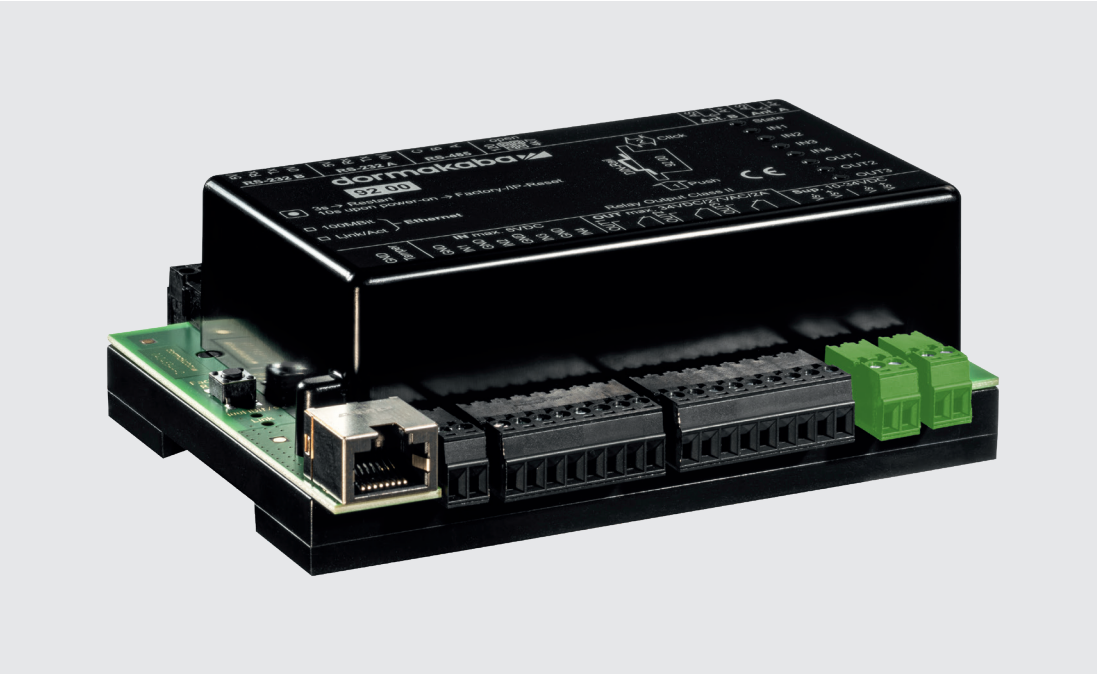
Papier blanc
B-Client AC30-K7
Gestionnaire d'accès



Contexte du système Linux

Les commandes de contrôle d'accès de génération K7 utilisent un Embedded Linux (embarqué) comme système d'exploitation. Le noyau Linux fournit d'importantes fonctions de sécurité telles qu'un modèle d'autorisation basé sur les utilisateurs, l'isolation des processus ou encore la possibilité de retirer du noyau les composants superflus et potentiellement vulnérables. Le système Linux est mis à jour en continu.

Selon les situations, des mises à jour peuvent être fournies pour l'ensemble du système ou uniquement pour l'application ou des sous-composants comme les lecteurs.

La gestion des comptes utilisateurs dans l'environnement AC30 est limitée au compte admin, l'accès en tant que root est exclu. Le compte update remplit une fonction spécifique : ses droits d'accès sont limités à un emplacement unique, utilisé pour le mécanisme de mise à jour.

La connexion aux unités de lecture se fait via une interface série RS485. Sur les modèles 92 00 / 92 30, 2 unités de saisie supplémentaires peuvent être connectées par câble coaxial. Les protocoles utilisés par ces connexions sont propriétaires. Le chiffrement de la communication série est actuellement en développement et sera disponible en option dans les versions à venir.

Le niveau de sécurité pour la protection du contenu des médias est déterminé par la technologie de médias choisie par l'exploitant de l'installation.

Serveur Web

L'application B-Client AC30 dispose d'un serveur Web intégré qui assure la mise à disposition de ce qu'on appelle l'interface de service. L'interface de service permet principalement d'administrer par navigateur la configuration réseau, la date et l'heure ainsi que les mots de passe utilisateurs. Elle permet également d'accéder aux données de diagnostic.

- L'accès aux pages de l'interface de service est uniquement possible via https. Pour cela, on utilise un certificat auto-signé généré par dormakaba (gestionnaire d'accès), à qui la confiance doit être initialement accordée. Les certificats auto-signés ne sont pas des certificats dangereux. L'utilisateur doit confirmer par lui-même qu'il fait confiance à cette connexion
- L'interface de service ne permet pas d'accéder directement à des fichiers sensibles
- Le serveur Web est constamment maintenu en état sûr
- L'utilisateur root n'est pas utilisable
- Lors de la première connexion, l'utilisateur est obligé de modifier le mot de passe par défaut. Des règles de mot de passe doivent être respectées (lettres minuscules/majuscules, chiffres et caractères spéciaux)

Serveur SSH

Le système Linux fournit un serveur SSH. Il permet d'accéder au système de fichiers et à une console SSH, ce qui est particulièrement utile pour obtenir rapidement des données à des fins de diagnostic. Un logiciel de communication hôte, par exemple B-COMM, permet de lire et d'écrire très rapidement les fichiers de paramètres dans l'appareil via la connexion SSH.

- L'accès s'effectue exclusivement via une authentification par un fichier clé privé qui peut être géré par l'utilisateur final ou, par exemple, par le logiciel de communication hôte
- À partir de la version de B-COMM 5.1, la fonctionnalité de gestion des clés (SSH) est prise en charge en standard.

  L'interface de service permet de réinitialiser le gestionnaire d'accès sur les paramètres d'usine. Ceci réinitialise également les clés SSH
- Le serveur SSH est constamment maintenu en état sûr
- Là aussi, l'accès est impossible pour l'utilisateur root

Communication hôte

- La communication avec le système hôte peut être réalisée via différents protocoles.
- La communication avec le système hôte peut être chiffrée en option

Matériel

- Les appareils sont dotés de branchements pour les connexions de communication et de contacts d'entrée et de sortie pour enregistrer les données des capteurs sur l'état des portes et la surveillance des franchissements. Le nombre de contacts dépend du type de matériel employé
- Selon le type de lecteur employé, il est également possible d'utiliser des contacts du lecteur

Un 92 00 dispose de contacts directement accessibles ; ces appareils doivent donc être installés dans des zones sécurisées. Le niveau de sécurisation contre les accès non autorisés peut être accru par un montage dans un boîtier verrouillable, mais relève en principe de la responsabilité de l'exploitant. Les appareils à boîtier fermé, tels que le 92 90 ou le 92 30, disposent d'un contact anti-sabotage interne qui déclenche un message d'alarme dès que le boîtier est ouvert.

- Les appareils ne disposent pas d'une interface de débogage
- L'exploitation du logiciel d'appareil nécessite une licence qui est associée à l'adresse MAC de l'interface réseau de l'appareil et n'est donc pas transmissible
- Directives Security
- Répond aux exigences du RGPD

Mesures de sécurité recommandées pour les clients

Outre les mesures de sécurité fournies par dormakaba et/ou Linux, le client doit également jouer un rôle actif pour assurer une sécurisation optimale de l'ensemble du système :

- Dans la mesure du possible, installez le gestionnaire d'accès dans un environnement sécurisé
- Désactivez le serveur Web et le serveur SSH après la mise en service s'ils ne sont pas requis pour l'exploitation
- Activez uniquement le serveur Web et le serveur SSH en cas de besoin
- Limitez l'accès au réseau en appliquant des règles de pare-feu Il n'est pas nécessaire d'autoriser une connexion entrante vers le gestionnaire d'accès dormakaba depuis l'extérieur de votre réseau d'entreprise
- Appliquez des règles de mots de passe pour le gestionnaire d'accès et modifiez tous les mots de passe utilisateur, phrases-codes et fichiers de clés standard

Authentification réseau IEEE 802.1X

Le gestionnaire d'accès peut être intégré dans des réseaux LAN protégés par IEEE-802.1X.
Pour cela, le gestionnaire d'accès peut être configuré comme supplicant IEEE 802.1X avec les procédures d'authentification courantes (EAP MD5 et EAP PEAPv0/ MSCHAPv2).

Le B-Client AC30 est conforme à la norme IEC 60839-11-1, niveau de sécurité 3

La norme IEC 60839-11-1 décrit les exigences générales applicables au fonctionnement des installations de contrôle d'accès employées dans les applications de sécurité.

La fonctionnalité minimale, les exigences de performances et les procédures de contrôle pour les installations et appareils électroniques de contrôle d'accès employés pour l'accès physique (entrée et sortie) à l'intérieur et à la périphérie des bâtiments et zones protégées font également partie de la norme, ainsi que les exigences minimales en matière d'environnement et de compatibilité électromagnétique applicables aux appareils d'une installation de contrôle d'accès selon son niveau.

Le B-Client AC30 remplit ces critères pour le niveau de sécurité 3.

Avez-vous des questions ? Nous serons ravis de vous accueillir et de vous conseiller.

dormakaba France | 2-4 rue des Sarrazins | FR-94046 Créteil cedex | T +33 1 41 94 24 00 | marketing.fr@dormakaba.com | www.dormakaba.fr
dormakaba Belgium N.V. | Monnikenwerve 17-19 | BE-8000 Brugge | T +32 50 45 15 70 | info.be@dormakaba.com | www.dormakaba.be
dormakaba Luxembourg S.A. | Duchscherstrooss 50 | LU-6868 Wecker | T +352 26710870 | info.lu@dormakaba.com | www.dormakaba.lu
dormakaba Suisse SA | Chemin de Budron A5 | CH-1052 Le Mont-sur-Lausanne | T +41 848 85 86 87 | info.ch@dormakaba.com | www.dormakaba.ch