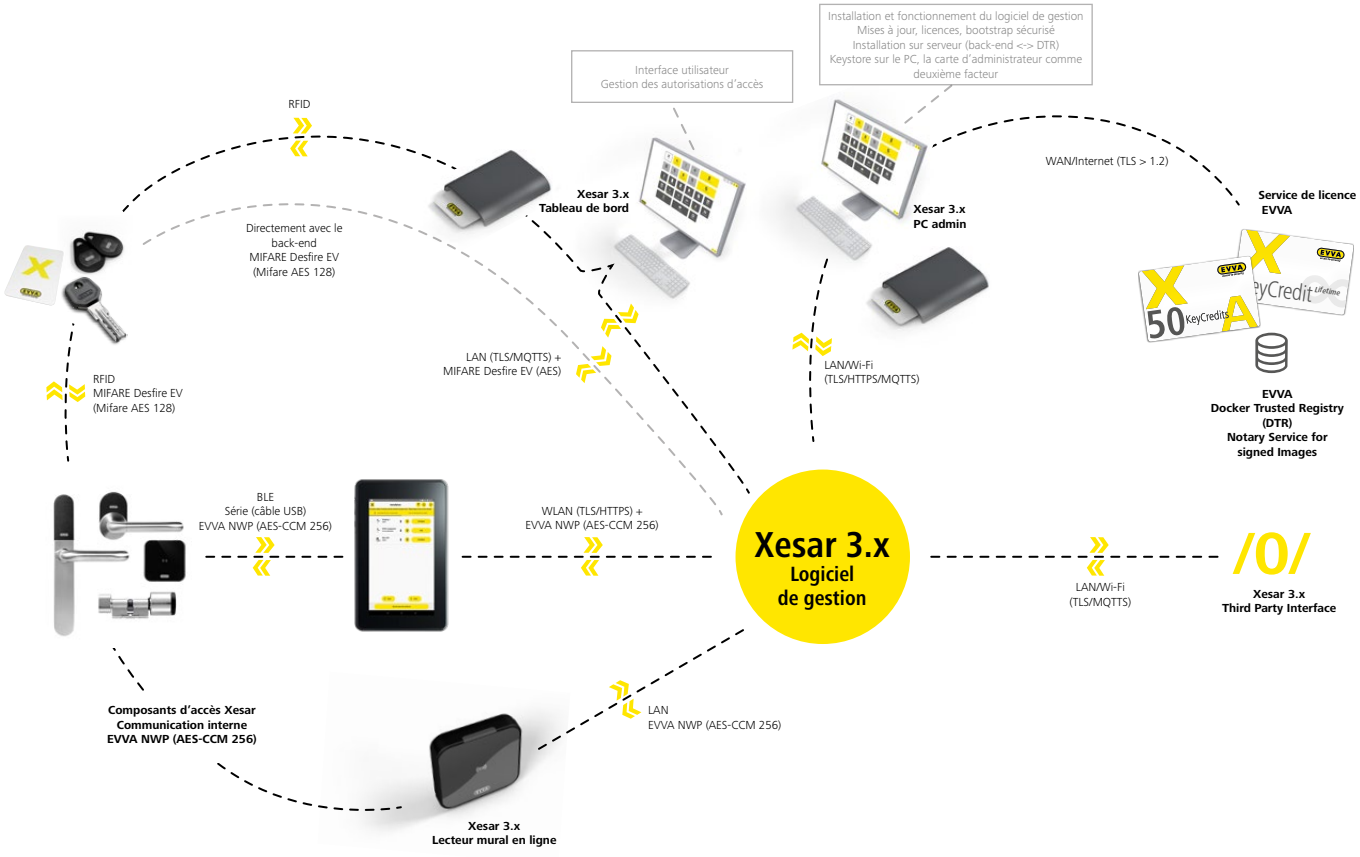
Xesar, le concept de sécurité étendu.

Aperçu des principales exigences de sécurité d'un système de contrôle d'accès Xesar

Cybersécurité Xesar



Supports d'accès (Xesar 3)

Interface et communication

Pour la communication entre les composants d'accès et les supports d'accès, on utilise toujours le procédé de cryptage MIFARE AES avec AES 128 bits.

- La clé d'application pour l'autorisation d'accès est générée selon une procédure sécurisée lors de l'installation de Xesar. Il s'agit d'un secret client qui n'est pas connu d'EVVA.
- Elle est uniquement enregistrée sous forme cryptée dans l'installation du service de sécurité sous forme persistante.
- Avec le procédé MIFARE utilisé, une session avec sa propre clé générée aléatoirement est ouverte pour chaque interaction.

Mémoire de données

Xesar utilise exclusivement des supports d'accès sécurisés avec une mémoire de données protégée

- Mifare Desfire EV1 avec certification EAL4+ ou
- Mifare Desfire EV2/EV3 avec certification EAL5+

Consignes de sécurité

- Afin d'éviter toute manipulation, le premier ajout d'un support d'accès à une installation Xesar ne doit être effectué que par un utilisateur autorisé à l'aide de la station d'encodage.
- La carte de construction est identique dans le monde entier et peut être utilisée partout pour l'accès aux composants d'accès Xesar en état de livraison ou en mode chantier. Par conséquent, elle ne permet d'effectuer aucun contrôle d'accès.
- Un support d'accès avec autorisation de passe général ne peut être remis qu'à titre exceptionnel et à des personnes de confiance. Motif : un support d'accès avec ce profil d'autorisation a
  - une durée de validité illimitée (pour la durée de validité maximale, voir le manuel)
  - Accès à tous les composants d'accès de l'installation, même s'ils ne sont ajoutés/créés qu'après la délivrance de ce support.

Un support d'accès avec autorisation de passe général doit être conservé dans un endroit sûr en dehors de l'installation sécurisée afin de permettre l'accès à l'installation en cas d'urgence.

Logiciel de gestion

Livraison

- Tous les composants numériques du système livrés par EVVA sont pourvus d'une signature de code valide et horodatée.
- Interface et communication
- Toute communication avec la gestion Xesar est sécurisée par TLS > 1.2 ; une liste des algorithmes TLS autorisés se trouve sur Cipher Suites.
  - pour la gestion de l'installation par plusieurs utilisateurs via l'accès par navigateur
  - pour la connexion du Periphery Manager (stations d'encodage dispersées)
  - pour l'interaction des services faisant partie intégrante de l'installation
  - pour l'interaction avec l'interface du système tiers

Authentification

De manière générale, les directives OWASP ont été suivies là où cela est judicieux.

- L'authentification pour la gestion de l'installation via l'accès par navigateur est protégée par mot de passe :
  - Le premier mot de passe administrateur est généré de manière aléatoire lors de l'installation (pas de mot de passe par défaut)
  - Tous les mots de passe créés doivent avoir une longueur minimale et s'accompagner d'un indicateur de qualité (zxcvbn : Low-Budget Password Strength Estimation)
  - Les mots de passe ne sont jamais enregistrés en texte clair (BCrypt)
  - Les échecs d'authentification sont délibérément traités de manière générique
- L'authentification sur les interfaces de service est basée sur des certificats avec mTLS :
  - pour la connexion du Periphery Manager
  - dans le cas de connexions internes de services qui font partie intégrante de l'installation
  - lors de la connexion à l'interface du système tiers via le broker MQTT ; un jeton est également utilisé pour l'autorisation interne

Autorisation
- Dans la gestion Xesar, des droits d'utilisateur peuvent être définis pour l'autorisation via des groupes d'utilisateurs, ces droits pouvant ensuite être facilement attribués aux utilisateurs respectifs
- Les actions respectives d'un utilisateur sont enregistrées dans le système
- L'autorisation et la journalisation s'appliquent également pour les utilisateurs de l'interface

Mémoire de données
- Toutes les données sensibles (par exemple, nomenclatures, mots de passe) sont exclusivement enregistrées par le biais du service de sécurité de l'installation (coffre-fort) et uniquement sous forme cryptée.
- Lors du bootstrap de l'installation, deux facteurs (carte d'administrateur et keystore crypté enregistré sur le PC admin) permettent d'« ouvrir » le coffre-fort pour l'exploitation.
  - Les données non sensibles de l'installation et de la configuration sont enregistrées dans une base de données qui n'est pas cryptée (voir consignes de sécurité).
  - Grâce à la conception architecturale du logiciel de gestion, qui sépare les modèles de lecture et d'écriture, toutes les modifications sont enregistrées sous forme de séquence d'événements (CQRS-ES). Cela augmente la traçabilité et complique la manipulation des bases de données.

Consignes de sécurité
- Seuls les artefacts non modifiés fournis par EVVA doivent être utilisés pour l'installation du système. L'authenticité et l'intégrité de tous les artefacts fournis par EVVA peuvent être vérifiées au moyen d'une signature.
- Le client est responsable de l'exploitation sécurisée du logiciel de gestion Xesar ;
  - L'accès (authentification et autorisation) à l'environnement serveur doit être sécurisé afin de prévenir toute manipulation aisée des bases de données non sensibles de l'installation et de la configuration.
  - L'accès au logiciel de gestion de l'installation doit être réservé aux utilisateurs clairement authentifiés et autorisés.
  - Les comptes d'installation configurés ne doivent être utilisés que lors de l'installation et ensuite uniquement dans des cas exceptionnels (par exemple, réinitialisation du mot de passe, récupération).
- La fiche de sécurité de l'installation générée lors de l'installation à des fins de récupération ne doit être conservée que sous forme imprimée dans un endroit sûr (par exemple, coffre-fort).

Informations concernant la protection des données
- Lors de l'activation de l'enregistrement des données d'accès à caractère personnel, les dispositions de protection des données spécifiques au pays doivent être connues et respectées.
- Une résolution automatique de la référence personnelle des données d'accès peut être configurée en conséquence via le logiciel de gestion. Pour connaître les possibilités et la procédure dans le logiciel, voir le manuel.

Composant d'entretien (tablette Xesar)

Interface et communication
- Pour ajouter un nouveau composant Xesar à une installation Xesar, la clé de l'installation est transportée de manière cryptée à l'aide du procédé de cryptage AEAD et d'une clé AES 128 bits. Cette clé est dérivée d'un code PIN en tant que deuxième facteur non stocké sur l'appareil à l'aide d'une fonction de dérivation de clé cryptographique (KDF, AES-CMAC-PRF-128).
- Les données de configuration des composants de l'installation sont transportées de manière cryptée à l'aide du procédé de cryptage AEAD et de la clé AES 256 bits spécifique au composant (voir également Cybersécurité des composants Xesar).

Consignes de sécurité
- La tablette d'entretien fournie par EVVA ne doit être utilisée qu'à des fins d'entretien de l'installation.
- Aucune autre application ne doit être installée sur cette tablette.
- Les données de configuration nécessaires à l'installation de nouveaux composants Xesar sont protégées par un code PIN. Celui-ci doit :
  - être configuré dans les paramètres du système après l'installation afin que la valeur par défaut (0000) ne soit pas utilisée par le système ;
  - être communiqué uniquement à des personnes connues et dignes de confiance.
- Il n'est pas nécessaire de s'enregistrer auprès de Google pour utiliser Xesar.
- L'activation de la communication réseau (Wi-Fi) ne doit avoir lieu que si nécessaire et un réseau privé sécurisé doit être utilisé (c.-à-d. pas Internet).
- Seules les mises à jour du système recommandées et testées par EVVA doivent être installées.

Composants d’accès

Interface et communication

- Pour la communication avec le composant, on utilise toujours un procédé de cryptage AEAD avec des clés AES 256 bits (radio et série) (AES-CCM).
- La clé de communication est générée spécifiquement pour chaque composant dans le logiciel de gestion Xesar selon un procédé sécurisé et constitue un secret client qui n’est pas connu d’EVVA.
- Une fois installée, seul l’utilisateur peut effectuer des modifications concernant l’état ou la configuration des composants
- La nomenclature peut être mise à jour sur le composant avec la protection correspondante (authentification, transmission cryptée)
- La taille de la clé et les procédés symétriques utilisés compliquent les attaques par force brute même pour le temps post-quantique. Dans le cas de composants alimentés par batterie, l’alimentation ne permettra en outre que peu d’essais en raison de la combinatoire, en particulier sur la ligne radio.

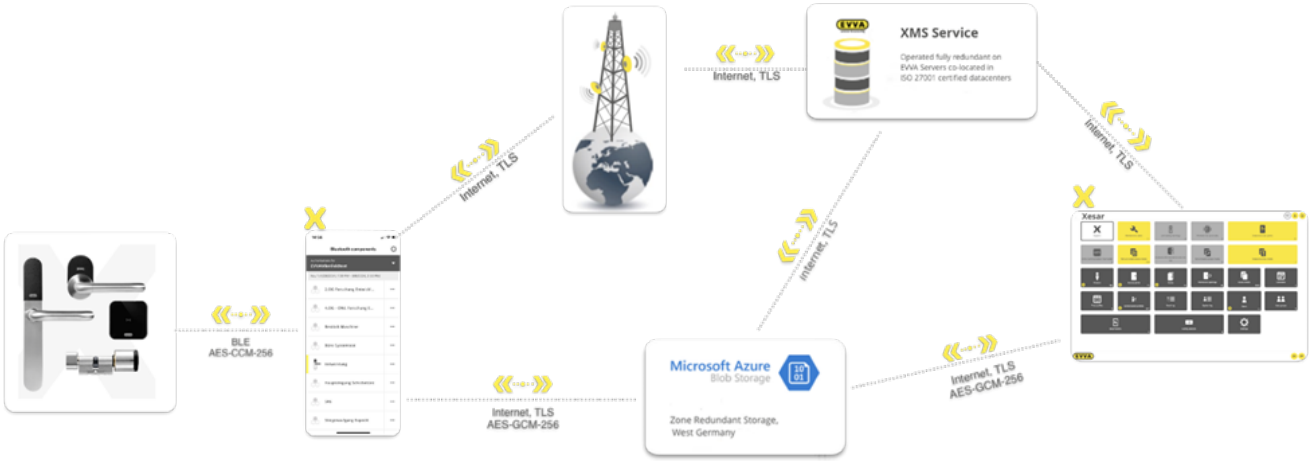
Mémoire de données

- La nomenclature, la configuration sensible et le code d’application sont enregistrés sur le microcontrôleur (MC) respectif avec la meilleure protection MC possible (NVRAM, mémoire flash interne)
  - Famille PIC24 : General Segment Protection and Code Segment Protection (Family Datasheet, 29.4)
  - NRF52 : Access port protection controlled by hardware (APPPROTECT)
  - Le boîtier protège contre un accès non destructif aux MC (voir également Sécurité mécanique des composants Xesar)
- Les données de l’installation sont enregistrées sur le composant dans une mémoire (EEPROM ou flash) et protégées par un procédé cryptographique à l’aide d’une clé AES 128 bits (AES-CMAC).

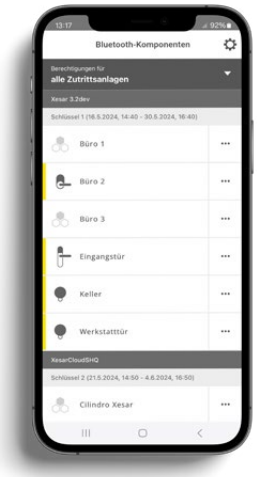
Firmware et mise à jour

- Le firmware existant est chargé en usine à l’aide d’un bootloader qui ne peut plus être modifié. Il peut être mis à jour par le bootloader avec une sauvegarde correspondante.
- Les packs-firmware d’EVVA sont signés selon un procédé asymétrique (RSA-SHA256) et délivrés à la gestion Xesar avec un cryptage symétrique. La chaîne de certificats est vérifiée tant dans le logiciel de gestion que dans l’application d’entretien.
- Pour la mise à jour dans l’installation, on utilise un procédé de cryptage AEAD avec des clés AES 256 bits (AES-CCM). La clé de mise à jour du firmware est générée spécifiquement pour l’installation par le logiciel de gestion Xesar selon un procédé sécurisé et constitue un secret client qui n’est pas connu d’EVVA.
- Une fois dans l’installation, seul l’utilisateur peut effectuer une mise à jour du firmware des composants
- Dans le cas du firmware pour les MC NRF52, il est également possible :
  - de signer le firmware avec une méthode asymétrique (RSA-SHA256, 2048 bit Key) et de le vérifier directement sur le MC.
  - le firmware est livré sécurisé par un procédé de cryptage AEAD (AES-CCM) à l’aide d’une clé AES 256 bits.
- Le firmware des composants nouvellement intégrés dans une installation est automatiquement mis à jour vers la dernière version de firmware connue du logiciel de gestion ou de l’application d’entretien.
- Les notifications et la vérification des mises à jour disponibles par EVVA sont prises en charge et rendues possibles par l’Installation Manager Xesar et l’application d’entretien Xesar.

Aperçu du blocage mobile



Application mobile Xesar (application Xesar)



Interfaces et communication

- Toute communication avec le XMS ou le stockage cloud est sécurisée par TLS.
- Toutes les transactions entre une installation Xesar et l'application Xesar sont authentifiées de bout en bout sur la base d'un protocole d'échange de clés (X25519), d'une fonction de dérivation de clé et de codes d'authentification de message (HKDF-SHA256).
- Toute communication entre un composant Xesar et l'application mobile pour la transmission des données d'accès est protégée contre la lecture et cryptée au sein d'une session
- Enregistrement des données
- Dans la mesure où le terminal le prend en charge, les nomenclatures sensibles sont stockées sur des mémoires sécurisées mises à disposition par le matériel
  - Android : StrongBox si disponible, affecté à l'appareil, sauvegarde cloud désactivée par manifeste
  - iOS : trousseau de clés CryptoKit, utilisable uniquement sur l'appareil, synchronisation iCloud avec le profil d'approvisionnement désactivée
- Toutes les données sont enregistrées dans une base de données cryptée supplémentaire sur le terminal mobile
- Les données d'accès d'une installation Xesar sont déjà cryptées et ne peuvent pas être décryptées, inspectées ou manipulées par l'application mobile.
- Consignes de sécurité
- L'application mobile doit être téléchargée dans sa forme originale signée par EVVA exclusivement à partir d'un store officiel (par ex. Google Play, Apple App Store)
- EVVA recommande à tous les utilisateurs de l'application mobile d'utiliser :
  - des terminaux équipés de mémoires de sécurité matérielles ;
  - un cryptage de la mémoire ;
  - la protection du terminal avec un mot de passe, un code PIN ou une connexion biométrique

.

Service d'assistance mobile Xesar (XMS)

Centre de données

- Le service est exploité sur des serveurs EVVA hébergés par colocation dans des centres de données certifiés ISO 27001 et physiquement séparés en Autriche.
- Toutes les ressources nécessaires sont redondantes et évolutives horizontalement
- Tous les terminaux de service sont sécurisés par un pare-feu avec des mécanismes de protection de pointe (IDS, IPS et DoS).

Interfaces et communication

- Toute communication avec le XMS est sécurisée par TLS > 1.2.
  - Broker MQTT (mqtts://MQTT.akx.cloud:443)
    - Pour la liste des certificats TLS autorisés, voir le broker MQTT

- Terminal REST (https://mss.akx.cloud)
  - Pour l'authentification et l'autorisation du logiciel de gestion Xesar
  - Liste des algorithmes TLS REST autorisés

› Le XMS est exclusivement une « station relais » entre une installation Xesar et un smartphone enregistré avec l'application Xesar
- Toutes les transactions entre une installation Xesar et un smartphone enregistré avec l'application Xesar sont authentifiées de bout en bout sur la base d'un protocole d'échange de clé (X25519), d'une fonction de dérivation de clé et de codes d'authentification de message (HKDF-SHA256).
- Les transactions ne peuvent donc jamais être initiées ou manipulées par le XMS ou d'autres installations Xesar.

Mémoire de données, sauvegarde de données et récupération après sinistre

› Seules les données nécessaires à la fonctionnalité sont enregistrées
› Les données ne sont enregistrées temporairement que pour une durée limitée et sous forme cryptée pour le transit entre l'installation Xesar et un smartphone enregistré à cet effet doté de l'application Xesar.
- Enregistrement : 48 h
- Mise à jour des autorisations : 16 jours

› Les données d'accès fournies par une installation Xesar sont cryptées avant la transmission sur site uniquement pour le smartphone enregistré avec l'application Xesar (AES-GCM-256). Le service XMS, EVVA ou d'autres installations Xesar ne peuvent pas accéder à ces données.
› Les données sont actuellement stockées de manière redondante dans des centres de données cloud certifiés en Allemagne occidentale. L'architecture est conçue pour que le stockage ciblé puisse être étendu à d'autres régions/zones.
› En cas de catastrophe affectant une zone entière, l'enregistrement peut être redirigé et la mise à jour des accès peut à nouveau être effectuée à l'aide de la gestion Xesar sur site.
› Des mesures organisationnelles ont été prises pour garantir un accès limité et autorisé aux données stockées
- Droits d'accès strictement contrôlés pour le personnel de service et d'assistance chez EVVA
- Gestion stricte des secrets pour le déploiement et l'exploitation (SecDevOps)

Surveillance et alarmes

› Le fonctionnement des composants de service est surveillé en permanence et le personnel opérateur est alerté en cas d'écarts.
- Les réglementations mises en place à cet effet sont vérifiées et améliorées en permanence.

› Les composants de service font l'objet d'une surveillance CVE continue et sont mis à jour rapidement en cas de scénarios de menace.

Informations concernant la protection des données

› Le développement a été réalisé selon le principe Privacy by Design
› Les clients ou les données à caractère personnel d'une installation Xesar ne sont jamais enregistrés dans le contexte du XMS
› Les données transmises par une installation Xesar à un smartphone enregistré avec l'application Xesar
- ne contiennent jamais de données à caractère personnel
- ne peuvent pas être consultées par le service XMS, EVVA ou d'autres installations Xesar
- les numéros de téléphone des terminaux mobiles sont utilisés exclusivement pour appeler le fournisseur de services SMS, mais ne sont pas enregistrés par le service XMS.

Caractéristiques de sécurité mécaniques des composants d'accès Xesar

Garniture

Aperçu des caractéristiques de sécurité mécaniques d'une garniture Xesar.

Certifications existantes

› EN 1634-1 : 90 minutes
› EN 1634-3
› EN 179
› EN 1906
› Avec plaque stabilisatrice DIN 18257 : ES0
› ÖNORM 3859 : 90 minutes

Protection contre les conditions environnementales

› Protection IP52 (IP55 avec joint collé) contre la pénétration de poussières néfastes et de jets d'eau à l'état monté
› Module électronique avec vernis de protection contre l'oxydation due à la condensation
› Conditions d'utilisation : -20 °C - +55 °C
› 3 piles dans la zone intérieure protégée

Sécurité physique
› Vissage multiple
  • Protection mécanique contre les manipulations
  • Béquille extérieure tournant librement

Béquille

Aperçu des caractéristiques de sécurité mécaniques d'une béquille Xesar.

Certifications existantes
› EN 1634-1 : 90 minutes
› EN 179
› EN 1906
› ÖNORM 3859 : 90 minutes
› Homologation CE

Protection contre les conditions environnementales
› Plage d'humidité : 90 % à 0 °C
› Température ambiante intérieure : +5 °C à +50 °C
› IP40

Sécurité physique
› Béquille extérieure tournant librement

Cylindre

Certifications existantes
› EN 5684 16B30D3D
› SKG***
› SSF 3522 pour les profils scandinaves
› Certification de protection incendie selon EN 1634 (90 min)
› Certification antipanique selon EN 179/1125
› ÖNORM B 5351:2011 WMZ6-BZ
› Homologation CE

Protection contre les conditions environnementales
› IP65 contre la pénétration nocive de poussière et de jets d'eau lors d'un montage conforme aux instructions de montage Xesar
› Module électronique avec vernis de protection contre l'oxydation due à la condensation
› Plage d'humidité : 90 % à 0 °C
› Conditions d'utilisation : -20 °C - +55 °C
› 2 piles parallèles pour une meilleure stabilité de l'alimentation en tension

Sécurité physique
› Bouton extérieur tournant librement
› Protection anti-perçage
› Protection anti-arrachage
› Frein de rotation contre les attaques à l'aide d'une broche haute fréquence
› Point de rupture défini sur le filetage du bouton extérieur pour protéger le rotor contre les attaques mécaniques et pour parer aux attaques de snapping
› Outil mécanique spécial pour le montage et le démontage du bouton du cylindre

Sécurité architecturale
› Le cylindre Xesar se compose d'un bouton de cylindre et d'un module de cylindre qui se trouve derrière la protection anti-perçage.
› Le bouton et le module sont reliés entre eux par une sécurité cryptographique :
  • la libération s'effectue exclusivement dans la zone mécaniquement « sécurisée »
  • un simple remplacement du bouton empêche tout accès non autorisé

Lecteur mural (en ligne, hors ligne)

Certifications existantes
› Homologation CE

Protection contre les conditions environnementales
› Plage d'humidité 90 % à 0 °C
› Température ambiante -25 °C jusqu'à +70 °C
› Indice de protection IP65

Sécurité physique
› Partie avant en verre véritable

Sécurité architecturale
› Le lecteur mural Xesar se compose d'une unité de lecture murale et d'une unité de contrôle du lecteur mural se trouvant dans une zone sécurisée.
› Le lecteur mural en ligne se compose d'une unité de lecture murale et d'une unité de contrôle en ligne se trouvant dans une zone sécurisée.
› L'unité de lecture et l'unité de contrôle sont reliées entre elles par une sécurité cryptographique :
  • la libération s'effectue exclusivement dans la zone « sécurisée »
  • un simple remplacement du lecteur mural empêche tout accès non autorisé

Autres caractéristiques générales de sécurité

Composants d'accès (lieu de montage) :
› Affectation des lieux de montage aux zones et autorisation pour les zones
› Liste noire pour les supports d'accès bloqués
› Fonction Delete-Key – Désactivation des supports d'accès bloqués figurant sur la liste noire du composant
› Modes Office (ouvertures permanentes de composants)
  • Ouverture permanente manuelle de composants
  • Ouverture permanente automatique, temporisée entre deux moments définis (début et fin)
  • Fin automatique de l'autorisation permanente à des moments définis où les autorisations permanentes manuelles sont également terminées (fin uniquement)
  • Mode Shop : Autorisation permanente automatique, uniquement activée après un accès autorisé
› Journal des événements pour les événements d'accès, de refus et de mode Office
› Restriction temporelle pour les autorisations d'accès

Supports d'accès :
› Le réseau virtuel permet le transport de données via des supports d'accès ou leur utilisation par des personnes dans l'installation.

Logiciel de gestion :
› Profils d'autorisation définis pour les utilisateurs avec différents droits d'utilisateur (groupe d'utilisateurs)
› Vues du panneau de contrôle définies pour les utilisateurs par droits d'utilisation (groupe d'utilisateurs)
› État de l'équipement sur le panneau de contrôle
  • Composants :
    - mises à jour nécessaires du firmware
    - mises à jour nécessaires de la configuration
    - affichage de l'état de charge de la pile
    - état en ligne en temps réel des lieux de montage avec composant EVVA en ligne
    - état de la connexion
    - état des contacts de porte
  • Composants d'accès et supports :
    - lieux de montage non sûrs
    - supports d'accès nécessitant une mise à jour
    - supports d'accès bloqués non sûrs
    - libérations effectuées avec des supports d'accès bloqués
› Protocole système pour la traçabilité des modifications de la configuration dans le logiciel de gestion

I.X.SJARC.ID.INFBL.SFR.LN 25R1