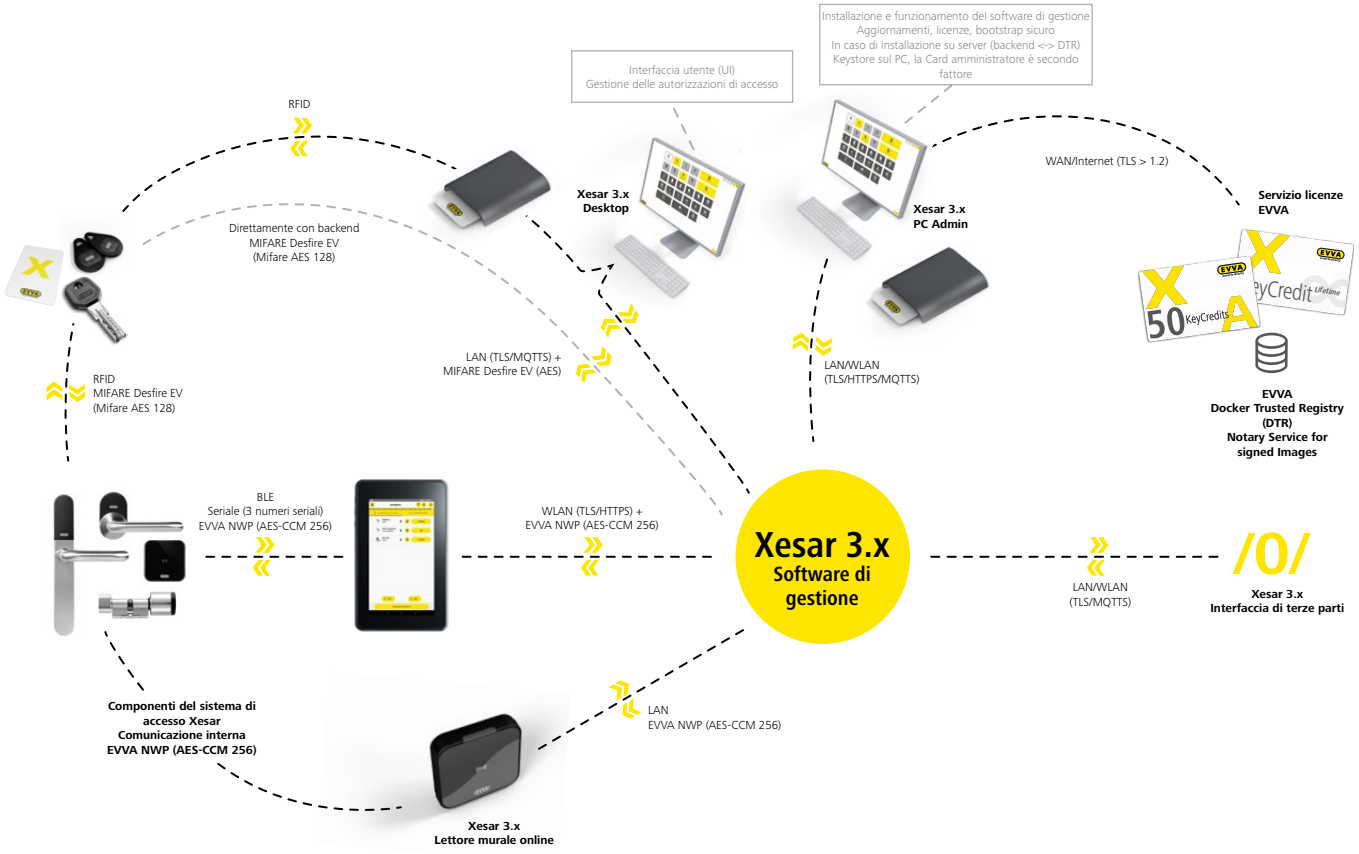
Concetto di sicurezza di Xesar

Panoramica delle principali caratteristiche tecniche di sicurezza di un sistema di accesso Xesar

Sicurezza informatica Xesar



Tag o card (Xesar 3)

Interfaccia e comunicazione

Per le comunicazioni tra componenti di accesso e tag o card viene utilizzato in tutti i casi il metodo di codifica MIFARE AES con crittografia AES a 128 bit.

- La chiave dell'applicazione per l'autorizzazione di accesso viene generata durante l'installazione di Xesar con una procedura sicura. È un segreto del cliente e EVVA non ne viene a conoscenza.
- Viene memorizzata in forma crittografata e persistente solo nell'installazione del servizio di sicurezza.
- Con la procedura MIFARE, per ogni interazione viene utilizzata una sessione con una propria chiave generata in maniera casuale.

Memorizzazione dei dati

Per Xesar vengono utilizzati esclusivamente tag o card sicuri con memorizzazione protetta dei dati:

- Mifare Desfire EV1 con certificazione EAL4+ oppure
- Mifare Desfire EV2/EV3 con certificazione EAL5+.

Indicazioni di sicurezza

- Per evitare manipolazioni, la prima aggiunta di un elemento di accesso a un impianto Xesar deve essere eseguita solo da un utente autorizzato in un luogo protetto con l'ausilio della stazione di codifica.
- L'elemento in modalità cantiere è identico in tutto il mondo e può essere utilizzato ovunque per l'accesso ai componenti Xesar in stato di fabbrica o in modalità cantiere. Pertanto non è possibile alcun controllo degli accessi.
- Un elemento di accesso con autorizzazione di chiave generale può essere consegnato solo in casi eccezionali e a persone fidate. Motivo: un elemento di accesso con questo profilo di autorizzazione ha:
  - una durata di validità illimitata (per la durata massima vedere il manuale);
  - accesso a tutti i componenti dell'impianto, anche se questi vengono aggiunti/creati solo dopo l'emissione di questo elemento di accesso.

Un elemento di accesso con autorizzazione di chiave generale deve essere conservato in un luogo sicuro all'esterno dell'impianto protetto, in modo da consentire l'accesso all'impianto in caso di emergenza.

Software di gestione

Consegna

- Tutti i componenti digitali del sistema forniti da EVVA sono dotati di una firma a codice valida e con marca temporale.
- Interfaccia e comunicazioni
- Le comunicazioni con il sistema di gestione Xesar sono protette con TLS > 1.2 (un elenco degli algoritmi TLS consentiti è disponibile nelle suite di cifratura):
  - per la gestione dell'impianto da parte di più utenti grazie all'accesso tramite browser;
  - per il collegamento del gestore di periferiche (stazione di codifica distribuita);
  - per l'interazione dei servizi facenti parte dell'impianto;
  - per l'interazione con l'interfaccia del sistema di terze parti.

Autenticazione

Sono state generalmente seguite, laddove opportuno, le linee guida OWASP.

- L'autenticazione per la gestione dell'impianto tramite accesso da browser è protetta da password:
  - La prima password dell'amministratore viene generata in modo casuale durante l'installazione (nessun valore predefinito).
  - Tutte le password create devono avere una lunghezza minima e un indicatore di qualità (zxcvbn: Low-Budget Password Strength Estimation).
  - Le password non vengono mai memorizzate come testo in chiaro (BCrypt).
  - Gli errori di autenticazione vengono intenzionalmente gestiti in modo generico.
- L'autenticazione sulle interfacce di servizio è basata su certificato con mTLS:
  - per il collegamento del gestore di periferiche;
  - in caso di collegamenti interni di servizi che sono parte integrante dell'impianto;
  - in caso di collegamento con l'interfaccia di sistema di terze parti tramite il broker MQTT; in questo caso viene aggiunto anche un token per l'autorizzazione interna.

Autorizzazione
› Nella gestione Xesar è possibile definire i diritti utente per l'autorizzazione tramite gruppi utenti che possono quindi essere facilmente assegnati ai rispettivi utenti.
› Le azioni degli utenti vengono registrate nel sistema.
› L'autorizzazione e la registrazione funzionano anche per gli utenti dell'interfaccia.

Memorizzazione dei dati
› Tutti i dati sensibili (ad es. materiale crittografato, password) vengono archiviati esclusivamente nell'installazione del servizio di sicurezza (Vault) e memorizzati solo in forma crittografata.
› Durante il bootstrap dell'installazione, il Vault viene "aperto" per il funzionamento tramite due fattori (Card amministratore e keystore cifrato memorizzato su AdminPC).
  • I dati non sensibili dell'installazione e della configurazione vengono memorizzati in un database non crittografato (vedere Indicazioni di sicurezza).
  • Grazie al design dell'architettura del software di gestione, in cui i modelli di lettura e scrittura sono separati, tutte le modifiche vengono salvate come una sequenza di eventi (CQRS-ES). Ciò aumenta la tracciabilità e rende più difficile la manipolazione dei database.

Indicazioni di sicurezza
› Per l'installazione del sistema devono essere utilizzati solo artefatti invariati forniti da EVVA. L'autenticità e l'integrità di tutti gli artefatti forniti da EVVA possono essere verificate tramite firma.
› Il cliente è responsabile del funzionamento sicuro del software di gestione Xesar:
  • L'accesso (autenticazione e autorizzazione) all'ambiente server deve essere protetto in modo che i database non sensibili dell'installazione e della configurazione non possano essere facilmente manipolati.
  • L'accesso alla gestione dell'impianto deve essere effettuato da utenti autenticati e autorizzati in modo univoco.
  • Gli account di installazione configurati dovrebbero essere utilizzati solo durante l'installazione e successivamente solo in casi eccezionali (ad es. reset della password, ripristino).
› Il documento di sicurezza impianto generato per i casi di ripristino durante l'installazione deve essere conservato solo in forma stampata in un luogo sicuro (ad es. cassaforte).

Avvertenze sulla tutela dei dati
› Quando si attiva la registrazione dei dati di accesso personali, è necessario conoscere e rispettare le disposizioni in materia di protezione dei dati specifiche del Paese.
› Tramite il software di gestione è possibile configurare la cancellazione automatica del riferimento personale nei dati di accesso. Consultare il manuale per le opzioni e le procedure del software.

Componente di manutenzione (tablet Xesar)

Interfaccia e comunicazione
› Per aggiungere un nuovo componente Xesar a un sistema Xesar, la chiave dell'impianto viene trasmessa crittografata con il metodo di crittografia AEAD e una chiave AES a 128 bit. Questa chiave viene derivata da un PIN come secondo fattore, non memorizzato sul dispositivo, tramite una funzione di derivazione delle chiavi crittografiche (KDF, AES-CMAC-PRF-128).
› I dati di configurazione dei componenti dell'impianto vengono trasmessi in modo crittografato con il metodo AEAD e la chiave AES a 256 bit, specifica per il componente, viene trasmessa crittografata (vedere anche Sicurezza informatica dei componenti Xesar).

Indicazioni di sicurezza
› Il tablet di manutenzione fornito da EVVA deve essere utilizzato esclusivamente per la manutenzione dell'impianto.
› Su questo tablet non devono essere installate altre applicazioni.
› Per l'inserimento di nuovi componenti Xesar, i dati di configurazione sono protetti tramite PIN. Il PIN deve:
  • essere configurato nelle impostazioni del sistema dopo l'installazione in modo che il sistema non utilizzi il valore predefinito (ad es. 0000);
  • essere condiviso solo con persone note e fidate.
› Per l'utilizzo di Xesar non è necessario registrarsi a Google.
› L'attivazione delle comunicazioni di rete (WLAN) deve avvenire solo se necessario e deve essere utilizzata una rete privata protetta (ossia non Internet)
› Installare solo gli aggiornamenti di sistema consigliati e testati da EVVA.

Componenti di accesso

Interfaccia e comunicazione

- Per le comunicazioni con il componente viene impiegato in tutti i casi (radio e seriale) un procedimento di crittografia AEAD con chiavi AES a 256 bit (AES-CCM).
- La chiave di comunicazione viene generata specificamente per ogni componente nel software di gestione Xesar con una procedura sicura ed è un segreto del cliente non noto a EVVA.
- Una volta inserita nell'impianto, solo l'utente può apportare modifiche allo stato o alla configurazione dei componenti.
- Il materiale crittografato può essere aggiornato sul componente con la relativa protezione (autenticazione, trasmissione crittografata).
- Gli attacchi brute force con procedure simmetriche non sono facili da portare a termine nemmeno nell'epoca post-quantistica grazie alla dimensione del codice di crittografia. Nel caso di componenti a batteria, inoltre, l'alimentazione consentirà di eseguire solo una piccola parte dei test necessari a causa del calcolo combinatorio, in particolare sul collegamento radio.

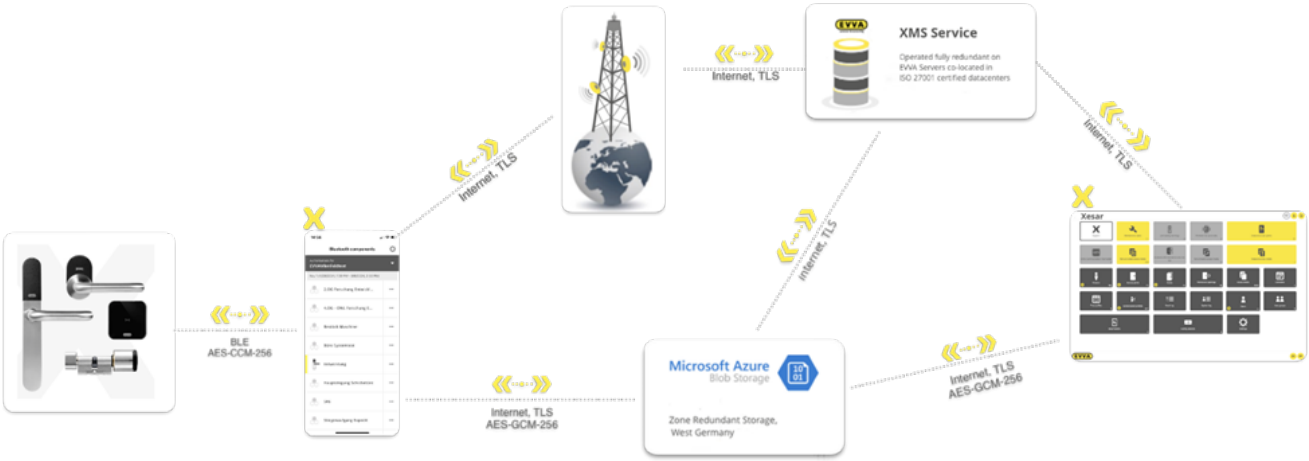
Memorizzazione dei dati

- Il materiale crittografato, la configurazione sensibile e il codice dell'applicazione vengono memorizzati sul rispettivo microcontroller (MC) con la migliore protezione MC possibile (NVRAM, memoria flash interna):
  - Famiglia PIC24: General Segment Protection e Code Segment Protection (Family Datasheet, 29.4);
  - NRF52: Access port protection controlled by hardware (APPPROTECT);
  - l'alloggiamento protegge dall'accesso non distruttivo ai microcontroller (vedere anche Sicurezza meccanica dei componenti Xesar).
- I dati dell'impianto vengono memorizzati in una memoria sul componente (EEPROM o Flash) e l'integrità è garantita dall'impiego di un processo crittografico con chiave AES a 128 bit (AES-CMAC).

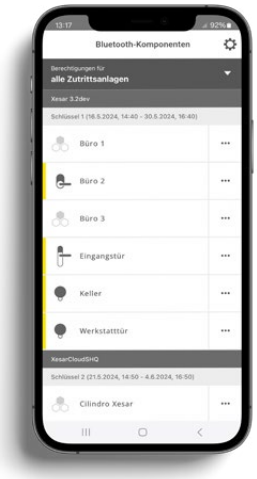
Firmware e aggiornamento

- Il firmware esistente viene caricato con un bootloader non più modificabile una volta uscito di fabbrica e può essere aggiornato dal bootloader con un'adeguata protezione.
- I pacchetti firmware di EVVA vengono firmati con una procedura asimmetrica (RSA-SHA256) e consegnati al sistema di gestione Xesar con una crittografia simmetrica. La catena di certificati viene verificata sia nel software di gestione che nell'applicazione di manutenzione.
- Per l'aggiornamento nell'impianto viene utilizzato un processo di crittografia AEAD con chiavi AES a 256 bit (AES-CCM). La chiave di aggiornamento del firmware viene generata dal software di gestione Xesar con una procedura sicura specifica per l'impianto ed è un segreto del cliente non noto a EVVA.
- Una volta inserita nell'impianto, solo l'utente può eseguire un aggiornamento del firmware sui componenti.
- Inoltre nel caso del firmware per microcontroller NRF52:
  - Il firmware è firmato con una procedura asimmetrica (RSA-SHA256, chiave a 2048 bit) e verificato direttamente sul microcontroller.
  - Il firmware viene fornito protetto con una procedura di crittografia AEAD (AES-CCM) che utilizza una chiave AES a 256 bit.
- Il firmware dei nuovi componenti inseriti in un impianto viene aggiornato automaticamente all'ultima versione nota al software di gestione o all'applicazione di manutenzione.
- Le notifiche e la verifica degli aggiornamenti disponibili da EVVA sono supportate e consentite dall'Installation Manager Xesar e dall'applicazione di manutenzione Xesar.

Panoramica della chiusura tramite dispositivo mobile



Applicazione mobile Xesar (app Xesar)



Interfacce e comunicazioni

- Tutte le comunicazioni con XMS o Cloud Storage sono protette da TLS.
- Tutte le transazioni tra un impianto Xesar e l'app Xesar vengono autenticate end-to-end sulla base di un protocollo di scambio crittografato (X25519), di una funzione di derivazione delle chiavi crittografiche e di codici di autenticazione tramite messaggi (HKDF-SHA256).
- Tutte le comunicazioni tra un componente Xesar e l'applicazione mobile per la trasmissione dei dati di accesso sono protette contro la riproduzione e crittografate all'interno di una sessione.
- Salvataggio dei dati
- Se supportato dal dispositivo, il materiale crittografato sensibile viene archiviato su memorie sicure messe a disposizione dall'hardware.
  - Android: StrongBox se disponibile, assegnata al dispositivo, backup su cloud disattivato dal file Manifest.
  - iOS: CryptoKit Keyring, utilizzabile solo sul dispositivo, sincronizzazione su iCloud con il profilo di provisioning disabilitata.
- Tutti i dati vengono memorizzati in un database ulteriormente crittografato sul dispositivo.
- I dati di accesso di un impianto Xesar sono già crittografati da quest'ultimo e non possono essere decrittografati, ispezionati o manipolati dall'applicazione mobile.
- Indicazioni di sicurezza
- L'applicazione mobile deve essere scaricata nella sua forma originale firmata da EVVA esclusivamente da uno store ufficiale (ad es. Google Play, Apple App Store).
- EVVA consiglia a tutti gli utenti dell'applicazione mobile di:
  - utilizzare dispositivi con memorie di sicurezza supportate da hardware;
  - utilizzare la crittografia della memoria;
  - proteggere il dispositivo tramite password, PIN o login biometrico.

Servizio di assistenza Xesar Mobile (XMS)

Datacenter

- Il servizio è gestito su server EVVA ospitati, tramite co-locazione, in data center certificati ISO 27001 e fisicamente separati in Austria.
- Tutte le risorse necessarie sono ridondanti e scalabili orizzontalmente.
- Tutti gli endpoint di servizio si trovano dietro un firewall dotato di meccanismi di protezione all'avanguardia (IDS, IPS e DoS).

Interfacce e comunicazioni

- Tutte le comunicazioni con XMS sono protette con TLS > 1.2.
  - Broker MQTT (mqtts://MQTT.akx.cloud:443)
    - Per l'elenco dei certificati TLS consentiti, vedere il broker MQTT
  - Endpoint REST (https://mss.akx.cloud)
    - Per l'autenticazione e l'autorizzazione del software di gestione Xesar
    - Elenco degli algoritmi TLS REST consentiti

- XMS è esclusivamente una "stazione relè" tra un impianto Xesar e uno smartphone registrato con l'app Xesar
  - Tutte le transazioni tra un sistema Xesar e uno smartphone registrato con l'app Xesar vengono autenticate end-to-end sulla base di un protocollo di scambio crittografato (X25519), di una funzione di derivazione delle chiavi crittografiche e di codici di autenticazione tramite messaggi (HKDF-SHA256).
  - Pertanto, le transazioni non possono mai essere attivate o manipolate da XMS o da altri impianti Xesar.

Memorizzazione dei dati, salvataggio dei dati e ripristino di emergenza

- Vengono memorizzati solo i dati necessari alla funzionalità specifica.
- I dati vengono memorizzati solo temporaneamente per un periodo di tempo limitato e in forma crittografata ai fini del transito tra il sistema Xesar e uno smartphone registrato su cui è presente l'app Xesar.
  - Registrazione: 48 ore
  - Aggiornamento delle autorizzazioni: 16 giorni
- I dati di accesso messi a disposizione da un impianto Xesar vengono crittografati già prima della trasmissione on-premise solo per lo smartphone registrato con l'app Xesar (AES-GCM-256). Questi dati non possono essere aperti dal servizio XMS, da EVVA o da altri impianti Xesar.
- I dati vengono attualmente memorizzati in modo ridondante in data center in cloud certificati in Germania occidentale. L'architettura è progettata in modo tale da poter essere estesa ad altre regioni/zone per l'archiviazione mirata.
- In caso di catastrofe che interessi un'intera zona, è possibile reindirizzare il salvataggio e ripristinare l'aggiornamento degli accessi con l'aiuto del sistema di gestione Xesar on-premise.
- Sono state adottate misure organizzative per limitare e autorizzare l'accesso ai dati archiviati:
  - Diritti di accesso rigorosamente controllati per il personale operativo e di supporto presso EVVA.
  - Gestione rigorosa delle risposte segrete per l'implementazione e le operazioni (SecDevOps).

Monitoraggio e allarmi

- Il funzionamento dei componenti di servizio viene costantemente monitorato e il personale operativo viene avvisato in caso di deviazioni.
  - I regolamenti istituiti a tale scopo vengono continuamente riesaminati e migliorati.
- I componenti del servizio sono sottoposti a monitoraggio CVE continuo e vengono aggiornati tempestivamente in caso di minaccia.

Avvertenze sulla tutela dei dati

- Lo sviluppo è stato realizzato secondo il principio Privacy by Design.
- I dati dei clienti o i dati personali di un impianto Xesar non vengono mai salvati nel contesto di XMS.
- I dati trasmessi da un sistema Xesar a uno smartphone registrato su cui è presente l'app Xesar:
  - non contengono dati personali;
  - non possono essere visibili in nessun caso dal servizio XMS, da EVVA o da altri impianti Xesar;
  - i numeri di telefono dei dispositivi mobili vengono utilizzati esclusivamente per chiamare il provider di servizi SMS, ma non vengono memorizzati dal servizio XMS.

Caratteristiche di sicurezza meccaniche dei componenti di accesso Xesar

Placca

Panoramica delle caratteristiche di sicurezza meccaniche di una placca Xesar.

Certificazioni ottenute

- EN 1634-1: 90 minuti
- EN 1634-3
- EN 179
- EN 1906
- con piastra di sostegno DIN 18257: ES0
- ÖNORM 3859: 90 minuti

Protezione dagli agenti ambientali

- Protezione IP 52 (IP55 con guarnizione incollata) contro la penetrazione di polveri dannose e getti d'acqua quando è installato
- Elettronica verniciata contro l'ossidazione provocata dalla condensa
- Condizioni di impiego: da -20°C a +55°C
- 3 batterie in ambienti interni protetti

Sicurezza fisica
- Collegamento a vite multiplo
  - Elevata protezione antimanomissione
  - Maniglia esterna a rotazione libera

Maniglia

Panoramica delle caratteristiche di sicurezza meccaniche di una maniglia Xesar.

Certificazioni ottenute
- EN 1634-1: 90 minuti
- EN 179
- EN 1906
- ÖNORM 3859: 90 minuti
- Certificazione CE

Protezione dagli agenti ambientali
- Intervallo di umidità: 90% a 0°C
- Temperatura ambiente interna: da +5°C a +50°C
- IP 40

Sicurezza fisica
- Maniglia esterna a rotazione libera

Cilindro

Certificazioni ottenute
- EN15684 16B30D3D
- SKG***
- SSF3522 per profili scandinavi
- Certificazione antincendio EN 1634 (90 min)
- Certificazione antipanico EN 179/1125
- ÖNORM B 5351:2011 WMZ6-BZ
- Certificazione CE

Protezione dagli agenti ambientali
- IP65 Protezione contro la penetrazione dannosa di polvere e getti d'acqua, se installato secondo le istruzioni di montaggio Xesar
- Elettronica verniciata contro l'ossidazione provocata dalla condensa
- Intervallo di umidità: 90% a 0°C
- Condizioni di impiego: da -20°C a +55°C
- 2 batterie in parallelo per una maggiore stabilità dell'alimentazione di tensione

Sicurezza fisica
- Pomolo esterno a rotazione libera
- Protezione antiperforazione
- Protezione antiestrazione
- Blocco di rotazione antieffrazione con un mandrino ad alta frequenza
- Spina di sicurezza presente sul filetto del pomolo esterno per proteggere il rotore da attacchi meccanici e prevenire i tentativi di snapping
- Speciale utensile meccanico per il montaggio e lo smontaggio del pomolo del cilindro

Sicurezza architettonica
- Il cilindro Xesar è costituito da un pomolo e da un modulo che si trova dietro la protezione antiperforazione.
- Il pomolo e il modulo sono collegati tra loro tramite un sistema protetto con crittografia:
  - Il rilascio avviene esclusivamente nella zona meccanicamente "sicura".
  - La semplice sostituzione del pomolo impedisce l'accesso non autorizzato.

Lettore murale (online, offline)

Certificazioni ottenute
› Certificazione CE

Protezione dagli agenti ambientali
› Intervallo di umidità 90% a 0°C
› Temperatura ambiente da –25°C a +70°C
› Grado di protezione IP65

Sicurezza fisica
› Frontale in vetro

Sicurezza architettonica
› Il lettore murale Xesar è composto da un'unità di lettura murale e da un'unità di controllo posizionata in una zona sicura.
› Il lettore murale online è composto da un'unità di lettura murale e da un'unità di controllo online posizionata in una zona sicura.
› L'unità di lettura e la centralina o l'unità di controllo sono collegate tra loro tramite un sistema protetto con crittografia:
  • Il rilascio avviene esclusivamente nella zona "sicura".
  • La semplice sostituzione del lettore murale impedisce l'accesso non autorizzato.

Altre caratteristiche generali di sicurezza

Componenti di accesso (porte):
› Assegnazione delle porte alle zone e autorizzazione per le zone
› Lista di blocco per tag o card bloccati
› Funzione Delete Key: disattivazione di tag o card bloccati che si trovano nella lista di blocco dei componenti
› Modalità ufficio (apertura permanente dei componenti)
  • Apertura permanente manuale di componenti
  • Apertura permanente automatica, temporizzata tra due punti temporali definiti (inizio e fine)
  • Office Mode End in punti temporali definiti in cui vengono terminate anche le aperture permanenti manuali (solo fine)
  • Shop Mode (modalità negozio): apertura permanente automatica, avviata solo dopo l'accesso autorizzato
› Registro eventi per eventi di accesso, di revoca e in modalità ufficio
› Limitazione temporale per le autorizzazioni di accesso

Tag o card:
› La rete virtuale consente il trasporto di dati tramite tag o card o il loro utilizzo da parte di persone all'interno dell'impianto.

Software di gestione:
› Profili di autorizzazione definiti per utenti con diritti utente diversi (gruppo utenti)
› Viste dashboard definite per utenti in base ai diritti di utilizzo (gruppo utenti)
› Stato dell'impianto su dashboard
  • Componenti:
    - aggiornamenti firmware necessari
    - aggiornamenti di configurazione necessari
    - visualizzazione dello stato della batteria
    - tempestivo stato online delle porte con componenti EVVA online
    - stato della connessione
    - stato dei contatti porta
  • Componenti di accesso ed elementi:
    - porte non sicure
    - tag o card che richiedono un aggiornamento
    - tag o card bloccati in modo non sicuro
    - aperture effettuate con tag o card bloccati
› Registro di sistema per la tracciabilità delle modifiche apportate alla configurazione nel software di gestione

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