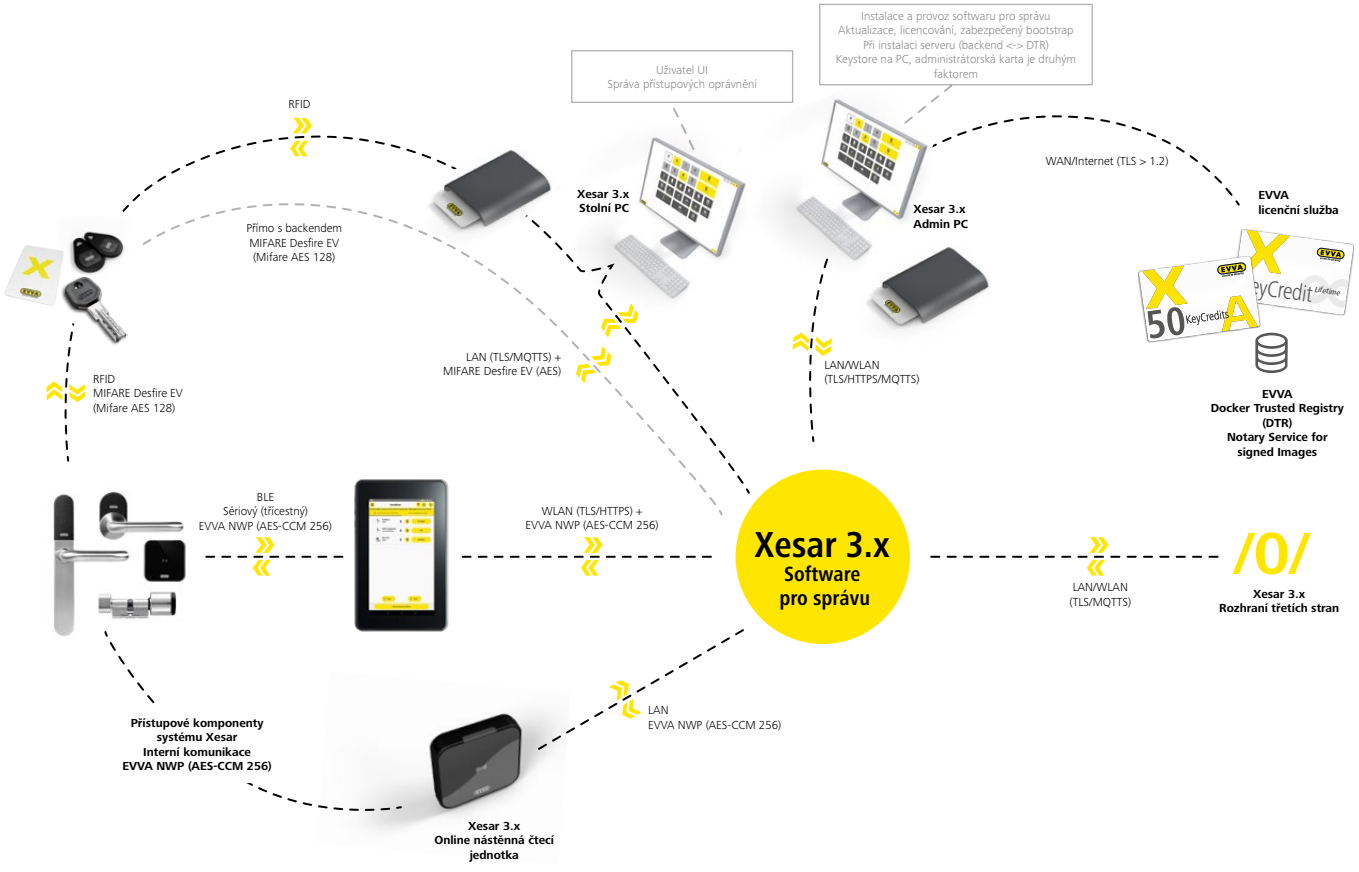
Koncepce zabezpečení Xesar

Přehled nejdůležitějších bezpečnostních funkcí přístupového systému Xesar

Kybernetická bezpečnost Xesar



Přístupová média (Xesar 3)

Rozhraní a komunikace

Pro komunikaci mezi přístupovými komponentami a přístupovými médii se ve všech případech používá šifrovací metoda MIFARE AES se 128bitovým šifrováním AES.

- Aplikační klíč pro oprávnění k přístupu se generuje během instalace systému Xesar bezpečným způsobem. Je to zákaznické tajemství a společnost EVVA ho nezná.
- Ukládá se v zašifrované podobě pouze v instalaci bezpečnostní služby v perzistentní podobě.
- U použitého postupu MIFARE se pro každou interakci používá relace s vlastním náhodně generovaným klíčem.

Paměťové médium

U systému Xesar se používají výhradně bezpečná přístupová média s chráněnou datovou pamětí

- Mifare Desfire EV1 s certifikací EAL4+ nebo
- Mifare Desfire EV2/EV3 s certifikací EAL5+

Bezpečnostní pokyny

- Aby se zabránilo manipulaci, mělo by se poprvé přidat přístupové médium do systému Xesar pouze oprávněným uživatelem na chráněném místě pomocí kódovací stanice.
- Identifikační médium v konstrukčním režimu je po celém světě stejné a lze ho použít všude pro přístup k přístupovým komponentám Xesar v původním stavu z výroby, popř. v konstrukčním režimu. Proto s ním nelze provádět kontrolu přístupu.
- Přístupové médium s oprávněním hlavního klíče se smí předávat pouze ve výjimečných případech a důvěryhodným osobám. Důvod: přístupové médium s tímto profilem s oprávněním má
  - neomezenou dobu platnosti (max. doba platnosti viz příručka)
  - Přístup ke všem přístupovým komponentám systému, i když jsou přidávány/vytvářeny až po vystavení tohoto média.

Přístupové médium s oprávněním hlavního klíče by mělo být uloženo na bezpečném místě mimo zabezpečenou instalaci, aby byl v případě nouze možný přístup k instalaci.

Software pro správu

Dodání

- Všechny digitální součásti systému dodané společností EVVA jsou opatřeny platným a časově označeným společným označením.
- Rozhraní a komunikace
- Veškerá komunikace se správou systému Xesar je zabezpečena protokolem TLS > 1.2, seznam povolených algoritmů TLS naleznete v šifrovacích sadách.
  - ke správě instalace více uživateli prostřednictvím přístupu prohlížeče
  - k připojení správce periferních zařízení (rozdělená kódovací stanice),
  - k interakci se službami, které jsou součástí instalace
  - pro interakci s rozhraním systému třetí strany

Autentizace

Zde byly obecně – kde je to smysluplné – dodržovány směrnice OWASP.

- Ověření pro správu instalace prostřednictvím přístupu prohlížeče je chráněno heslem:
  - První administrátorské heslo je při instalaci náhodně generováno (neexistují žádná výchozí hesla)
  - Všechna nově vytvořená hesla musí splňovat požadovanou minimální délku a obsahují indikátor kvality hesla (zxcvbn: Low-Budget Password Strength Estimation)
  - Hesla se nikdy neukládají v nešifrované podobě (BCrypt)
  - Neúspěšné pokusy o autentizaci jsou záměrně zodpovídány obecnými odpověďmi
- Autentizace na servisních rozhraních je realizována na bázi certifikátů pomocí mTLS:
  - k připojení správce periferních zařízení
  - u interních připojení služeb jsou součástí instalace
  - Při připojení k rozhraní třetího systému přes MQTT broker se navíc používá token pro interní

Autorizace
- Ve správě systému Xesar lze definovat oprávnění uživatelů prostřednictvím skupin uživatelů, které pak lze jednoduše přiřadit příslušným uživatelům
- Příslušné akce uživatele jsou v systému protokolovány
- Autorizace a protokolování funguje i pro uživatele rozhraní

Paměťové médium
- Veškerá citlivá data (např. materiál klíčů, hesla) se ukládají výhradně v bezpečnostní službě Instalace (Vault) a pouze šifrovaně.
- Při bootstrapu instalace se pomocí dvou faktorů (admin karty a šifrovaného úložiště klíčů uloženého na AdminPC) „otevírá“ Vault pro provoz.
  - Necitlivá data související s instalací a konfigurací jsou uložena v databázi, která není šifrována (viz bezpečnostní pokyny).
  - Architektonický design softwaru pro správu, který odděluje modely čtení a zápisu, ukládá všechny změny jako sekvenci událostí (CQRS-ES). To zvyšuje sledovatelnost a ztěžuje manipulaci s datovými záznamy.

Bezpečnostní pokyny
- K instalaci systému by se měly používat pouze nezměněné artefakty dodané společností EVVA. Pravost a bezúhonnost všech artefaktů dodaných společností EVVA lze ověřit podpisem.
- Odpovědnost za bezpečný provoz správního softwaru Xesar nese zákazník;
  - Přístup (autentifikace a autorizace) k serverovému prostředí musí být zajištěn, aby nemohlo dojít k jednoduché manipulaci s necitlivými datovými soubory instalace a konfigurace
  - Přístup ke správě instalace by měl být umožněn jednoznačně ověřeným a náležitě oprávněným uživatelům.
  - Zřízené instalační účty by se měly používat pouze při instalaci a poté pouze ve výjimečných případech (např. resetování hesla, obnovení).
- Bezpečnostní list instalace, který je generován pro případy obnovení při instalaci, by měl být uložen pouze v tištěné podobě na bezpečném místě (např. v trezoru).

Zásady ochrany osobních údajů
- Při aktivaci záznamu osobních přístupových údajů by měla být známa a dodržována ustanovení o ochraně osobních údajů specifická pro danou zemi.
- Automatické zrušení vztahu osob k přístupovým údajům lze odpovídajícím způsobem nakonfigurovat prostřednictvím správního softwaru. Možnosti a postupy v softwaru jsou popsány v příručce.

Komponenta údržby (tablet Xesar)

Rozhraní a komunikace
- Chcete-li do systému Xesar přidat novou komponentu Xesar, je instalační klíč zašifrován metodou šifrování AEAD a 128bitovým klíčem AES. Tento klíč je odvozen z PIN kódu jako druhého faktoru, který není uložen v zařízení, pomocí funkce kryptografického odvození klíče (KDF, AES-CMAC-PRF-128).
- Konfigurační data pro komponenty v instalaci jsou přenášena šifrovaným způsobem AEAD a 256bitovým klíčem AES specifickým pro komponentu (viz také kybernetická bezpečnost komponent Xesar).

Bezpečnostní pokyny
- Tablet pro údržbu dodaný společností EVVA by měl být používán výhradně pro účely údržby systému.
- Na tomto tabletu by neměly být instalovány žádné další aplikace.
- Při vkládání nových komponent Xesar jsou konfigurační data chráněna PIN kódem. Ten by měl:
  - Po instalaci do systému nakonfigurujte nastavení tak, aby systém nepoužil výchozí hodnotu (tj. 0000).
  - Sdílet pouze se známými a důvěryhodnými osobami
- Registrace u Google není pro provoz se systémem Xesar nutná.
- Aktivace síťové komunikace (WIFI) by měla být prováděna pouze v případě potřeby a měla by být používána zabezpečená soukromá síť (tj. nikoli internet)
- Měly by se instalovat pouze aktualizace systému doporučené a testované společností EVVA.

Přístupové komponenty

Rozhraní a komunikace

- Pro komunikaci s komponentou se ve všech případech (rádiová a sériová) používá šifrovací metoda AEAD s 256bitovými klíči AES (AES-CCM).
- Komunikační klíč je generován bezpečným způsobem specificky pro každou komponentu ve správním softwaru Xesar a je neznámým zákaznickým tajemstvím společnosti EVVA.
- Po vložení do instalace může provádět změny stavu nebo konfigurace komponent pouze několik uživatelů
- Klíčový materiál lze aktualizovat na komponentě s odpovídajícím zabezpečením (autentifikace, šifrovaný přenos)
- Brute force útoky jsou díky velikosti klíče v symetrických šifrovacích algoritmech obtížné a neúspěšné i pro období po příchodu kvantových počítačů. U komponent napájených baterií je navíc energetická kapacita natolik omezená, že umožňuje pouze malý podíl pokusů vyžadovaných kombinatorikou, zejména na rádiové (bezdrátové) komunikaci.

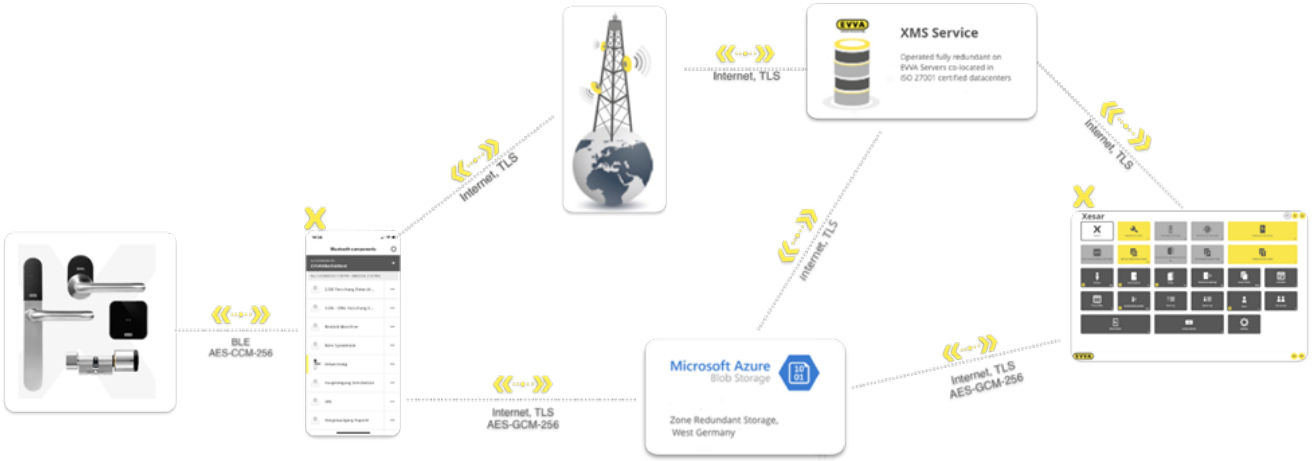
Paměťové médium

- Klíčový materiál, citlivá konfigurace a aplikační kód jsou uloženy na příslušném mikrokontroléru (MC) s nejlepším možným zabezpečením MC (NVRAM, interní flash paměť)
  - Rodina PIC24: Obecná ochrana segmentu a ochrana kódového segmentu (Family Datasheet, 29.4)
  - NRF52: Ochrana přístupového portu řízená hardwarem (APPPROTECT)
  - Tělo chrání před nedestruktivním přístupem k MC (viz také Mechanická bezpečnost komponent Xesar)
- Data systému se ukládají na komponentě do paměti (EEPROM nebo flash) a jejich integrita je zajištěna použitím kryptografického postupu s 128bitovým klíčem AES (AES-CMAC).

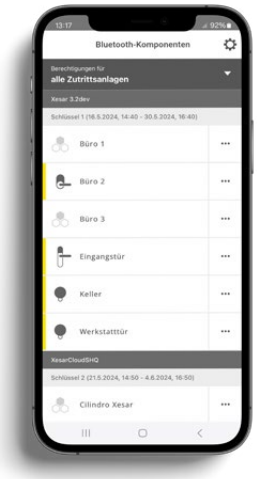
Firmware a aktualizace

- Stávající firmware je nahrán pomocí bootloaderu, který nelze po výrobě změnit, a aktualizace firmwaru jsou prováděny za použití ochranných mechanismů zajištěných samotným bootloaderem.
- Firmware balíčky od společnosti EVVA jsou podepsány asymetrickou metodou (RSA-SHA256) a symetricky zašifrovány a dodávány správě systému Xesar. Řetězec certifikátů se ověřuje jak ve správním softwaru, tak v aplikaci údržby.
- Pro aktualizaci v instalaci se používá šifrování AEAD s 256bitovými klíči AES (AES-CCM). Klíč k aktualizaci firmwaru je generován správním softwarem Xesar pomocí zabezpečeného postupu specificky pro danou instalaci a je neznámým zákaznickým tajemstvím společnosti EVVA.
- Po instalaci do systému může aktualizaci firmwaru na komponentách provádět pouze více uživatelů.
- V případě firmwaru pro NRF52 MC je tento navíc také:
  - podepsán asymetrickou metodou (RSA-SHA256, 2048bitový klíč) a ověřen přímo na MC.
  - zabezpečený metodou šifrování AEAD (AES-CCM), která používá 256bitový klíč AES.
- Firmware komponent nově přidaných do instalace se automaticky aktualizuje na poslední verzi firmwaru známou správcovskému softwaru nebo aplikaci údržby.
- Upozornění a kontrola aktualizací dostupných společností EVVA jsou podporovány a umožněny správcem instalace Xesar a aplikací údržby Xesar.

Přehled mobilního uzamykání



Mobilní aplikace Xesar (aplikace Xesar)



Rozhraní a komunikace

- Veškerá komunikace s XMS nebo cloudovým úložištěm je zabezpečena TLS.
- Všechny transakce mezi systémem Xesar a aplikací Xesar jsou ověřovány na základě protokolu výměny klíčů (X25519), funkce odvozování klíčů a ověřovacích kódů zpráv (HKDF-SHA256) End-to-End.
- Veškerá komunikace mezi komponentou Xesar a mobilní aplikací pro přenos přístupových dat je chráněna proti přehrávání a v rámci relace je šifrována
- Zálohování databáze
- Pokud je to koncovým zařízením podporováno, ukládá se citlivý materiál klíče do zabezpečených pamětí poskytnutých hardwarem
  - Android: StrongBox, pokud je dostupný, svázán s konkrétním zařízením, záloha do cloudu je deaktivována prostřednictvím manifestu
  - iOS: CryptoKit klíčenka, použitelná výhradně na konkrétním zařízení, synchronizace s iCloudem je deaktivována pomocí provisioning profile
- Všechny údaje jsou na mobilním zařízení uloženy v dodatečně šifrované databázi
- Přístupová data systému Xesar jsou tímto již předem zašifrována a mobilní aplikace je nemůže dešifrovat, kontrolovat ani manipulovat s nimi.
- Bezpečnostní pokyny
- Mobilní aplikace by se měla stahovat ve své původní podobě podepsané společností EVVA výhradně z oficiálního obchodu (tj. Google Play, Apple App Store)
- Společnost EVVA doporučuje všem uživatelům mobilní aplikace
  - používání koncových zařízení s hardwarově podporovanými bezpečnostními paměťmi
  - Používání šifrování paměti
  - Používání zabezpečení koncového zařízení heslem, PIN kódem nebo biometrickým přihlášením

Mobilní podpora systému Xesar (XMS)

Datové centrum

- Služba je provozována na serverech společnosti EVVA, které jsou umístěny formou kolokace v datových centrech v Rakousku, jež jsou fyzicky oddělená a certifikována podle normy ISO 27001.
- Všechny potřebné zdroje jsou navrženy redundantně a umožňují horizontální škálování
- Všechny koncové body služby jsou chráněny firewallem s moderními ochrannými mechanismy (IDS, IPS a ochrana proti DoS útokům).

Rozhraní a komunikace

- Veškerá komunikace se systémem XMS je zabezpečena protokolem TLS > 1.2.
  - MQTT Broker (mqtts://mqtt.akx.cloud:443)
    - Seznam povolených certifikátů TLS viz broker MQTT
  - Koncový bod REST (https://mss.akx.cloud)
    - Pro autentizaci a autorizaci správního softwaru Xesar
    - Seznam povolených algoritmů TLS REST

- XMS je výhradně „reléová stanice“ mezi systémem Xesar a registrovaným smartphonem s aplikací Xesar
  - Všechny transakce mezi systémem Xesar a registrovaným smartphonem s aplikací Xesar jsou end-to-end autentizovány pomocí protokolu pro výměnu klíčů (X25519), funkce pro odvození klíče (HKDF-SHA256) a autentizačních kódů zpráv.
  - Díky tomu nemohou být transakce nikdy iniciovány nebo manipulovány prostřednictvím systému XMS ani jinými systémy Xesar.

Ukládání dat, zálohování dat a obnovení po havárii

- Ukládají se pouze data, která jsou potřebná pro funkci
- Data se dočasně ukládají pouze po omezenou dobu a v zašifrované podobě pro přenos mezi systémem Xesar a smartphonem registrovaným s aplikací Xesar.
  - Registrace: 48h
  - Aktualizace oprávnění: 16 dní
- Přístupová data, která jsou poskytována systémem Xesar, jsou již před přenosem na místě šifrována pouze pro smartphone registrovaný v aplikaci Xesar (AES-GCM-256). Tato data nelze otevřít pomocí služby XMS, společnosti EVVA ani jiných systémů Xesar.
- Data jsou v současné době redundantně ukládána v certifikovaných cloudových datových centrech v zóně západní Německo. Architektura je navržena tak, aby ji bylo možné rozšířit pro cílené ukládání do jiných regionů/zón.
- V případě katastrofy, která se týká celé zóny, lze ukládání přesměrovat a aktualizaci přístupů opět provést pomocí správy Xesar On-Premises.
- Byla přijata organizační opatření pro omezený a výhradně autorizovaný přístup k uloženým údajům
  - Přísně kontrolovaná přístupová práva pro personál obsluhy a podpory u společnosti EVVA
  - Přísné řízení tajemství pro zavádění a provoz (SecDevOps)

Monitorování a alarmy

- Provoz servisních komponent je neustále monitorován a obsluha je upozorňována na odchylky.
  - K tomuto účelu vytvořené předpisy jsou průběžně kontrolovány a zlepšovány.
- Komponenty služby podléhají nepřetržitému monitorování CVE a v případě scénářů ohrožení jsou včas aktualizovány.

Zásady ochrany osobních údajů

- Při vývoji bylo pracováno podle principu Privacy by Design
- Zákazníci ani osobní údaje systému Xesar se nikdy neukládají v kontextu systému XMS
- Data, která jsou přenášena ze systému Xesar na smartphone registrovaný s aplikací Xesar
  - neobsahují žádné osobní údaje
  - nemohou být v žádném případě viditelné ze strany služby XMS, společnosti EVVA nebo jiných systémů Xesar
  - Telefonní čísla mobilních koncových zařízení se používají výhradně pro volání poskytovateli SMS služeb, ale nejsou ukládána službou XMS.

Mechanické bezpečnostní prvky přístupových komponent Xesar

Kování

Přehled mechanických bezpečnostních prvků kování Xesar.

Úspěšné certifikace

- EN 1634-1: 90 minut
- EN 1634-3
- EN 179
- EN 1906
- se stabilizační deskou DIN 18257: ES0
- ÖNORM 3859: 90 minut

Ochrana před vlivy prostředí

- IP 52 (IP55 s nalepeným těsněním) Ochrana proti vniknutí škodlivého prachu a stříkající vody v instalovaném stavu
- Lakovaná elektronika proti oxidaci kondenzovanou vodou
- Podmínky použití: -20 °C - +55 °C
- 3 baterie v bezpečném vnitřním prostoru

Fyzická bezpečnost

- Vícenásobné šroubové spojení
  - Mechanická ochrana proti neoprávněné manipulaci
  - Volně se otáčející vnější klika

Dveřní klika

Přehled mechanických bezpečnostních prvků dveřní kliky Xesar.

Úspěšné certifikace
- EN 1634-1: 90 minut
- EN 179
- EN 1906
- ÖNORM 3859: 90 minut
- Certifikace CE

Ochrana před vlivy prostředí
- Rozsah vlhkosti vzduchu: 90% při 0 °C
- Okolní teplota uvnitř: +5 °C až +50 °C
- IP 40

Fyzická bezpečnost
- Volně se otáčející vnější klika

Cylindrická vložka

Úspěšné certifikace
- EN15684 16B30D3D
- SKG***
- SSF3522 pro skandinávské profily
- Certifikace požární ochrany EN1634 (90 min)
- Paniková certifikace EN179/1125
- ÖNORM B 5351:2011 WMZ6-BZ
- Certifikace CE

Ochrana před vlivy prostředí
- Ochrana IP65 před škodlivým vniknutím prachu a stříkající vody při montáži podle montážního návodu Xesar
- Lakovaná elektronika proti oxidaci kondenzovanou vodou
- Rozsah vlhkosti vzduchu: 90% při 0 °C
- Podmínky použití: -20 °C - +55 °C
- 2 baterie paralelně pro vyšší stabilitu napájení

Fyzická bezpečnost
- Volně se otáčející vnější hlavice
- Ochrana proti odvrtání
- a proti vytažení jádra
- Rotační brzda proti napadení vysokofrekvenčním vřetenem
- Definovaný bod zlomu na závitu vnějšího knoflíku pro ochranu jádra před mechanickými útoky a pro zabránění napadení
- Speciální mechanický nástroj pro montáž a demontáž knoflíku cylindrické vložky

Architektonická bezpečnost
- Cylindrická vložka Xesar se skládá z hlavice cylindrické vložky a modulu cylindrické vložky, který se nachází za ochranou proti odvrtání.
- Hlavice a modul jsou vzájemně propojeny kryptografickým zabezpečením:
  - Uvolnění probíhá výhradně v mechanicky „bezpečném“ úseku
  - jednoduchá výměna hlavice neumožňuje neoprávněný přístup

Nástěnná čtecí jednotka (online, offline)

Úspěšné certifikace
› Certifikace CE

Ochrana před vlivy prostředí
› Rozsah vlhkosti vzduchu 90% při 0 °C
› Okolní teplota -25 °C až +70 °C
› Stupeň krytí IP65

Fyzická bezpečnost
› Pravé sklo vpředu

Architektonická bezpečnost
› Nástěnná čtecí jednotka Xesar se skládá z nástěnné čtecí jednotky a řídicí jednotky nástěnné čtecí jednotky, která se nachází v zabezpečeném úseku.
› Online nástěnná čtecí jednotka se skládá z nástěnné čtecí jednotky a online řídicí jednotky, která se nachází v zabezpečeném úseku.
› Čtecí jednotka a řídicí jednotka jsou vzájemně propojeny kryptografickým zabezpečením:
  • Uvolnění probíhá výhradně v „bezpečném“ úseku
  • Jednoduchá výměna nástěnné čtecí jednotky neumožňuje neoprávněný přístup

Další obecné bezpečnostní prvky

Přístupové komponenty (přístupové místo):
› Přiřazení přístupové místa k úsekům a oprávnění pro úseky
› Blokovací seznam pro zakázaná přístupová média
› Delete-Key – deaktivace zablokovaných přístupových médií, která se nacházejí na seznamu blokovaných komponent
› Office modes (trvalé otevření komponent)
  • Manuální trvalé otevření komponent
  • Automatické trvalé otevření, časově řízené mezi dvěma definovanými okamžiky (začátek a konec)
  • Automatické ukončení trvalého otevření v definovaných okamžicích, ve kterých jsou ukončena také manuální trvalá otevření (pouze konec)
  • Obchodní režim: Automatické trvalé otevření, spustí se až po oprávněném přístupu
› Protokol událostí pro události přístupu, odmítnutí a Office mode
› Časové omezení pro oprávnění k přístupu

Přístupová média:
› Virtuální síť umožňuje přenos dat přes přístupová média, popř. jejich používání osobami v instalaci.

Software pro správu:
› Definovaný profil s oprávněním pro uživatele s různými uživatelskými právy (skupina uživatelů)
› Definovaná zobrazení ovládacího panelu pro uživatele podle uživatelských práv (skupina uživatelů)
› Stav instalace na ovládacím panelu
  • komponenty:
    - potřebné aktualizace firmwaru
    - potřebné aktualizace konfigurace
    - zobrazení stavu baterie
    - okamžitý online stav přístupového místa s online EVVA komponenty
    - stav připojení
    - stav dveřních kontaktů
  • Přístupové komponenty a média:
    - nezabezpečená místa instalace
    - přístupová média, která vyžadují aktualizaci
    - nezabezpečená blokovaná přístupová média
    - uvolnění, která byla provedena se zablokovanými přístupovými médii
› Systémový protokol pro sledovatelnost změn konfigurace v softwaru pro správu

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