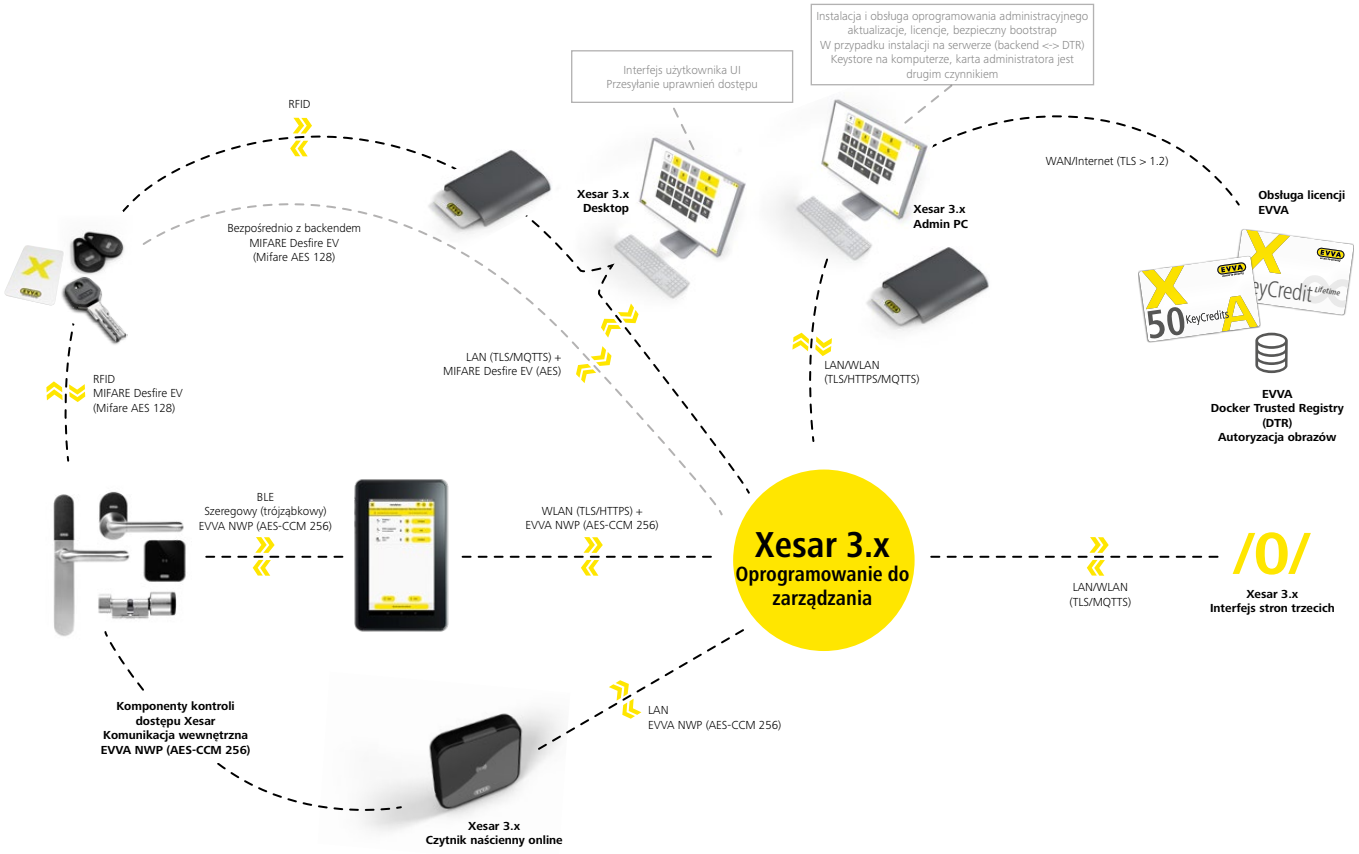
Koncepcja bezpieczeństwa Xesar

Przegląd najważniejszych cech bezpieczeństwa systemu kontroli dostępu Xesar

Cyberbezpieczeństwo Xesar



Nośniki dostępu (Xesar 3)

Interfejs i komunikacja

Do komunikacji między komponentami dostępu a nośnikami dostępu we wszystkich przypadkach stosowana jest metoda szyfrowania MIFARE AES z 128-bitowym szyfrowaniem AES.

- Klucz aplikacji do uprawnienia dostępu jest generowany w bezpieczny sposób podczas instalacji systemu Xesar. Jest on tajemnicą klienta i nie jest znany firmie EVVA.
- Jest on zapisywany w formie trwałej i zaszyfrowanej tylko w ramach instalacji usługi bezpieczeństwa.
- W przypadku zastosowanej metody MIFARE do każdej interakcji wykorzystywana jest sesja z własnym losowo wygenerowanym kluczem.

Magazyn danych

W systemie Xesar stosowane są wyłącznie bezpieczne nośniki dostępu z zabezpieczoną pamięcią danych

- Mifare Desfire EV1 z certyfikatem EAL4+ lub
- Mifare Desfire EV2/EV3 z certyfikatem EAL5+

Wskazówki bezpieczeństwa

- Aby zapobiec manipulacjom, nośnik dostępu powinien być dodawany do systemu Xesar po raz pierwszy wyłącznie przez upoważnionego użytkownika korzystającego ze stacji kodującej w chronionej lokalizacji.
- Nośnik fabryczny jest identyczny na całym świecie i może być stosowany wszędzie w celu uzyskania dostępu do komponentu kontroli dostępu Xesar w stanie fabrycznym lub w trybie serwisowym. W związku z tym nie można za jego pomocą przeprowadzić kontroli dostępu.
- Nośnik dostępu z uprawnieniem klucza generalnego można przekazywać tylko w wyjątkowych przypadkach i zaufanym osobom. Powód: nośnik dostępu z tym profilem uprawnień ma
  - nieograniczony okres ważności (maks. okres ważności – patrz podręcznik)
  - Dostęp do wszystkich komponentów dostępu instalacji, nawet jeśli zostaną one dodane/utworzone dopiero po wydaniu tego nośnika.

Nośnik dostępu z uprawnieniem klucza generalnego należy przechowywać w bezpiecznym miejscu, poza zabezpieczoną instalacją, aby w sytuacji awaryjnej umożliwić dostęp do niej.

Oprogramowanie administracyjne

Dostawa

- Wszystkie dostarczane przez firmę EVVA cyfrowe komponenty systemu posiadają ważną i opatrzoną stemplem czasowym sygnaturę kodową.
- Interfejs i komunikacja
- Każda komunikacja z systemem administracyjnym Xesar jest zabezpieczona protokołem TLS > 1.2, listę dozwolonych algorytmów TLS można znaleźć na stronie Cipher Suites.
  - do zarządzania instalacją przez wielu użytkowników za pośrednictwem przeglądarki
  - do podłączenia Menedżera Urządzeń Peryferyjnych (rozproszona stacja kodująca),
  - do interakcji z usługami będącymi elementami instalacji
  - do interakcji z interfejsem systemu zewnętrznego

Uwierzytelnianie

W stosownych przypadkach przestrzegano wytycznych OWASP.

- Uwierzytelnianie w celu zarządzania instalacją poprzez dostęp do przeglądarki jest chronione hasłem:
  - Pierwsze hasło administratora jest generowane losowo podczas instalacji (brak wartości domyślnych)
  - Wszystkie utworzone hasła muszą mieć minimalną długość i posiadać wskaźnik jakości (zxcvbn: Low-Budget Password Strength Estimation)
  - Hasła nigdy nie są zapisywane w formie tekstowej (BCrypt)
  - Odpowiedzi na niepowodzenia w trakcie uwierzytelniania są celowo udzielane w sposób ogólny
- Uwierzytelnianie na interfejsach serwisowych jest oparte na certyfikacie z mTLS:
  - do podłączenia Menedżera urządzeń peryferyjnych
  - w przypadku wewnętrznych połączeń z usługami, które są elementami instalacji

- podczas łączenia się z interfejsem systemowym innej firmy za pośrednictwem brokera MQTT; w tym przypadku dodatkowo token jest używany dla wewnętrznego interfejsu

Autoryzacja

- W obszarze zarządzania systemem Xesar można zdefiniować uprawnienia użytkownika poprzez grupy użytkowników, które następnie można łatwo przypisać do poszczególnych użytkowników
- Odpowiednie działania użytkownika są rejestrowane w systemie
- Autoryzacja i protokołowanie działają również dla użytkowników interfejsu

Magazyn danych

- Wszystkie wrażliwe dane (np. klucze, hasła) są przechowywane wyłącznie w instalacji usługi bezpieczeństwa („sejfie") i tylko w postaci zaszyfrowanej.
- Podczas uruchamiania instalacji sejf jest „otwierany" do działania za pomocą dwóch czynników (karty administratora i zaszyfrowanego magazynu kluczy AdminPC).
  - Niewrażliwe dane instalacji i konfiguracji są zapisywane w bazie danych, która nie jest szyfrowana (patrz wskazówki bezpieczeństwa).
  - Ze względu na projekt architektoniczny oprogramowania zarządzającego, w którym modele odczytu i zapisu są oddzielone, wszystkie zmiany są zapisywane jako sekwencja zdarzeń (CQRS-ES). Zwiększa to przejrzystość i utrudnia manipulowanie bazami danych.

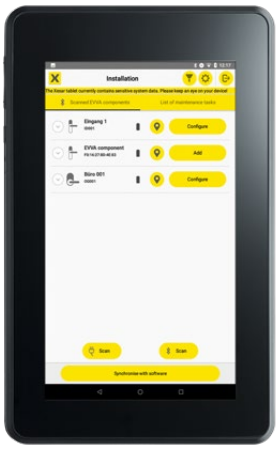
Wskazówki bezpieczeństwa

- Do instalacji systemu należy używać wyłącznie niezmodyfikowanych elementów dostarczonych przez firmę EVVA. Autentyczność i integralność wszystkich artefaktów dostarczanych przez firmę EVVA można sprawdzić za pomocą podpisu.
- Odpowiedzialność za bezpieczne działanie oprogramowania administracyjnego Xesar spoczywa na kliencie;
  - Dostęp (uwierzytelnianie i autoryzacja) do środowiska serwera musi być zabezpieczony, aby nie można było po prostu manipulować niewrażliwymi danymi instalacyjnymi i konfiguracyjnymi.
  - Dostęp do zarządzania systemem powinien być zapewniony przez wyraźnie uwierzytelnionych i odpowiednio upoważnionych użytkowników.
  - Utworzone konta instalacyjne powinny być używane tylko podczas instalacji, a następnie wyłącznie w wyjątkowych przypadkach (np. resetowanie hasła, odzyskiwanie).
- Karta bezpieczeństwa instalacji, która jest generowana dla przypadków odzyskiwania podczas instalacji, powinna być przechowywana wyłącznie w formie drukowanej w bezpiecznym miejscu (np. sejfie).

Wskazówki na temat ochrony danych

- Podczas aktywacji rejestracji osobistych danych dostępowych należy znać i przestrzegać przepisów o ochronie danych obowiązujących w danym kraju.
- Automatyczne anulowanie odniesienia osoby do danych dostępu można odpowiednio skonfigurować za pomocą oprogramowania zarządzającego. Informacje na temat możliwości i sposobu postępowania w oprogramowaniu można znaleźć w podręczniku.

Komponent konserwacyjny (tablet Xesar)



Interfejs i komunikacja

- Aby dodać nowy komponent Xesar do systemu Xesar, klucz instalacyjny jest szyfrowany metodą szyfrowania AEAD i 128-bitowym kluczem AES. Klucz ten jest wyprowadzany z kodu PIN jako drugiego czytnika - nie przechowywanego w urządzeniu, za pomocą funkcji kryptograficznego wyprowadzania klucza (KDF, AES-CMAC-PRF-128).
- Dane konfiguracyjne komponentów w instalacji są przesyłane w formie zaszyfrowanej za pomocą szyfrowania AEAD i specyficznego dla komponentu 256-bitowego klucza AES (patrz również Cyberbezpieczeństwo komponentów Xesar).

Wskazówki bezpieczeństwa

- Dostarczony przez firmę EVVA tablet serwisowy powinien być używany wyłącznie do celów konserwacji systemu.
- Na tym tablecie nie należy instalować żadnych innych aplikacji.
- W przypadku wprowadzania nowych komponentów Xesar dane konfiguracyjne są zabezpieczone kodem PIN. Należy go:
  - skonfigurować po zainstalowaniu w ustawieniach systemu, aby system nie używał wartości domyślnej (tj. 0000).
  - udostępniać tylko znanym i zaufanym osobom
- Rejestracja w Google nie jest wymagana do korzystania z Xesar.
- Komunikacja sieciowa (WLAN) powinna być aktywowana tylko wtedy, gdy jest to wymagane i powinna być używana bezpieczna sieć prywatna (tj. nie Internet).
- Należy instalować wyłącznie aktualizacje systemu zalecane i przetestowane przez firmę EVVA.

Komponenty dostępowe

Interfejs i komunikacja

- Do komunikacji z komponentem we wszystkich przypadkach (bezprzewodowo i szeregowo) stosowana jest metoda szyfrowania AEAD z 256-bitowymi kluczami AES (AES-CCM).
- Klucz komunikacyjny jest w bezpieczny sposób generowany specjalnie dla każdego komponentu w oprogramowaniu zarządzającym Xesar i jako tajemnica klienta nie jest znany dla EVVA.
- Po wprowadzeniu do instalacji tylko użytkownik może dokonywać zmian stanu lub konfiguracji komponentów
- Materiał klucza można zaktualizować w komponencie z odpowiednim zabezpieczeniem (uwierzytelnianie, szyfrowana transmisja)
- Ze względu na wielkość klucza z zastosowaniem symetrycznych metod, ataki siłowe nie są łatwe do przeprowadzenia nawet w czasie postkwantowym. W przypadku komponentów zasilanych bateryjnie, zasilanie umożliwi również tylko niewielką część wymaganych testów ze względu na kombinatorykę, zwłaszcza na łączu radiowym.

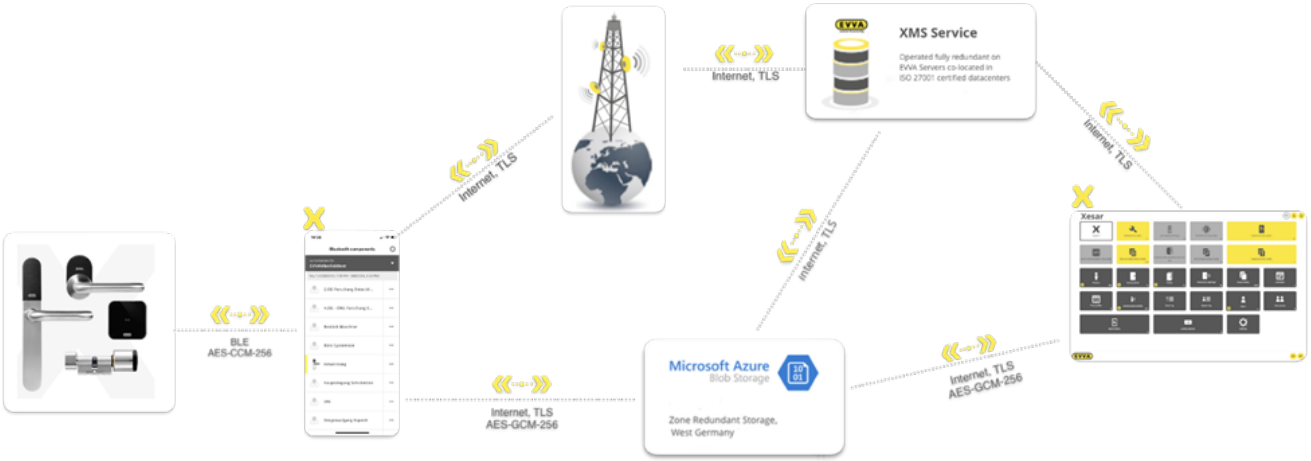
Magazyn danych

- Materiał klucza, wrażliwa konfiguracja i kod aplikacji są zapisywane na odpowiednim mikrokontrolerze (MC) z najlepszym możliwym zabezpieczeniem MC (NVRAM, wewnętrzna pamięć flash)
  - Rodzina PIC24: Ogólna ochrona segmentów i ochrona segmentów kodu (Family Datasheet, 29.4)
  - NRF52: Ochrona portu dostępu kontrolowana sprzętowo (APPPROTECT)
  - Obudowa chroni przed nieinwazyjnym dostępem do MC (patrz również bezpieczeństwo mechaniczne komponentów Xesar)
- Dane systemowe są zapisywane na komponencie w pamięci (EEPROM lub Flash) i zabezpieczane integralnością za pomocą metody kryptograficznej z 128-bitowym kluczem AES (AES-CMAC).

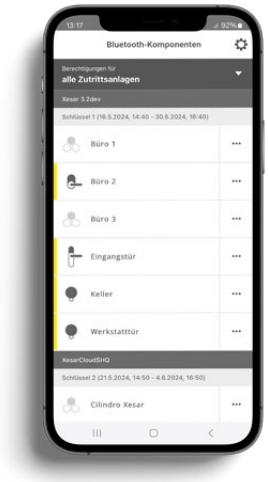
Firmware i aktualizacja

- Istniejący firmware jest załadowany bootloaderem, który nie może być zmieniony fabrycznie i może być aktualizowany przez bootloader z odpowiednimi zabezpieczeniami.
- Pakiety firmware firmy EVVA są podpisywane metodą asymetryczną (RSA-SHA256) i dostarczane do systemu administracyjnego Xesar w postaci symetrycznie zaszyfrowanej. Łańcuch certyfikatu jest weryfikowany zarówno w oprogramowaniu administracyjnym, jak i w aplikacji konserwacyjnej.
- Do aktualizacji w instalacji stosowana jest metoda szyfrowania AEAD z 256-bitowymi kluczami AES (AES-CCM). Klucz aktualizacji firmware jest w bezpieczny sposób generowany specjalnie dla danej instalacji przez oprogramowanie administracyjne Xesar i jest nieznaną firmie EVVA tajemnicą klienta.
- Po wprowadzeniu do instalacji tylko użytkownik może przeprowadzić aktualizację firmware na komponentach.
- W przypadku firmware dla NRF52 MC dodatkowo:
  - firmware podpisywany jest metodą asymetryczną (RSA-SHA256, 2048-bitowy klucz) i weryfikowany bezpośrednio na MC.
  - firmware zabezpieczane jest metodą szyfrowania AEAD (AES-CCM) z wykorzystaniem 256-bitowego klucza AES.
- Oprogramowanie sprzętowe komponentów dodawanych do instalacji jest automatycznie aktualizowane do najnowszej wersji znanej oprogramowaniu zarządzającemu lub aplikacji konserwacyjnej.
- Menedżer instalacji Xesar oraz aplikacja konserwacyjna Xesar wspierają i umożliwiają wyświetlanie wskazówek i sprawdzanie aktualizacji dostępnych w firmie EVVA.

Przegląd blokowania mobilnego



Aplikacja mobilna Xesar (aplikacja Xesar)



Interfejsy i komunikacja

- Wszelka komunikacja z XMS lub pamięcią w chmurze jest zabezpieczona protokołem TLS.
- Wszystkie transakcje między instalacją Xesar a aplikacją Xesar są uwierzytelniane od początku do końca na podstawie protokołu wymiany kluczy (X25519), funkcji wyprowadzania kluczy i kodów uwierzytelniania wiadomości (HKDF-SHA256).
- Każda komunikacja między komponentem Xesar a aplikacją mobilną do przesyłania danych dostępowych jest zabezpieczona przed odtwarzaniem i szyfrowana w ramach sesji
- Zapisywanie danych
- Jeśli urządzenie końcowe to obsługuje, wrażliwe materiały kluczowe są zapisywane w bezpiecznych pamięciach udostępnionych przez sprzęt
  - Android StrongBox, jeśli jest dostępny, przypisany do urządzenia, kopia zapasowa w chmurze wyłączona przez Manifest
  - iOS: zestaw kluczy CryptoKit, do użytku wyłącznie na urządzeniu, synchronizacja iCloud z profilem udostępniania wyłączona
- Wszystkie dane są zapisywane w dodatkowo zaszyfrowanej bazie danych na urządzeniu mobilnym
- Dane dostępowe systemu Xesar są już wcześniej zaszyfrowane i nie mogą być deszyfrowane, kontrolowane ani manipulowane przez aplikację mobilną.
- Wskazówki bezpieczeństwa
- Aplikacja mobilna powinna być pobierana w oryginalnej formie podpisanej przez firmę EVVA wyłącznie z oficjalnego sklepu (tj. Google Play, Apple App Store)
- EVVA zaleca wszystkim użytkownikom aplikacji mobilnej
  - korzystanie z urządzeń końcowych z pamięciami bezpieczeństwa wspomaganymi sprzętowo
  - Korzystanie z szyfrowania pamięci
  - Korzystanie z zabezpieczenia urządzenia końcowego za pomocą hasła, kodu PIN lub logowania biometrycznego

Mobilne wsparcie techniczne Xesar (XMS)

Centrum danych

- Usługa jest obsługiwana na serwerach EVVA, które są umieszczone w certyfikowanych zgodnie z ISO 27001, fizycznie oddzielnych centrach danych w Austrii za pomocą certyfikatów kolokacji.
- Wszystkie potrzebne zasoby są redundantne i mogą być skalowane poziomo
- Wszystkie punkty końcowe usług znajdują się za zaporą sieciową z najnowocześniejszymi mechanizmami ochronnymi (IDS, IPS i DoS).

Współpraca i komunikacja

- Wszelka komunikacja z XMS jest zabezpieczona przy użyciu TLS > 1.2.
  - Broker MQTT (mqtts://MQTT.akx.cloud:443)
    - Lista dozwolonych certyfikatów TLS, patrz broker MQTT

- Punkt końcowy REST (https://mss.akx.cloud)
  - Do uwierzytelniania i autoryzacji oprogramowania administracyjnego Xesar
  - Lista dozwolonych algorytmów TLS REST

› XMS jest wyłącznie „stacją przekaźnikową" pomiędzy systemem Xesar a zarejestrowanym smartfonem z aplikacją Xesar
- Wszystkie transakcje między instalacją Xesar a zarejestrowanym smartfonem z aplikacją Xesar są uwierzytelniane end-to-end na podstawie protokołu wymiany kluczy (X25519), funkcji wyprowadzania kluczy i kodów uwierzytelniania wiadomości (HKDF-SHA256).
- Transakcje nie mogą być zatem nigdy inicjowane ani manipulowane przez XMS lub inne systemy Xesar.

Pamięć danych, tworzenie kopii zapasowych i awaryjne przywracanie danych

› Przechowywane są wyłącznie te dane, które są niezbędne do działania funkcji
› Dane są przechowywane tymczasowo tylko przez ograniczony czas i w zaszyfrowanej formie, na potrzeby przenoszenia między systemem Xesar a zarejestrowanym smartfonem z aplikacją Xesar.
- Rejestracja: 48h
- Aktualizacja uprawnień: 16 dni

› Dane dostępowe dostarczane przez system Xesar są szyfrowane (AES-GCM-256) tylko dla zarejestrowanego smartfona z aplikacją Xesar, zanim zostaną przesłane lokalnie. Te dane nie mogą być otwierane przez XMS-Service, EVVA ani inne systemy Xesar.
› Dane są obecnie przechowywane redundantnie w certyfikowanych centrach danych w chmurze, w strefie Niemiec Zachodnich. Architektura została zaprojektowana w taki sposób, aby można ją było rozbudować w celu ukierunkowanego przechowywania w innych regionach/strefach.
› W przypadku katastrofy, która dotyczy całej strefy, można przekierować zapisywanie i ponownie przeprowadzić aktualizację dostępów za pomocą systemu zarządzania Xesar On-Premises.
› Podjęto środki organizacyjne mające na celu zapewnienie ograniczonego i wyłącznie autoryzowanego dostępu do przechowywanych danych
- Ściśle kontrolowane uprawnienia dostępu dla personelu operatorskiego i wsparcia technicznego w firmie EVVA
- Rygorystyczne zarządzanie tajemnicami wdrożeniowymi i operacyjnymi (SecDevOps)

Monitorowanie i alarmy

› Działanie komponentów serwisowych jest stale monitorowane, a personel obsługujący jest ostrzegany w przypadku odchyleń.
- Ustanowione w tym celu przepisy są stale sprawdzane i ulepszane.

› Komponenty serwisowe podlegają ciągłemu monitorowaniu CVE i w przypadku scenariuszy zagrożeń są szybko aktualizowane.

Wskazówki na temat ochrony danych

› Projekt został opracowany zgodnie z zasadą Privacy by Design
› XMS nigdy nie zapisuje danych osobowych ani danych klientów w sposób powiązany z systemem Xesar
› Dane, które przesyłane są z systemu Xesar do zarejestrowanego smartfona z aplikacją Xesar
- nie zawierają żadnych danych osobowych
- nie mogą być przeglądane przez usługę XMS, EVVA lub inne systemy Xesar
- Numery telefonów z mobilnych urządzeń końcowych są wykorzystywane wyłącznie do połączenia z dostawcą usług SMS, ale nie są zapisywane przez usługę XMS.

Mechaniczne cechy bezpieczeństwa komponentów kontroli dostępu Xesar

Okucie

Przegląd mechanicznych cech bezpieczeństwa okucia Xesar.

Uzyskane certyfikaty

› EN 1634-1: 90 minut
› EN 1634-3
› EN 179
› EN 1906
› z płytą stabilizującą DIN 18257: ES0
› ÖNORM 3859: 90 minut

Ochrona przed wpływami atmosferycznymi

› IP 52 (IP55 z naklejaną uszczelką) Ochrona – w stanie wbudowanym – przed wnikaniem szkodliwego pyłu i strumienia wody
› Powlekane układy elektroniczne chroniące przed utlenianiem spowodowanym kondensacją
› Warunki eksploatacji: od -20°C do +55°C
› 3 baterie w bezpiecznym wnętrzu

Bezpieczeństwo fizyczne
- Wielokrotne złącza śrubowe
  - Mechaniczna ochrona przed manipulacją
  - Swobodna klamka

Klamka

Przegląd mechanicznych cech bezpieczeństwa klamki Xesar.

Uzyskane certyfikaty
- EN 1634-1: 90 minut
- EN 179
- EN 1906
- ÖNORM 3859: 90 minut
- Certyfikat CE

Ochrona przed wpływami atmosferycznymi
- Zakres wilgotności powietrza: 90% przy 0°C
- Temperatura otoczenia wewnątrz: od +5°C do +50°C
- IP 40

Bezpieczeństwo fizyczne
- Swobodna klamka

Wkładka

Uzyskane certyfikaty
- EN15684 16B30D3D
- SKG***
- SSF3522 dla profilu skandynawskiego
- EN1634, certyfikat ognioodporności (90 min)
- EN179/1125, certyfikat funkcji antypanicznej
- ÖNORM B 5351:2011 WMZ6-BZ
- Certyfikat CE

Ochrona przed wpływami atmosferycznymi
- IP65 – ochrona przed wnikaniem szkodliwych pyłów i silnych strumieni wody z dowolnego kierunku
- Powlekane układy elektroniczne chroniące przed utlenianiem spowodowanym kondensacją
- Zakres wilgotności powietrza: 90% przy 0°C
- Warunki eksploatacji: od -20°C do +55°C
- 2 równoległe baterie dla większej stabilności zasilania

Bezpieczeństwo fizyczne
- Swobodnie obracająca się głowica
- Zabezpieczenie przed rozwierceniem
- Zabezpieczenie przed wyciągnięciem rotora
- Hamulec rotacyjny przeciw ingerencjom z użyciem wrzeciona frezarskiego wysokiej częstotliwości
- Wyznaczone miejsce zniszczenia na gwincie gałki zewnętrznej chroni rdzeń przed ingerencją mechaniczną i zniszczeniem zamka (snapping)
- Specjalne narzędzie mechaniczne do montażu i demontażu gałki z wkładką

Architektura Bezpieczeństwa
- Wkładka Xesar składa się z gałki i modułu wkładki, który znajduje się za zabezpieczeniem przed rozwierceniem.
- Gałka i moduł są ze sobą połączone przez zabezpieczenie kryptograficzne:
  - Stałe otwarcie odbywa się wyłącznie w strefie mechanicznie „bezpiecznej”
  - Prosta wymiana gałki nie umożliwia nieuprawnionego dostępu

Czytnik naścienny (online, offline)

Uzyskane certyfikaty
› Certyfikat CE

Ochrona przed wpływami atmosferycznymi
› Zakres wilgotności powietrza 90% przy 0°C
› Temperatura otoczenia od -25°C do +70°C
› Stopień ochrony IP65

Bezpieczeństwo fizyczne
› Szklany front

Architektura Bezpieczeństwa
› Czytnik naścienny Xesar składa się z jednostki naściennej i panelu sterowania, który znajdują się w bezpiecznej strefie.
› Czytnik ścienny online składa się z jednostki naściennej i panelu sterowania online, który znajduje się w strefie bezpiecznej.
› Jednostka czytnika i jednostka sterująca są ze sobą połączone za pomocą zabezpieczenia kryptograficznego:
  • Stałe otwarcie odbywa się wyłącznie w strefie „bezpiecznej"
  • Prosta wymiana czytnika naściennego nie umożliwia nieuprawnionego dostępu

Inne ogólne funkcje bezpieczeństwa

Komponenty dostępu (miejsca instalacji):
› Przyporządkowanie miejsc instalacji do stref i uprawnienia do stref
› Lista blokad dla zablokowanych nośników dostępu
› Delete-Key – dezaktywacja zablokowanych nośników dostępu znajdujących się na liście blokowanych komponentów
› Tryby Office (stałe otwarcie komponentów)
  • Ręczne stałe otwarcie komponentów
  • Automatyczne stałe otwarcie, sterowane czasowo pomiędzy dwoma określonymi okresami czasowymi (początek i koniec)
  • Office Mode End w określonych okresach czasowych, w których kończą się również Manual Office Mode (tylko koniec)
  • Tryb Shop: Automatyczne stałe otwarcie, uruchamiane dopiero po uprawnionym dostępie
› Protokół zdarzeń dla zdarzeń dostępu, odrzucenia i trybu Office
› Ograniczenie czasowe dla uprawnień dostępu

Nośniki dostępowe:
› Sieć wirtualna umożliwia transport danych za pomocą nośników dostępu lub ich wykorzystanie przez osoby w instalacji.

Oprogramowanie administracyjne:
› Zdefiniowane profile uprawnień dla użytkowników z różnymi uprawnieniami (grupa użytkowników)
› Zdefiniowane widoki pulpitu dla użytkowników według uprawnień użytkownika (grupa użytkowników)
› Stan instalacji na panelu sterowania
  • Składowe:
    - konieczne aktualizacje firmware
    - konieczne aktualizacje konfiguracji
    - wyświetlanie stanu baterii
    - terminowy status online miejsc instalacji dzięki komponentowi EVVA Online
    - status połączenia
    - stan styków drzwi
  • Komponenty dostępu i media:
    - niezabezpieczone miejsca instalacji
    - nośniki dostępu, które wymagają aktualizacji
    - niedostatecznie zablokowane nośniki dostępu
    - stałe otwarcia za pomocą zablokowanych nośników dostępu
› Protokół systemu umożliwiający prześledzenie zmian konfiguracji w oprogramowaniu administracyjnym

I.X.SJARC.ID.INFBL.SPL.LN