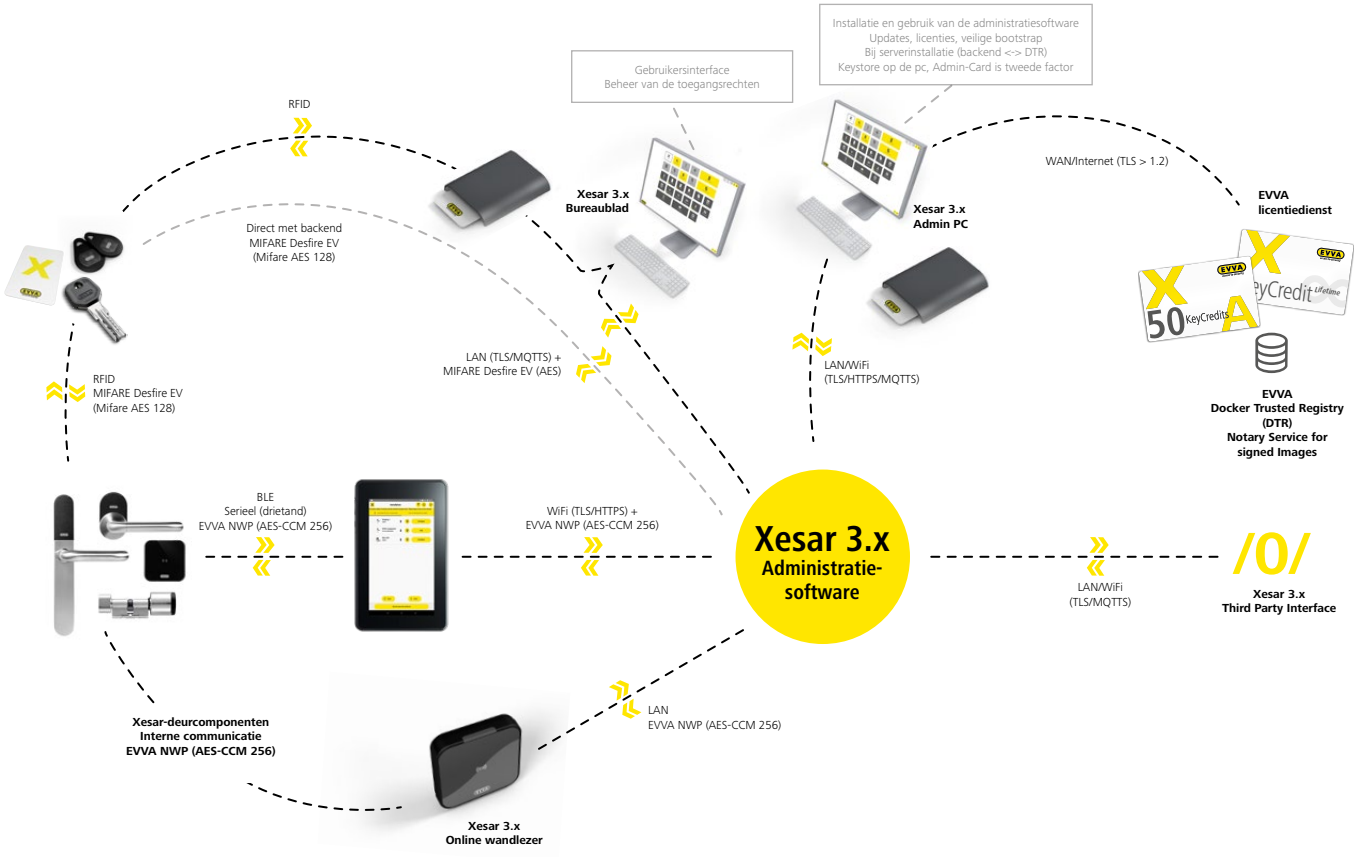
Xesar-veiligheidsconcept

Overzicht van de belangrijkste veiligheidstechnische kenmerken van een Xesar-toegangssysteem

Xesar-cyberbeveiliging



Toegangsmedia (Xesar 3)

Interface en communicatie

Voor de communicatie tussen deurcomponenten en toegangsmedia wordt in alle gevallen het MIFARE AES-coderingsmethode met 128-bits AES-encryptie gebruikt.

- De applicatiesleutel voor de toegangsrechten wordt tijdens de Xesar-installatie met een veilige procedure gegenereerd. Het is een klantengeheim dat EVVA niet kent.
- Het wordt alleen in de installatie van de beveiligingsservice in permantente vorm versleuteld opgeslagen.
- Bij het gebruikte MIFARE-proces wordt voor elke interactie een sessie met een eigen willekeurig gegenereerde sleutel gebruikt.

Gegevensopslag

Bij Xesar worden uitsluitend veilige toegangsmedia met beveiligde gegevensopslag gebruikt

- Mifare Desfire EV1 met EAL4+ certificering of
- Mifare Desfire EV2/EV3 met EAL5+ certificering

Veiligheidsaanwijzingen

- Een toegangsmedium voor het eerst aan een Xesar-installatie toevoegen mag – om manipulatie te voorkomen – alleen door een bevoegde beheerder met behulp van het codeerstation op een beveiligde plaats worden uitgevoerd.
- De opleversleutel is wereldwijd gelijk en overal bruikbaar voor toegang tot Xesar-deurcomponenten in de uitlever- of oplevermodus. Daarom kan hiermee geen toegangscontrole worden uitgevoerd.
- Een toegangsmedium met hoofdsleutelrechten mag alleen in uitzonderlijke gevallen en aan betrouwbare gebruikers worden overhandigd. Reden: een toegangsmedium met dit toegangsprofiel is
  - onbeperkt geldig (max. geldigheidsduur zie handboek)
  - Toegang tot alle deurcomponenten van de installatie, ook als deze pas na het verstrekken van dit medium worden toegevoegd/ aangemaakt.

Een toegangsmedium met hoofdsleutelrechten moet op een veilige plaats buiten het beveiligde systeem worden bewaard, zodat de installatie in geval van nood toegankelijk is.

Administratiesoftware

Levering

- Alle digitale componenten van het systeem die EVVA levert, zijn voorzien van een geldige codehandtekening met tijdstempel.
- Interface en communicatie
- Elke communicatie met het Xesar-beheer is beveiligd met TLS > 1.2, een lijst van de toegestane TLS-algoritmen vindt u op Cipher Suites.
  - voor het beheer van de installatie door meerdere gebruikers via browsertoegang
  - voor de aansluiting van de Periphery Manager (verdeeld codeerstation),
  - voor de interactie van de diensten die deel uitmaken van de installatie
  - voor interactie met de interface van systemen van derden

Authenticatie

De OWASP-richtlijnen werden hier algemeen – indien de toepassing zinvol is – gevolgd.

- De authenticatie voor het beheer van de installatie via de browsertoegang is beveiligd met een wachtwoord:
  - Het eerste beheerderswachtwoord wordt bij de installatie willekeurig gegenereerd (geen defaults)
  - Alle wachtwoorden die worden aangemaakt, moeten een minimumlengte hebben en er is een indicator voor de kwaliteit (zxcvbn: Low-Budget Password Strength Estimation)
  - Wachtwoorden worden nooit in leesbare tekst opgeslagen (BCrypt)
  - Fouten bij de authenticatie worden bewust generiek beantwoord
- De authenticatie op service-interfaces is op basis van certificaten met mTLS afgebeeld:
  - voor de aansluiting van de Periphery Manager
  - bij interne verbindingen van diensten die delen van de installatie zijn
  - bij de verbinding met de interface van het systeem van derden via de MQTT Broker; hier is een extra token nodig voor de interne verbinding

Autorisatie
- In het Xesar-beheer kunnen voor de autorisatie gebruikersrechten via gebruikersgroepen worden gedefinieerd. Vervolgens kunnen deze eenvoudig aan de betreffende gebruikers worden toegewezen
- De specifieke acties van een beheerder worden in het systeem geregistreerd
- De autorisatie en protocollering werken ook voor de interfacebeheerders

Gegevensopslag
- Alle gevoelige gegevens (bv. sleutelmateriaal, wachtwoorden) worden uitsluitend in de Security Service Installation (Vault) opgeslagen en alleen versleuteld bewaard.
- Bij de bootstrap van de installatie wordt via twee factoren (Admin-Card en op de admin-pc opgeslagen gecodeerde keystore) de vault voor het gebruik 'geopend'.
  - Niet-gevoelige gegevens van de installatie en de configuratie worden in een database opgeslagen, die niet versleuteld is (zie veiligheidsaanwijzingen).
  - Door het architectonische ontwerp van de administratiesoftware, waarin de lees- en schrijfmodellen gescheiden zijn, worden alle wijzigingen opgeslagen als een reeks gebeurtenissen (CQRS-ES). Dit verhoogt de traceerbaarheid en maakt manipulatie van de gegevensbestanden moeilijker.

Veiligheidsaanwijzingen
- Er mogen alleen ongewijzigde, door EVVA geleverde artefacten voor de installatie van het systeem worden gebruikt. De authenticiteit en integriteit van alle door EVVA geleverde artefacten kan door middel van een handtekening worden gecontroleerd.
- De verantwoordelijkheid voor het veilige gebruik van de Xesar-administratiesoftware ligt bij de klant;
  - de toegang (authenticatie en autorisatie) tot de serveromgeving moet worden beveiligd, zodat de niet-gevoelige gegevensbestanden van de installatie en configuratie niet eenvoudig te manipuleren zijn
  - Toegang tot het beheer van het systeem moet worden verleend door duidelijk geauthenticeerde en voldoende geautoriseerde gebruikers.
  - De ingestelde installatieaccounts mogen alleen bij de installatie worden gebruikt en daarna alleen nog in uitzonderlijke gevallen (bv. wachtwoord resetten, herstel).
- Het veiligheidsinformatieblad van het systeem, dat voor herstelgevallen bij de installatie wordt gegenereerd, mag alleen in afgedrukte vorm op een veilige plaats worden bewaard (bv. kluis).

Informatie over gegevensbescherming
- Bij het activeren van de registratie van de persoonlijke toegangsgegevens moeten de specifieke nationale gegevensbeschermingsbepalingen per land bekend zijn en in acht worden genomen.
- Een automatische opheffing van de toegangsgegevens van de persoon kan dienovereenkomstig via de administratiesoftware worden geconfigureerd. Raadpleeg het handboek voor de mogelijkheden en de procedure in de software.

Onderhoudscomponent (Xesar-tablet)

Interface en communicatie
- Om een nieuwe Xesar-component aan een Xesar-installatie toe te voegen, wordt de systeemcode met de AEAD-coderingsmethode en een 128-bits AES-sleutel gecodeerd getransporteerd. Deze sleutel wordt afgeleid van een pincode als tweede – niet op het apparaat opgeslagen – factor door middel van een cryptografische sleutelafleidingsfunctie (KDF, AES-CMAC-PRF-128).
- Configuratiegegevens voor componenten in de installatie worden gecodeerd getransporteerd met de AEAD-coderingsmethode en de voor de component specifieke 256-bits AES-sleutel (zie ook Cyberbeveiliging Xesar-componenten).

Veiligheidsaanwijzingen
- De door EVVA geleverde onderhoudstablet mag uitsluitend voor systeemonderhoud worden gebruikt.
- Er mogen geen andere toepassingen op deze tablet worden geïnstalleerd.
- Voor het invoeren van nieuwe Xesar-componenten zijn de configuratiegegevens met een pincode beveiligd. Deze moet:
  - na een installatie in de systeeminstellingen geconfigureerd worden om te voorkomen dat de standaardwaarde (d.w.z. 0000) door het systeem wordt gebruikt.
  - alleen aan bekende en vertrouwde gebruikers worden doorgegeven
- Voor het gebruik van Xesar is geen registratie bij Google vereist.
- Netwerkcommunicatie (wifi) mag alleen worden geactiveerd wanneer dat nodig is en er moet een beveiligd privénetwerk worden gebruikt (d.w.z. geen internet)
- Er mogen alleen door EVVA aanbevolen en geteste systeemupdates worden geïnstalleerd.

Deurcomponenten

Interface en communicatie

- Voor de communicatie met de component wordt in alle gevallen (draadloos en serieel) een AEAD-coderingsmethode met 256-bit AES-sleutels gebruikt (AES-CCM).
- De communicatiesleutel wordt specifiek voor elke component in de Xesar-administratiesoftware met een veilige procedure gegenereerd en is een klantengeheim dat EVVA niet kent.
- Eenmaal in de installatie kan alleen de beheerder de status of configuratie van de componenten wijzigen
- Sleutelmateriaal kan op de component met overeenkomstige beveiliging (authenticatie, versleutelde overdracht) worden bijgewerkt
- Aanvallen met bruut geweld zijn door de sleutelgrootte met de symmetrische methoden ook voor de post-quantum tijd niet eenvoudig succesvol uit te voeren. Bij componenten die op batterijen werken zal de voeding bovendien slechts een klein deel van de vereiste tests mogelijk maken vanwege de combinatoriek, vooral op de draadloze verbinding.

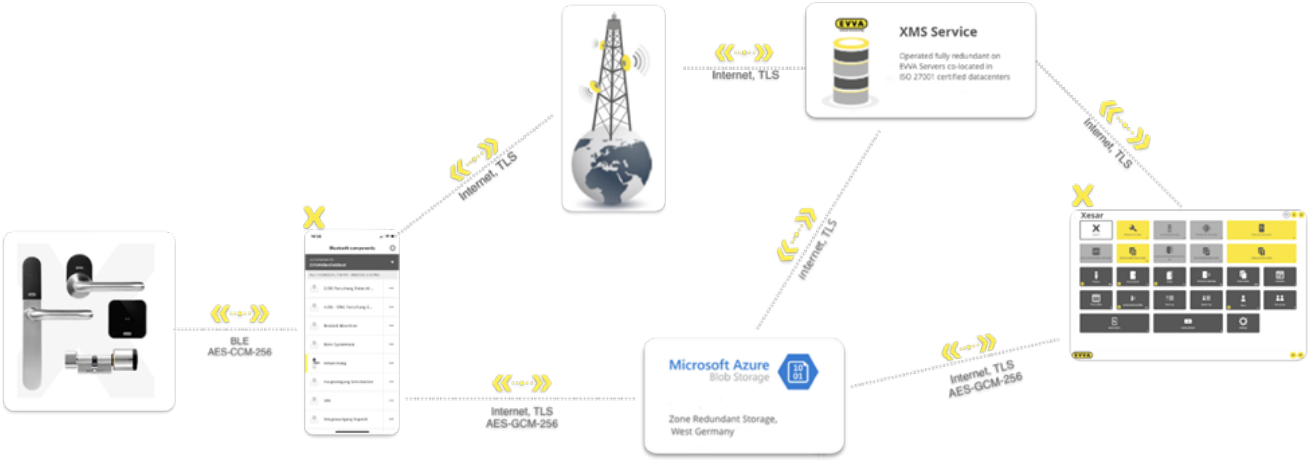
Gegevensopslag

- Sleutelmateriaal, gevoelige configuratie- en applicatiecode worden op de betreffende microcontroller (MC) opgeslagen met de best mogelijke MC-beveiliging (NVRAM, intern flashgeheugen)
  - PIC24-familie: algemene segmentbescherming en codesegmentbescherming (Family Datasheet, 29.4)
  - NRF52: hardwaregestuurde toegangspoortbeveiliging (APPPROTECT)
  - Het modulehuis beschermt tegen onherstelbare toegang tot de MC's (zie ook Mechanische veiligheid van Xesar-componenten)
- Systeemgegevens worden op de component in een geheugen (EEPROM of flash) opgeslagen en door gebruik van een cryptografisch proces met een 128-bits AES-sleutel integraal beveiligd (AES-CMAC).

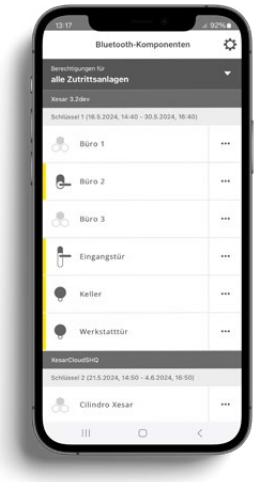
Firmware en actualiseren

- De bestaande firmware wordt met een bootloader geladen die af fabriek niet meer kan worden gewijzigd en kan met de betreffende beveiliging door de bootloader worden geactualiseerd.
- Firmwarepakketten van EVVA worden met een asymmetrische procedure gesigneerd (RSA-SHA256) en symmetrisch versleuteld aan het Xesar-beheer geleverd. Zowel in de administratiesoftware als in de onderhoudstoepassing wordt de certificaatketen geverifieerd.
- Voor het actualiseren in de installatie wordt een AEAD-coderingsmethode met 256-bit AES-sleutels gebruikt (AES-CCM). De firmware-updatesleutel wordt specifiek voor de installatie door de Xesar-administratiesoftware met een veilige procedure gegenereerd en is een klantengeheim dat EVVA niet kent.
- Eenmaal aangebracht in de installatie kan alleen nog de beheerder een firmware-update op de componenten uitvoeren.
- In het geval van de firmware voor NRF52 MC's wordt bovendien ook:
  - de firmware met een asymmetrische procedure gesigneerd (RSA-SHA256, 2048-bit Key) en direct op de MC geverifieerd.
  - de firmware beveiligd met een AEAD-coderingsmethode (AES-CCM) geleverd waarbij een 256-bit AES-sleutel wordt gebruikt.
- De firmware van componenten die nieuw in een installatie worden geïnstalleerd, wordt automatisch geactualiseerd naar de laatste in de administratiesoftware of onderhoudsapplicatie bekende firmwareversie.
- Aanwijzingen en controle van de door EVVA beschikbaar gestelde updates worden ondersteund en mogelijk gemaakt door de Xesar-Installation Manager en de Xesar-onderhoudsapplicatie.

Overzicht mobiel blokkeren



Mobiele Xesar-app (Xesar-app)



Interfaces en communicatie

- Elke communicatie met het XMS of de cloudopslag is beveiligd met TLS.
- Alle transacties tussen een Xesar-installatie en de Xesar-app worden op basis van een sleuteluitwisselingsprotocol (X25519), sleutelafleidingsfunctie en berichtauthenticatiecodes (HKDF-SHA256) end-to-end geauthenticeerd.
- Elke communicatie tussen een Xesar-component en de mobiele applicatie voor de overdracht van de toegangsgegevens is binnen een sessie beveiligd tegen weergave en versleuteld
- Gegevensopslag
- Voor zover ondersteund door het eindapparaat, wordt gevoelig sleutelmateriaal opgeslagen op veilige opslagplaatsen die de hardware ter beschikking stelt
  - Android: StrongBox indien beschikbaar, toegewezen aan het apparaat, cloudback-up gedeactiveerd door manifest
  - iOS: CryptoKit-sleutelbos, uitsluitend bruikbaar op het apparaat, iCloud-synchronisatie met het provisioneringsprofiel gedeactiveerd
- Alle gegevens worden in een extra versleutelde database op het mobiele eindapparaat opgeslagen
- Toegangsgegevens van een Xesar-installatie zijn al vooraf versleuteld en kunnen door de mobiele applicatie niet worden ontsleuteld, geïnspecteerd of gemanipuleerd.
- Veiligheidsaanwijzingen
- De mobiele applicatie mag in de door EVVA gesigneerde, originele vorm uitsluitend vanuit een officiële store worden gedownload (d.w.z. Google Play, Apple App Store)
- EVVA adviseert alle gebruikers van de mobiele applicatie
  - om eindapparaten te gebruiken met hardwareondersteunde veiligheidsgeheugens
  - Gebruik van de geheugencodering
  - Gebruik van de beveiliging van het eindapparaat met een wachtwoord, pincode of biometrische login

Xesar Mobile Support Service (XMS)

Datacenter

- De service wordt uitgevoerd op EVVA-servers die via colocatie in ISO 27001 gecertificeerde, fysiek gescheiden datacenters in Oostenrijk zijn ondergebracht.
- Alle benodigde resources zijn redundant ontworpen en horizontaal schaalbaar
- Alle service-eindpunten bevinden zich achter een firewall met geavanceerde beveiligingsmechanismen (IDS, IPS en DoS).

Interfaces en communicatie

- Elke communicatie met het XMS is beveiligd met TLS > 1.2.
  - MQTT Broker (mqtts://mqtt.akx.cloud:443)
    - Zie MQTT Broker voor een lijst met toegestane TLS-certificaten
  - REST-eindpunt (https://mss.akx.cloud)

- Voor de authenticatie en autorisatie van de Xesar-administratiesoftware
- Lijst van toegestane TLS-algoritmen REST

› Het XMS is uitsluitend een 'relaisstation' tussen een Xesar-installatie en een geregistreerde smartphone met Xesar-app
  • Alle transacties tussen een Xesar-installatie en een geregistreerde smartphone met Xesar-app worden op basis van een sleuteluitwisselingsprotocol (X25519), sleutelafleidingsfunctie en berichtauthenticatiecodes (HKDF-SHA256) end-to-end geauthenticeerd.
  • De transacties kunnen daarom nooit door het XMS of andere Xesar-installaties worden gestart of gemanipuleerd.

Gegevensopslag, back-up en herstel in noodsituaties

› Alleen gegevens die nodig zijn voor de functionaliteit worden opgeslagen
› Gegevens worden slechts voor een beperkte tijd en in versleutelde vorm tussentijds opgeslagen voor de overdracht tussen de Xesar-installatie en een daarvoor geregistreerde smartphone met Xesar-app.
  • Registratie: 48 uur
  • Update van rechten: 16 dagen
› Toegangsgegevens die door een Xesar-installatie ter beschikking worden gesteld, worden al voor de overdracht on-premises alleen voor de geregistreerde smartphone met Xesar-app versleuteld (AES-GCM-256). Deze gegevens kunnen niet door de XMS-dienst, EVVA of andere Xesar-installaties worden geopend.
› Gegevens worden momenteel redundant opgeslagen in gecertificeerde clouddatacenters in een zone in het westen van Duitsland. De architectuur is zo ontworpen dat deze kan worden uitgebreid naar andere regio's/zones voor gerichte opslag.
› In geval van een calamiteit die een hele zone betreft, kan de opslag worden omgeleid en kan het bijwerken van de toegangen met behulp van het Xesar-beheer On-Premises weer worden uitgevoerd.
› Er zijn organisatorische maatregelen getroffen voor beperkte en uitsluitend geautoriseerde toegang tot opgeslagen gegevens
  • Strikt gecontroleerde toegangsrechten voor bedienings- en supportpersoneel bij EVVA
  • Strikt management van geheimen voor de uitrol en werking (SecDevOps)

Bewaking en alarmen

› De werking van de servicecomponenten wordt voortdurend bewaakt en het bedieningspersoneel wordt gewaarschuwd bij afwijkingen.
  • De daarvoor opgestelde regels worden voortdurend geëvalueerd en verbeterd.
› De servicecomponenten zijn onderworpen aan een continue CVE-monitoring en worden in geval van bedreigingsscenario's tijdig bijgewerkt.

Informatie over gegevensbescherming

› Bij de ontwikkeling werd het privacy by design-principe gehanteerd
› Er worden nooit klanten- of persoonsgegevens van een Xesar-installatie in de context van het XMS opgeslagen
› Gegevens die van een Xesar-installatie naar een geregistreerde smartphone met Xesar-app worden verzonden
  • bevatten geen persoonsgegevens
  • kunnen eventueel niet door de XMS-service, EVVA of andere Xesar-installaties worden ingezien
  • Telefoonnummers van mobiele eindapparaten worden uitsluitend voor het oproepen van de SMS-serviceprovider gebruikt, maar niet door de XMS-dienst opgeslagen.

Mechanische veiligheidskenmerken van Xesar-deurcomponenten

Beslag

Overzicht van de mechanische veiligheidskenmerken van een Xesar-beslag.

Behaalde certificeringen

› EN 1634-1: 90 minuten
› EN 1634-3
› EN 179
› EN 1906
› met stabiliteitsplaat DIN 18257: ES0
› ÖNORM 3859: 90 minuten

Bescherming tegen omgevingsinvloeden

› IP 52 (IP55 met gelijmde afdichting) bescherming tegen het binnendringen van schadelijk stof en waterstralen in ingebouwde toestand
› Elektronica met coating tegen oxidatie door condensatie
› Gebruiksomstandigheden: -20 °C - +55 °C
› 3 batterijen in beveiligd binnenbereik

Fysieke beveiliging
- Meervoudige schroefverbinding
  - Mechanische manipulatiebeveiliging
  - Vrij draaiende buitenkruk

Deurkruk

Overzicht van de mechanische veiligheidskenmerken van een Xesar-deurkruk.

Behaalde certificeringen
- EN 1634-1: 90 minuten
- EN 179
- EN 1906
- ÖNORM 3859: 90 minuten
- CE-keurmerk

Bescherming tegen omgevingsinvloeden
- Luchtvochtigheidsbereik: 90% bij 0 °C
- Omgevingstemperatuur binnen: +5 °C tot +50 °C
- IP40

Fysieke beveiliging
- Vrij draaiende buitenkruk

Cilinder

Behaalde certificeringen
- EN15684 16B30D3D
- SKG***
- SSF3522 voor Scandinavische profielen
- EN 1634 brandveiligheidscertificaat (90 min)
- EN179/1125 anti-paniekcertificaat
- ÖNORM B 5351:2011 WMZ6-BZ
- CE-keurmerk

Bescherming tegen omgevingsinvloeden
- IP65-bescherming tegen schadelijk binnendringen van stof en waterstralen bij installatie volgens de Xesar-montagehandleiding
- Elektronica met coating tegen oxidatie door condensatie
- Luchtvochtigheidsbereik: 90% bij 0 °C
- Gebruiksomstandigheden: -20 °C - +55 °C
- 2 parallelle batterijen voor een hogere stabiliteit van de voeding

Fysieke beveiliging
- Vrij draaiende buitenknop
- Uitboorbeveiliging
- Kerntrekbeveiliging
- Rotatierem tegen aanvallen met een spil met hoge frequentie
- Gedefinieerde breeksterktegrens op de schroefdraad van de buitenknop om de kern te beschermen tegen mechanische aanvallen en om snapping-aanvallen af te weren
- Speciaal mechanisch gereedschap voor het monteren en demonteren van de cilinderknop

Architectonische beveiliging
- De Xesar-cilinder bestaat uit een cilinderknop en een cilindermodule die zich achter de uitboorbeveiliging bevindt.
- Knop en module zijn door een cryptografische beveiliging met elkaar verbonden:
  - De vrijgave vindt uitsluitend plaats in de mechanisch 'veilige' zone
  - een eenvoudige vervanging van de knop maakt onbevoegde toegang niet mogelijk

Wandlezer (online, offline)

Behaalde certificeringen
- CE-keurmerk

Bescherming tegen omgevingsinvloeden
- Luchtvochtigheidsbereik 90% bij 0 °C
- Omgevingstemperatuur –25 °C tot +70 °C
- Beschermingsklasse IP65

Fysieke beveiliging
- Voorkant van echt glas

Architectonische beveiliging
- De Xesar-wandlezer bestaat uit een lezereenheid en een besturing die zich in een beveiligde zone bevindt.
- De online-wandlezer bestaat uit een wandlezer en een online besturing die zich in een beveiligde zone bevindt.
- De leeseenheid en de besturing zijn met elkaar verbonden door middel van een cryptografische beveiliging:
  - De vrijgave vindt uitsluitend plaats in de 'veilige' zone
  - een eenvoudige vervanging van de wandlezer maakt onbevoegde toegang niet mogelijk

Andere algemene veiligheidskenmerken

Deurcomponenten (montageplaatsen):
- toewijzing van montageplaatsen aan zones en rechten voor zones
- lijst voor geblokkeerde toegangsmedia
- Delete-Key – deactivering van geblokkeerde toegangsmedia die op de blacklist van de component staan
- Office Modes (permanente openingen van componenten)
  - Handmatige permanente opening van componenten
  - Automatische permanente opening, tijdgestuurd tussen twee vastgelegde tijdstippen (begin en einde)
  - Automatische permanente vrijgave eindigen op gedefinieerde tijden waarop handmatige permanente vrijgave ook wordt beëindigd (alleen einde)
  - Shop-modus: Automatische permanente opening, pas gestart na geautoriseerde toegang
- Logboek voor gebeurtenissen voor toegang, afwijzing en Office Mode
- Tijdelijke beperking voor toegangsrechten

Toegangsmedia:
- virtueel netwerk maakt het transport van gegevens via toegangsmedia resp. het gebruik ervan door gebruikers in de installatie mogelijk.

Administratiesoftware:
- Gedefinieerde toegangsprofielen voor beheerders met verschillende gebruikersrechten (beheerdersgroep)
- Gedefinieerde dashboardweergaven voor beheerders volgens gebruikersrechten (beheerdersgroep)
- Systeemstatus op het dashboard
  - Componenten:
    - noodzakelijke firmware-updates
    - noodzakelijke configuratie-updates
    - weergave batterijstatus
    - tijdige onlinestatus van montageplaatsen met online EVVA-component
    - verbindingsstatus
    - status van deurcontacten
  - Deurcomponenten en media:
    - onveilige montageplaatsen
    - toegangsmedia die een update vereisen
    - onveilig geblokkeerde toegangsmedia
    - vrijgaven die met geblokkeerde toegangsmedia zijn uitgevoerd
- Systeemprotocol voor de traceerbaarheid van configuratiewijzigingen in de administratiesoftware

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