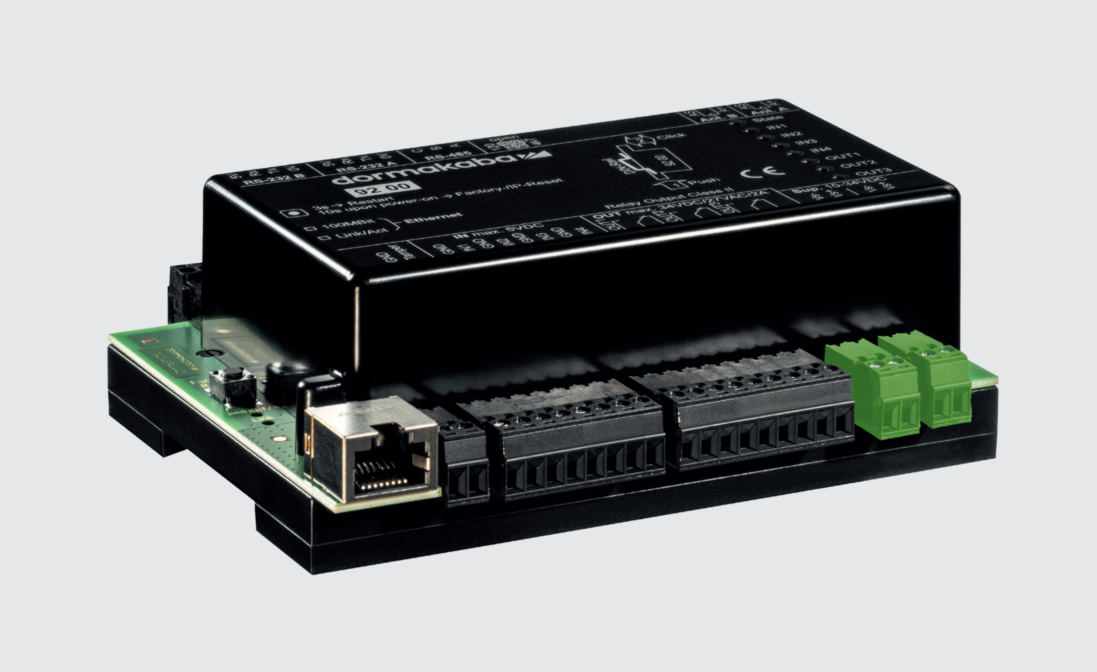
Whitepaper B-Client AC30-K7 Access Manager



Linux system context

The access control management systems of the K7 generation have an embedded Linux operating system. The Linux kernel provides important security functions, such as a user-based authorisation model, process isolation, or the option of removing unnecessary or potentially unsafe components from the kernel. The Linux system is continuously maintained.

Updates can be provided specifically as the situation requires: either for the entire system, only for the application, or for sub-components like readers, for example.

Administration of the user accounts in the AC30 environment is limited to the account admin; access as root is ruled out. The account update user is an exception, as its access rights are limited to a single directory that is used for the update mechanism.

The connection to the reader units is established via a serial RS485 interface. With the 92 00 and 92 30, it is possible to additionally connect two registration units via coaxial cable. The protocols via these connections are proprietary. Encryption of the serial communication is currently under development and will be available as an option in future versions.

The security level for the protection of media content is determined by the system operator through their choice of media technology.

Presented by dormakaba

Web server

The B-Client AC30 application has an integrated web server which ensures that the service interface is available. Via the service interface, the network configuration as well as the date/time and user passwords can be managed using a browser. Access to diagnostic data is also possible.

- The pages of the service interface can be accessed exclusively via https. For this purpose, an (access manager) self-signed certificate created by dormakaba is used, which must be trusted initially. Self-signed certificates do not constitute unsafe certificates. The user must independently confirm that they trust this connection.
- Sensitive data cannot be accessed via the service interface.
- The security of the web server is continuously maintained.
- The user root cannot be used.
- The user is forced to change the default password on first login. This is subject to password rules (upper/lower case letters, numbers, and special characters).

SSH server

The Linux system provides an SSH server. This allows access to the file system and an SSH console. Particularly for diagnostic purposes, this is a useful option for obtaining the needed data quickly. Host communication software like B-COMM can very quickly read and write the parameter files in the device through the SSH connection.

- Access is only possible by means of authentication via a private key file, which can be managed by the end user or, for example, by the host communication software.
- Starting with B-COMM Version 5.1, the key management (SSH) functionality is already supported as standard.

  Via the service interface, the access manager can be reset to factory settings. This also resets the SSH keys accordingly.
- The security of the SSH server is continuously maintained.
- Here as well, access for the user root is not possible.

Host communication

- Communication with the host system is possible via different protocols.
- Optionally, the communication with the host system can be encrypted.

Hardware

- The devices are equipped with connectors for the communications connections as well as input and output contacts for registration of the sensors regarding, for example, door status and access monitoring. The number of contacts depends on the device type used.
- Depending on the reader type, the contacts of the reader can be used as well.

A access manager 92 00 is equipped with directly accessible contacts, so these devices must be installed in secure areas. The level of protection against unauthorised access can be increased by installing the device in a lockable housing, but this is generally the facility operator's responsibility. Devices with closed covers like the 92 90 or 92 30 have an internal tamper switch which triggers an alarm message as soon as the cover is opened.

- The devices do not have a debug interface.
- To operate, the device software requires a license, which is linked to the MAC address of the network interface and thus is not transferrable.
- Security guidelines
- Satisfies the requirements of the GDPR.

Recommended security measures for customers

Apart from the security measures provided by dormakaba and Linux, the customer must also take an active role in optimally securing the overall system:

- Place the access managers in a secure environment whenever possible.
- Deactivate the SSH and web server when commissioning is completed and the servers are not needed for operation.
- Activate the SSH and web server only when needed.
- Limit network access by implementing firewall rules. It is not necessary to allow an incoming connection to the dormakaba access manager from outside your company network.
- Implement a password rule for the access manager and change all standard user passwords, pass phrases, and key files.

Network authentication IEEE 802.1X

The access manager offers the option of integration in IEEE 802.1X-protected LAN networks.
For this purpose, the access manager can be configured as an IEEE 802.1X supplicant with the conventional authentication procedures (EAP MD5 & EAP PEAPv0/ MSCHAPv2) .

B-Client AC30 satisfies the international IEC 60839-11-1 standard, security level 3

The IEC 60839-11-1 standard describes the general requirements for the function of electronic access control systems for use in security applications.

The standard covers minimum functionality, performance requirements, and testing procedures for electronic access control systems and devices used for physical access (entry and exit) in and around buildings and secured areas, as well as minimum requirements in terms of environmental and EMC conformity criteria that apply to devices of electronic access control systems at the respective level.

B-Client AC30 satisfies those criteria according to security level 3.

Any questions? We would be happy to answer any questions you may have.

dormakaba International Holding AG | Hofwisenstrasse 24 | CH-8153 Rümlang | T +41 44 818 90 11 | info@dormakaba.com | www.dormakaba.com

Subject to technical modifications.