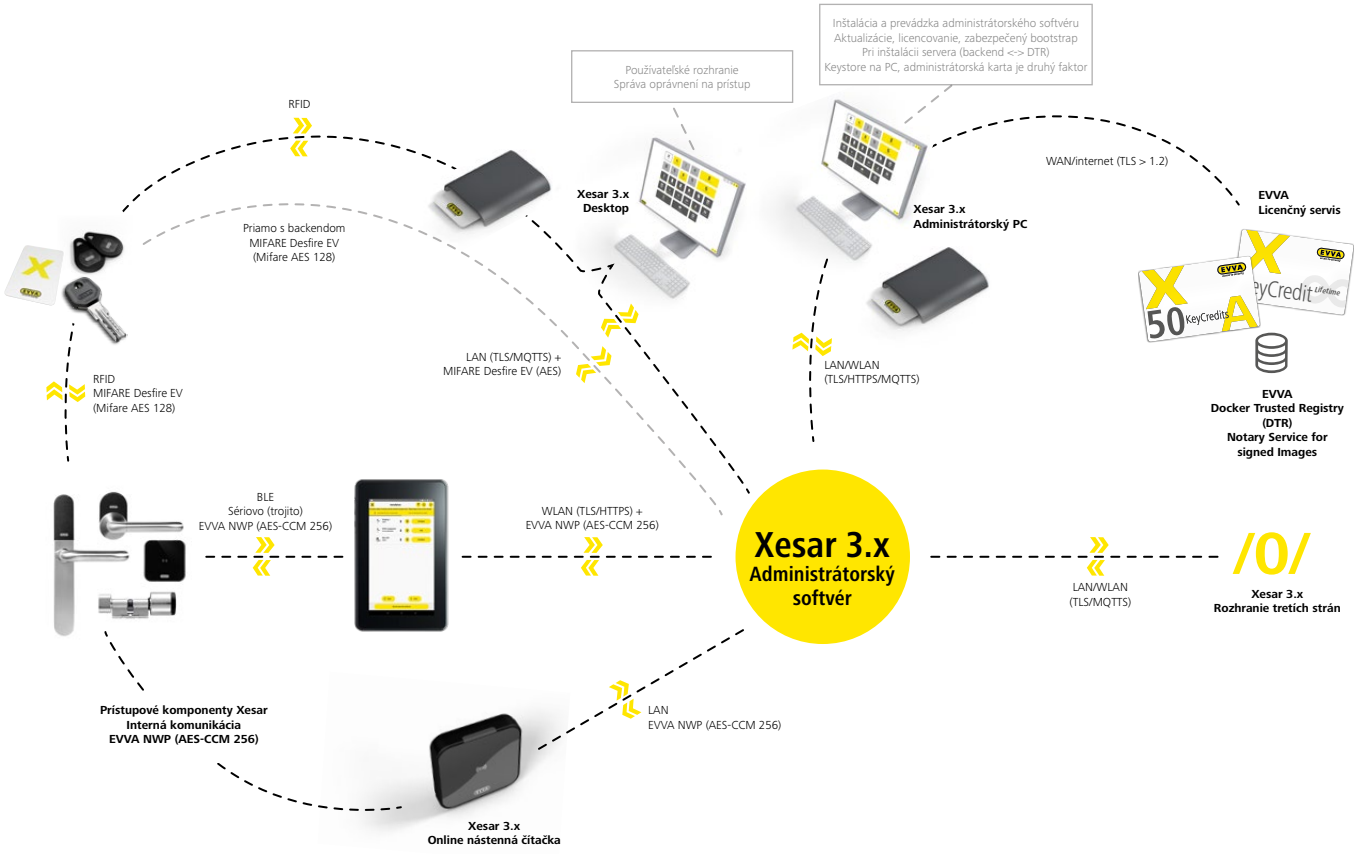
Bezpečnostná koncepcia Xesar

Prehľad najdôležitejších bezpečnostných prvkov prístupového systému Xesar

Kybernetická bezpečnosť Xesar



Prístupové médiá (Xesar 3)

Rozhranie a komunikácia

Na komunikáciu medzi prístupovými komponentmi a prístupovými médiami sa vo všetkých prípadoch používa postup šifrovania MIFARE AES so 128-bitovým šifrovaním AES.

- Aplikačný kľúč pre oprávnenie na prístup sa generuje počas inštalácie Xesar bezpečným postupom. Je to tajomstvo zákazníka a EVVA ho nepozná.
- Ukladá sa len v trvalej zašifrovanej forme v inštalácii bezpečnostnej služby.
- Pri používanom postupe MIFARE sa pre každú interakciu používa relácia s vlastným náhodne vygenerovaným kľúčom.

Dátová pamäť

V rámci systému Xesar sa používajú výlučne bezpečné prístupové médiá s chránenou dátovou pamäťou

- Mifare Desfire EV1 s certifikáciou EAL4+ alebo
- Mifare Desfire EV2/EV3 s certifikáciou EAL5+

Bezpečnostné upozornenia

- Prvé pridanie prístupového média do inštalácie Xesar by mal – na zabránenie manipulácii – robiť iba oprávnený používateľ pomocou kódovacej stanice na chránenom mieste.
- Konštrukčné médium je na celom svete rovnaké a môže sa všade používať na prístup k prístupovým komponentom Xesar v stave pri odoslaní, resp. v režime stavby. Preto sa s ním nemôže vykonávať žiadna kontrola prístupu.
- Prístupové médium s oprávnením generálneho kľúča sa smie odovzdávať len vo výnimočných prípadoch a dôveryhodným osobám. Dôvod: prístupové médium s týmto profilom oprávnenia má
  - neobmedzenú dobu platnosti (max. doba platnosti sa opisuje v príručke),
  - prístup ku všetkým prístupovým komponentom inštalácie, aj keď sa pridajú/vytvoria až po vydaní tohto média.

Prístupové médium s oprávnením generálneho kľúča by sa malo uchovávať na bezpečnom mieste mimo zabezpečenej inštalácie, aby bol v núdzovom prípade možný prístup k inštalácii.

Administrátorský softvér

Dodanie

- Všetky digitálne súčasti systému dodané spoločnosťou EVVA sú vybavené platným a časovo označeným podpisom kódu.
- Rozhranie a komunikácia
- Každá komunikácia so správou Xesar je zabezpečená TLS > 1.2, zoznam povolených algoritmov TLS nájdete na Cipher Suites;
  - na správu inštalácie viacerými používateľmi prostredníctvom prístupu cez prehliadač,
  - na pripojenie Manažéra periférie (rozdelená kódovacia stanica),
  - na interakciu so službami, ktoré sú súčasťou inštalácie,
  - na interakciu s rozhraním systému tretej strany.

Overenie

Vo všeobecnosti sa – keď je to zmysluplné– dodržujú usmernenia OWASP.

- Overenie na správu inštalácie prostredníctvom prístupu cez prehliadač je chránené heslom:
  - prvé heslo administrátora sa generuje náhodne pri inštalácii (žiadne predvolené nastavenia),
  - všetky heslá, ktoré sa vytvoria, musia mať minimálnu dĺžku a je k dispozícii indikátor kvality (zxcvbn: Low-Budget Password Strength Estimation),
  - heslá sa nikdy neukladajú v nezabezpečenom texte (BCrypt),
  - na zlyhania overovania sa zámerne odpovedá všeobecne.
- Overenie na servisných rozhraniach je zobrazené na základe certifikátu s mTLS:
  - na pripojenie Manažéra periférie,
  - pri interných pripojeniach k službám, ktoré sú súčasťou inštalácie,
  - pri pripojení k rozhraniu systému tretej strany prostredníctvom brokera MQTT; tu sa dodatočne použije ešte token na interné overenie.

Autorizácia
- V správe Xesar sa môžu na autorizáciu definovať používateľské práva prostredníctvom skupín používateľov, ktoré sa potom môžu jednoducho priradiť príslušným používateľom.
- Príslušné akcie používateľa sa protokolujú v systéme.
- Autorizácia a protokolovanie fungujú aj pre používateľov rozhrania.

Dátová pamäť
- Všetky citlivé údaje (napr. šifrovací materiál, heslá) sa ukladajú výlučne v bezpečnostnej službe inštalácie (Vault) a ukladajú sa len šifrovane.
- Pri bootstrape inštalácie sa prostredníctvom dvoch faktorov (administrátorská karta a uložené šifrované úložisko kľúčov Keystore v administrátorskom počítači) „otvorí“ Vault na prevádzku.
  - Necitlivé údaje inštalácie a konfigurácie sa ukladajú do databázy, ktorá nie je šifrovaná (pozri bezpečnostné pokyny).
  - Architektonický dizajn administrátorského softvéru, v ktorom sú modely čítania a zápisu oddelené, ukladá všetky zmeny ako sekvenciu udalostí (CQRS-ES). To zvyšuje vysledovateľnosť a sťažuje manipuláciu s dátovými súbormi.

Bezpečnostné upozornenia
- Na inštaláciu systému by sa mali používať len nezmenené artefakty dodané spoločnosťou EVVA. Pravosť a integrita všetkých artefaktov dodaných spoločnosťou EVVA sa môže overiť prostredníctvom podpisu.
- Zodpovednosť za bezpečnú prevádzku administrátorského softvéru Xesar nesie zákazník;
  - prístup (overenie a autorizácia) k serverovému prostrediu musí byť zabezpečený, aby sa s necitlivými dátovými súbormi inštalácie a konfigurácie nemohlo jednoducho manipulovať,
  - prístup k správe inštalácie by mali mať jednoznačne overení a príslušne autorizovaní používatelia,
  - zriadené inštalačné účty by sa mali používať len pri inštalácii a potom už len vo výnimočných prípadoch (napr. resetovanie hesla, obnovenie).
- Bezpečnostný list inštalácie, ktorý sa generuje pre prípady obnovenia pri inštalácii, by sa mal uchovávať len vo vytlačenej forme na bezpečnom mieste (napr. trezor).

Informácie o ochrane údajov
- Pri aktivácii zaznamenávania osobných prístupových údajov by sa mali poznať a dodržiavať predpisy o ochrane údajov danej krajiny.
- Automatické odstránenie väzby medzi osobnými údajmi a prístupovými údajmi sa môže príslušne nakonfigurovať prostredníctvom administrátorského softvéru. Možnosti a postup v softvéri nájdete v príručke.

Komponenty údržby (tablet Xesar)

Rozhranie a komunikácia
- Keď chcete pridať nový komponent Xesar do inštalácie Xesar, inštalačný kľúč sa prepravuje zašifrovaný pomocou postupu šifrovania AEAD a 128-bitového kľúča AES. Tento kľúč je odvodený z PIN kódu ako druhého faktora, ktorý nie je uložený v zariadení, pomocou funkcie odvodzovania kryptografického kľúča (KDF, AES-CMAC-PRF-128).
- Konfiguračné údaje pre komponenty v inštalácii sa prenášajú zašifrované pomocou postupu šifrovania AEAD a 256-bitového kľúča AES špecifického pre komponent (pozri tiež Kybernetická bezpečnosť komponentov Xesar).

Bezpečnostné upozornenia
- Tablet údržby dodaný spoločnosťou EVVA by sa mal používať výlučne na účely údržby inštalácie.
- Na tento tablet by sa nemali inštalovať žiadne ďalšie aplikácie.
- Na zavedenie nových komponentov Xesar sú konfiguračné údaje chránené PIN kódom. Tento PIN kód by sa mal:
  - po inštalácii nakonfigurovať v nastaveniach systému tak, aby systém nepoužíval predvolenú hodnotu (t. j. 0000),
  - poskytovať len známym a dôveryhodným osobám.
- Na prevádzku so Xesar nie je potrebná registrácia na Google.
- Aktivácia sieťovej komunikácie (WLAN) by sa mala vykonávať len v prípade potreby a mala by sa používať zabezpečená súkromná sieť (t. j. nie internet).
- Inštalovať by sa mali iba aktualizácie systému odporúčané a testované spoločnosťou EVVA.

Prístupové komponenty

Rozhranie a komunikácia

- Na komunikáciu s komponentom sa vo všetkých prípadoch (rádiovo a sériovo) používa postup šifrovania AEAD s 256-bitovými kľúčmi AES (AES-CCM).
- Komunikačný kľúč sa generuje špecificky pre každý komponent v administrátorskom softvéri Xesar bezpečným postupom a je neznámym tajomstvom zákazníka EVVA.
- Po zadaní do inštalácie môže zmeny stavu alebo konfiguráciu komponentov vykonávať už len používateľ.
- Šifrovací materiál sa môže aktualizovať na komponente s príslušným zabezpečením (overenie, šifrovaný prenos).
- Útoky hrubou silou nie je ľahké úspešne vykonať vzhľadom na veľkosť kľúča pri symetrických postupoch, a to ani v postkvantovom čase. V prípade komponentov napájaných batériami napájanie navyše umožní len malú časť pokusov potrebných na základe kombinatoriky, najmä na rádiovom spojení.

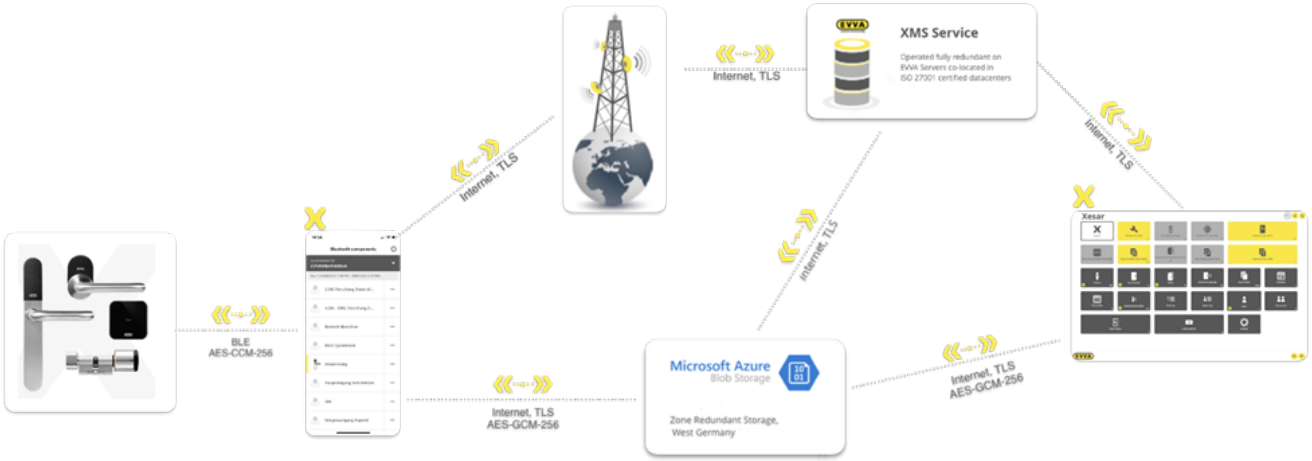
Dátová pamäť

- Šifrovací materiál, citlivá konfigurácia a aplikačný kód sa ukladajú na príslušný mikrokontrolér (MC) s najlepším možným zabezpečením MC (NVRAM, interná flash pamäť);
  - rodina PIC24: General Segment Protection and Code Segment Protection (Family Datasheet, 29.4),
  - NRF52: Access port protection controlled by hardware (APPPROTECT),
  - chráni telo pred nedeštruktívnym prístupom k mikrokontrolóru MC (pozri tiež mechanickú bezpečnosť komponentov Xesar).
- Údaje inštalácie sú uložené na komponente v pamäti (EEPROM alebo Flash) a zabezpečené pomocou kryptografického postupu s 128-bitovým kľúčom AES (AES-CMAC).

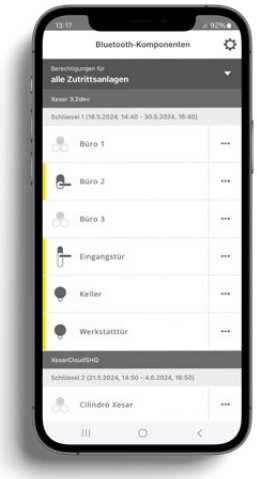
Firmvér a aktualizácia

- Existujúci firmvér sa načíta pomocou bootloadera, ktorý už nie je možné meniť z výroby, a môže sa aktualizovať pomocou bootloadera s príslušným zabezpečením.
- Firmvérové balíky EVVA sa podpisujú asymetrickou metódou (RSA-SHA256) a správe Xesar sa dodávajú symetricky zašifrované. Reťazec certifikátov sa overuje v administrátorskom softvéri a aj v aplikácii údržby.
- Na aktualizáciu v inštalácii sa používa postup šifrovania AEAD s 256-bitovými kľúčmi AES (AES-CCM). Kľúč na aktualizáciu firmvéru generuje administrátorský softvér Xesar špecificky pre inštaláciu bezpečným postupom a je neznámym tajomstvom zákazníka EVVA.
- Po zadaní do inštalácie môže aktualizáciu firmvéru na komponentoch vykonávať už len používateľ.
- V prípade firmvéru pre NRF52 MC sa navyše:
  - firmvér podpisuje asymetrickým postupom (RSA-SHA256, 2048 bit Key) a overuje sa priamo na mikrokontroléri MC,
  - firmvér zabezpečuje postupom šifrovania AEAD (AES-CCM), ktorá využíva 256-bitový kľúč AES.
- Firmvér komponentov, ktoré sa ako nové pridávajú do inštalácie, sa automaticky aktualizuje na poslednú verziu firmvéru známu administrátorskému softvéru alebo aplikácii údržby.
- Upozornenia a kontrola aktualizácií dostupných od spoločnosti EVVA podporuje a umožňuje manažér inštalácie Xesar a aplikácia údržby Xesar.

Mobilné zamykanie – prehľad



Mobilná aplikácia Xesar (aplikácia Xesar)



Rozhrania a komunikácia

- Každá komunikácia s XMS alebo cloudovými úložiskami je zabezpečená protokolom TLS.
- Všetky transakcie medzi inštaláciou Xesar a aplikáciou Xesar sa overujú na základe protokolu výmeny kľúčov (X25519), funkcie odvodzovania kľúčov a autentifikačných kódov správ (HKDF-SHA256) End-to-End.
- Každá komunikácia medzi komponentom Xesar a mobilnou aplikáciou na prenos prístupových údajov je chránená proti prehrávaniu a šifrovaná v rámci relácie.
- Uchovávanie údajov
- Ak to koncové zariadenie podporuje, citlivý šifrovací materiál sa ukladá na zabezpečených úložiskách hardvéru.
  - Android: StrongBox, ak je k dispozícii, priradený zariadeniu, cloudová záloha deaktivovaná prostredníctvom manifestu.
  - iOS: Zväzok kľúčov CryptoKit, použiteľný výlučne na zariadení, synchronizácia iCloud s konfiguračným profilom deaktivovaná.
- Všetky údaje sa ukladajú v ešte raz dodatočne zašifrovanej databáze na mobilnom koncovom zariadení.
- Prístupové údaje inštalácie Xesar sú tým už predtým zašifrované a mobilná aplikácia ich nemôže dešifrovať, kontrolovať ani nimi manipulovať.
- Bezpečnostné upozornenia
- Mobilná aplikácia by sa mala sťahovať vo svojej pôvodnej forme podpísanej spoločnosťou EVVA výlučne z oficiálneho obchodu (t. j. Google Play, Apple App Store).
- Spoločnosť EVVA odporúča všetkým používateľom mobilnej aplikácie
  - používanie koncových zariadení s hardvérovými bezpečnostnými pamäťami,
  - používanie šifrovania pamäte,
  - používanie zabezpečenia koncového zariadenia heslom, kódom PIN alebo biometrickým prihlásením.

Mobilná podpora Xesar (XMS – Xesar Mobile Support)

Dátové centrum

- Služba sa prevádzkuje na serveroch EVVA, ktoré sú umiestnené prostredníctvom Colocation vo fyzicky oddelených dátových centrách certifikovaných podľa normy ISO 27001 v Rakúsku.
- Všetky potrebné zdroje sú navrhnuté redundantne a horizontálne škálovateľné.
- Všetky koncové body služby sú za firewallom s najmodernejšími ochrannými mechanizmami (IDS, IPS a DoS).

Rozhrania a komunikácia

- Každá komunikácia s XMS je zabezpečená protokolom TLS > 1.2.
  - MQTT Broker (mqtts://mqtt.akx.cloud:443)
    – zoznam povolených certifikátov TLS pozri broker MQTT,

- koncový bod REST (https://mss.akx.cloud)
  – na overenie a autorizáciu administrátorského softvéru Xesar,
  – zoznam povolených algoritmov TLS REST.

› XMS je výlučne „reléová stanica“ medzi inštaláciou Xesar a registrovaným smartfónom s aplikáciou Xesar.
  - Všetky transakcie medzi inštaláciou Xesar a registrovaným smartfónom s aplikáciou Xesar sa autentifikujú na základe protokolu výmeny kľúčov (X25519), funkcie odvodzovania kľúčov a autentifikačných kódov správ (HKDF-SHA256) End-to-End.
  - Transakcie sa preto nemôžu nikdy iniciovať ani s nimi manipulovať prostredníctvom XMS ani iných inštalácií Xesar.

Dátová pamäť, zálohovanie údajov a obnova po núdzovej situácii

› Uchovávajú sa len údaje, ktoré sú potrebné na fungovanie.
› Údaje sa dočasne ukladajú len na obmedzený čas a v zašifrovanej forme pre prechod medzi inštaláciou Xesar a smartfónom s aplikáciou Xesar registrovaným na tento účel.
  - Registrácia: 48 h
  - Aktualizácia oprávnení: 16 dní
› Prístupové údaje, ktoré poskytuje inštalácia Xesar, sa už pred prenosom na mieste šifrujú len pre registrovaný smartfón s aplikáciou Xesar (AES-GCM-256). Tieto údaje nemôže otvoriť XMS-Service, EVVA ani iné inštalácie Xesar.
› Údaje sa v súčasnosti redundantne uchovávajú v certifikovaných cloudových dátových centrách v zóne západného Nemecka. Architektúra je navrhnutá tak, aby ju bolo možné rozšíriť na cielené uchovávanie v iných regiónoch/zónach.
› V prípade katastrofy, ktorá sa týka celej zóny, sa môže uchovávanie presmerovať a aktualizácia prístupov môže byť opäť vykonateľná pomocou správy Xesar na mieste.
› Prijali sa organizačné opatrenia na obmedzený a výlučne autorizovaný prístup k uchovávaným údajom:
  - prísne kontrolované prístupové práva pre obslužný a podporný personál spoločnosti EVVA,
  - prísne riadenie tajomstiev pri zavádzaní a prevádzke (SecDevOps).

Monitorovanie a alarmy

› Prevádzka servisných komponentov sa nepretržite monitoruje a obslužný personál sa upozorňuje na odchýlky.
  - Pravidlá stanovené na tento účel sa priebežne revidujú a vylepšujú.
› Servisné komponenty podliehajú priebežnému monitorovaniu CVE a v prípade scenárov ohrozenia sa včas aktualizujú.

Informácie o ochrane údajov

› Pri vývoji sa pracovalo podľa princípu Privacy by Design.
› Zákazníci ani osobné údaje inštalácie Xesar sa nikdy neukladajú v kontexte XMS.
› Údaje, ktoré sa prenášajú z inštalácie Xesar na registrovaný smartfón s aplikáciou Xesar
  - neobsahujú žiadne osobné údaje,
  - nemôže vidieť služba XMS, EVVA ani iné inštalácie Xesar,
  - telefónne čísla mobilných koncových zariadení sa používajú výlučne na volanie poskytovateľovi služby SMS, služba XMS ich neuchováva.

Mechanické bezpečnostné prvky prístupových komponentov Xesar

Kovanie

Prehľad mechanických bezpečnostných prvkov kovania Xesar.

Získané certifikácie

› EN 1634-1: 90 minút
› EN 1634-3
› EN 179
› EN 1906
› so stabilizačnou doskou DIN 18257: ES0
› ÖNORM 3859: 90 minút

Ochrana pred poveternostnými vplyvmi

› IP 52 (IP55 s nalepeným tesnením) ochrana proti vniknutiu škodlivého prachu a prúdu vody v zabudovanom stave
› Elektronika s ochranným lakom proti oxidácii v dôsledku kondenzujúcej vody
› Podmienky používania: -20 °C – +55 °C
› 3 batérie v bezpečnom vnútornom priestore

Fyzická bezpečnosť
› Viacnásobné skrutkové spoje
  • Mechanická ochrana proti manipulácii
  • Voľne sa otáčajúca vonkajšia kľučka

Kľučka

Prehľad mechanických bezpečnostných prvkov kľučky Xesar.

Získané certifikácie
› EN 1634-1: 90 minút
› EN 179
› EN 1906
› ÖNORM 3859: 90 minút
› Testované podľa CE

Ochrana pred poveternostnými vplyvmi
› Rozsah vlhkosti vzduchu: 90 % pri 0 °C
› Teplota okolia vnútri: +5 °C až +50 °C
› IP 40

Fyzická bezpečnosť
› Voľne sa otáčajúca vonkajšia kľučka

Cylindrická vložka

Získané certifikácie
› EN15684 16B30D3D
› SKG***
› SSF3522 pre škandinávske profily
› EN1634 certifikácia protipožiarnej ochrany (90 minút)
› EN179/1125 certifikácia protipanikovej funkcie
› ÖNORM B 5351:2011 WMZ6-BZ
› Testované podľa CE

Ochrana pred poveternostnými vplyvmi
› Ochrana IP65 proti škodlivému vniknutiu prachu a striekajúcej vode pri inštalácii podľa montážnych pokynov Xesar
› Elektronika s ochranným lakom proti oxidácii v dôsledku kondenzujúcej vody
› Rozsah vlhkosti vzduchu: 90 % pri 0 °C
› Podmienky používania: -20 °C – +55 °C
› 2 paralelné batérie pre vyššiu stabilitu napájania

Fyzická bezpečnosť
› Voľne sa otáčajúci vonkajší gombík
› Ochrana proti odvŕtaniu
› Ochrana proti vytiahnutiu jadra vložky
› Rotačná brzda proti zásahom vysokofrekvenčným vretenom
› Definované miesto žiadaného zlomu na závite vonkajšieho gombíka na ochranu jadra pred mechanickými zásahmi a zabránenie útokom rozlomením
› Mechanické špeciálne náradie na montáž a demontáž cylindrickej vložky

Architektonická bezpečnosť
› Cylindrická vložka Xesar pozostáva z gombíka cylindrickej vložky a modulu cylindrickej vložky, ktorý je za ochranou proti odvŕtaniu.
› Gombík a modul sú navzájom prepojené kryptografickým zabezpečením:
  • sprístupnenie sa uskutočňuje výlučne v mechanicky „bezpečnej“ oblasti,
  • jednoduchá výmena gombíka neumožní neoprávnený prístup.

Nástenná čítačka (online, offline)

Získané certifikácie
› Testované podľa CE

Ochrana pred poveternostnými vplyvmi
› Rozsah vlhkosti vzduchu: 90 % pri 0 °C
› Teplota okolia: -25 °C až +70 °C
› Stupeň ochrany IP65

Fyzická bezpečnosť
› Sklená predná časť

Architektonická bezpečnosť
› Nástenná čítačka Xesar pozostáva z nástennej čítačky a riadiacej jednotky nástennej čítačky, ktorá sa nachádza v bezpečnej oblasti.
› Online nástenná čítačka pozostáva z nástennej čítačky a online riadiacej jednotky, ktorá sa nachádza v bezpečnej oblasti.
› Čítacia jednotka a riadiaca jednotka sú navzájom prepojené kryptografickým zabezpečením:
  • sprístupnenie sa uskutočňuje výlučne v „bezpečnej" oblasti,
  • jednoduchá výmena nástennej čítačky neumožní neoprávnený prístup.

Ďalšie všeobecné bezpečnostné prvky

Prístupové komponenty (dvere):
› Priradenie dverí oblastiam a oprávnenia pre oblasti
› Zoznam zablokovaných prístupových médií
› Delete-Key – deaktivácia zablokovaných prístupových médií, ktoré sú v zozname zablokovaných komponentov
› Kancelársky režim (trvalé otvorenia komponentov)
  • Manuálne trvalé otvorenie komponentov
  • Automatické trvalé otvorenie, časovo riadené medzi dvoma stanovenými časovými bodmi (začiatok a koniec)
  • Automatický koniec trvalého otvorenia – Office Mode End v stanovených časových bodoch, v ktorých sa končia aj manuálne trvalé povolenia – Manual Office Mode (len koniec)
  • Režim obchodu: Automatické trvalé povolenie – Office Mode, spustené až po oprávnenom prístupe
› Protokol udalostí pre udalosti prístupu, odmietnutia a Office mode
› Časové obmedzenie pre oprávnenia na prístup

Prístupové médiá:
› Virtuálna sieť umožňuje prenos údajov prostredníctvom prístupových médií, resp. ich používanie osobami v inštalácii.

Administrátorský softvér:
› Definované profily oprávnení pre používateľov s rôznymi používateľskými právami (skupina používateľov)
› Definované zobrazenia ovládacieho panela pre používateľov podľa používateľských práv (skupina používateľov)
› Stav inštalácie na ovládacom paneli
  • Komponenty:
    – potrebné aktualizácie firmvéru,
    – potrebné aktualizácie konfigurácie,
    – zobrazenie stavu batérie,
    – aktuálny online stav dverí s online EVVA-komponentom,
    – stav pripojenia,
    – stav kontaktov dverí;
  • Prístupové komponenty a médiá:
    – nezabezpečené dvere,
    – prístupové médiá, ktoré vyžadujú aktualizáciu,
    – nezabezpečené zablokované prístupové médiá,
    – sprístupnenia, ktoré sa uskutočnili so zablokovanými prístupovými médiami.
› Systémový protokol na sledovanie zmien konfigurácie v administrátorskom softvéri

I.X.SJARC.ID.INFBL.SSK.LN 15R1