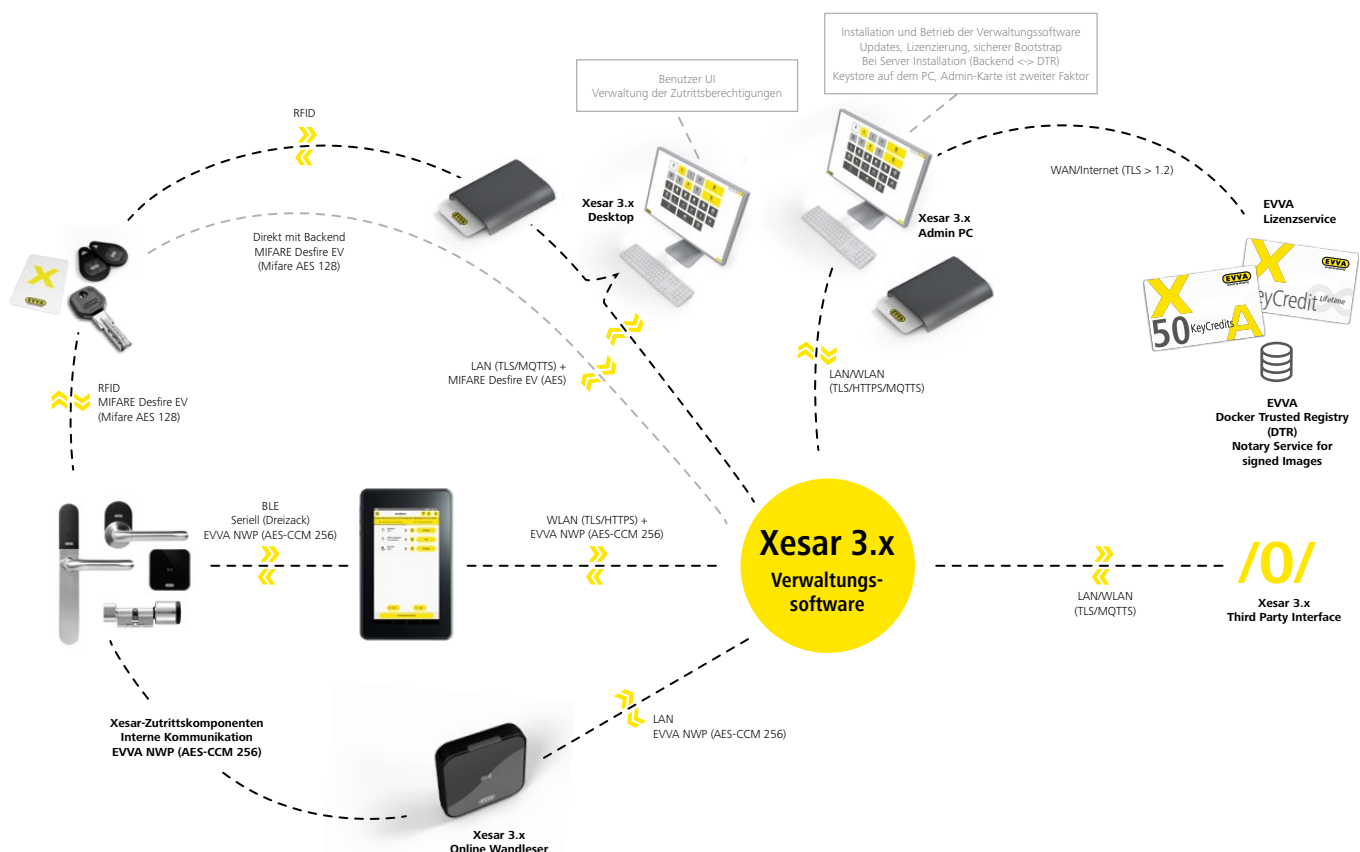




Xesar-Sicherheitskonzept

Überblick über die wichtigsten sicherheitstechnischen Merkmale eines Xesar-Zutrittssystems

Xesar-Cybersicherheit



Zutrittsmedien (Xesar 3)

Schnittstelle und Kommunikation

Für die Kommunikation zwischen Zutrittskomponenten und Zutrittsmedien wird in allen Fällen das MIFARE AES Verschlüsselungsverfahren mit 128 bit AES-Verschlüsselung eingesetzt.

- › Der Applikationsschlüssel für die Zutrittsberechtigung wird während der Xesar-Installation mit einem sicheren Verfahren generiert. Er ist ein Kundengeheimnis und EVVA nicht bekannt.
- › Er wird nur im Sicherheitsservice Installation in persistenter Form verschlüsselt gespeichert.
- › Bei dem eingesetzten MIFARE Verfahren wird für jede Interaktion eine Sitzung mit einem eigenen zufallsgenerierten Schlüssel verwendet.



Datenspeicher

Bei Xesar kommen ausschließlich sichere Zutrittsmedien mit geschütztem Datenspeicher zum Einsatz

- › Mifare Desfire EV1 mit EAL4+ Zertifizierung oder
- › Mifare Desfire EV2/EV3 mit EAL5+ Zertifizierung

Sicherheitshinweise

- › Das erstmalige Hinzufügen eines Zutrittsmediums in eine Xesar-Anlage sollte - um eine Manipulation zu vermeiden - nur durch einen berechtigten Benutzer mit Hilfe der Codierstation an einem geschützten Ort stattfinden.
- › Das Baustellenmedium ist weltweit gleich und kann überall für den Zugang an Xesar-Zutrittskomponente im Auslieferungszustand bzw. im Baustellenmodus eingesetzt werden. Daher kann keine Zutrittskontrolle damit durchgeführt werden.
- › Ein Zutrittsmedium mit Generalschlüssel-Berechtigung darf nur in Ausnahmefällen und an vertrauenswürdige Personen ausgehändigt werden. Grund: ein Zutrittsmedium mit diesem Berechtigungsprofil hat
 - eine unbeschränkte Gültigkeitsdauer (max. Gültigkeitsdauer siehe Handbuch)
 - Zutritt zu allen Zutrittskomponenten der Anlage, auch wenn diese erst nach dem Ausstellen dieses Mediums hinzugefügt/angelegt werden.

Ein Zutrittsmedium mit Generalschlüsselberechtigung soll an einem sicheren Ort außerhalb der besicherten Anlage aufbewahrt werden, damit im Notfall der Zutritt zur Anlage möglich ist.

Verwaltungssoftware

Auslieferung

- › Alle von EVVA ausgelieferten digitalen Bestandteile des Systems sind mit einer gültigen und zeitgestempelten Codesignatur versehen.
- › Schnittstelle und Kommunikation
- › Jede Kommunikation mit der Xesar-Verwaltung ist mit TLS > 1.2 gesichert, eine Liste der erlaubten TLS-Algorithmen ist auf Cipher Suites zu finden.
 - zur Verwaltung der Anlage durch mehrere Benutzer über den Browser-Zugang
 - zur Anbindung des Peripherie-Managers (verteilte Codierstation),
 - zur Interaktion der Services, die Bestandteile der Anlage sind
 - zur Interaktion mit der Dritt-System-Schnittstelle



Authentifizierung

Es wurde hier generell - wo sinnvoll anwendbar - den OWASP-Guidelines gefolgt.

- › Die Authentifizierung zur Verwaltung der Anlage über den Browser-Zugang ist Passwort geschützt:
 - Das erste Administrator Passwort wird bei der Installation zufallsgeneriert (keine Defaults)
 - Alle Passwörter, die angelegt werden, müssen eine Mindestlänge aufweisen und es gibt einen Indikator für die Qualität (zxcvbn: Low-Budget Password Strength Estimation)
 - Passwörter werden nie im Klartext abgespeichert (BCrypt)
 - Fehlschläge bei der Authentifizierung werden bewusst generisch beantwortet
- › Die Authentifizierung auf Service-Schnittstellen ist zertifikatsbasiert mit mTLS abgebildet:
 - zur Anbindung des Peripherie-Managers
 - bei internen Verbindungen von Services die Bestandteile der Anlage sind
 - bei der Verbindung mit der Dritt-System-Schnittstelle über den MQTT-Broker; hier wird zusätzlich noch ein Token zur internen Autorisierung eingesetzt.

Autorisierung

- › In der Xesar-Verwaltung können zur Autorisierung Benutzerrechte über Benutzergruppen definiert werden, die dann den jeweiligen Benutzern einfach zugeordnet werden können
- › Die jeweiligen Aktionen eines Benutzers werden im System protokolliert
- › Die Autorisierung und die Protokollierung funktionieren auch für die Schnittstellen-Benutzer

Datenspeicher

- › Alle sensiblen Daten (z.B. Schlüsselmaterial, Passwörter) werden ausschließlich im Sicherheitsservice Installation abgelegt (Vault) und nur verschlüsselt gespeichert.
- › Beim Bootstrap der Installation wird über zwei Faktoren (Admin-Karte und AdminPC gespeicherter verschlüsselter Keystore) der Vault für den Betrieb „geöffnet“.
 - Nicht sensitive Daten der Installation und Konfiguration werden in einer Datenbank abgelegt, diese ist nicht verschlüsselt (siehe Sicherheitshinweise).
 - Durch das architekturelle Design der Verwaltungssoftware, in der die Lese- und Schreibmodelle getrennt sind, werden alle Änderungen als eine Sequenz von Ereignissen abgespeichert (CQRS-ES). Das erhöht die Nachvollziehbarkeit und erschwert die Manipulation der Datenbestände.

Sicherheitshinweise

- › Es sollten nur unveränderte, von EVVA ausgelieferte Artefakte für die Installation des Systems eingesetzt werden. Die Authentizität und Integrität aller von EVVA ausgelieferten Artefakte kann mittels Signatur überprüft werden.
- › Die Verantwortung für den sicheren Betrieb der Xesar-Verwaltungssoftware liegt beim Kunden;
 - Zugriff (Authentifizierung und Autorisierung) auf die Serverumgebung muss gesichert werden damit die nicht sensitiven Datenbestände der Installation und Konfiguration nicht einfach manipuliert werden können
 - Der Zugriff auf die Verwaltung der Anlage sollte durch eindeutige authentifizierte und entsprechend autorisierten Benutzer erfolgen.
 - Die eingerichteten Installationskonten sollten nur bei der Installation zum Einsatz kommen und danach nur mehr in Ausnahmefällen (z.B. Passwort Resets, Recovery).
- › Das Anlagensicherheitsblatt, das für Recovery Fälle bei der Installation generiert wird, sollte nur in ausgedruckter Form an einem sicheren Ort aufbewahrt werden (z.B. Tresor).

Hinweise zum Datenschutz

- › Bei der Aktivierung der Aufzeichnung der personenbezogenen Zutrittsdaten sollten länderspezifische Datenschutzbestimmungen bekannt sein und eingehalten werden.
- › Eine automatische Auflösung des Personenbezugs von Zutrittsdaten kann über die Verwaltungssoftware entsprechend konfiguriert werden. Für die Möglichkeiten und Vorgangsweise in der Software sollte das Handbuch konsultiert werden.

Wartungskomponente (Xesar-Tablet)

Schnittstelle und Kommunikation

- › Für das Hinzufügen einer neuen Xesar-Komponente zu einer Xesar-Anlage wird der Anlagenschlüssel mit dem AEAD-Verschlüsselungsverfahren und einem 128-bit AES-Schlüssel verschlüsselt transportiert. Dieser Schlüssel wird von einem PIN als zweitem - nicht am Gerät gespeicherten - Faktor mittels einer kryptografischen Schlüsselableitungsfunktion (KDF, AES-CMAC-PRF-128) abgeleitet.
- › Konfigurationsdaten für Komponenten in der Anlage werden mit AEAD-Verschlüsselungsverfahren und dem für die Komponente spezifischen 256-bit AES-Schlüssel (siehe auch Cybersicherheit Xesar Komponenten) verschlüsselt transportiert.

Sicherheitshinweise

- › Das von EVVA ausgelieferte Wartungs-Tablet sollte ausschließlich für Anlagenwartungszwecke eingesetzt werden.
- › Es sollten keine anderen Applikationen auf diesem Tablet installiert werden.
- › Für das Einbringen von neuen Xesar-Komponenten sind die Konfigurationsdaten mit einem PIN besichert. Dieser sollte:
 - Nach einer Installation in den System Einstellungen konfiguriert werden, damit nicht der Standardwert (i.e. 0000) vom System verwendet wird.
 - Nur an bekannte und vertrauenswürdige Personen weitergegeben werden
- › Die Registrierung bei Google ist für den Betrieb mit Xesar nicht erforderlich.
- › Die Aktivierung von Netzwerk-Kommunikation (WLAN) sollte nur bei Bedarf stattfinden und ein gesichertes privates Netzwerk verwendet werden (i.e. nicht Internet)
- › Es sollen nur von EVVA empfohlene und getestete System-Updates installiert werden.



Zutrittskomponenten

Schnittstelle und Kommunikation

- › Für die Kommunikation mit der Komponente wird in allen Fällen (Funk und seriell) ein AEAD-Verschlüsselungsverfahren mit 256 bit AES-Schlüsseln eingesetzt (AES-CCM).
- › Der Kommunikationsschlüssel wird spezifisch für jede Komponente in der Xesar-Verwaltungssoftware mit einem sicheren Verfahren generiert und ist ein EVVA nicht bekanntes Kundengeheimnis.
- › Einmal in die Anlage eingebracht, kann nur mehr der Benutzer Änderungen am Zustand oder an der Konfiguration der Komponenten vornehmen
- › Schlüsselmaterial kann auf der Komponente mit entsprechender Besicherung (Authentifizierung, verschlüsselte Übertragung) aktualisiert werden
- › Brute Force Attacks sind durch die Schlüsselgröße mit den symmetrischen Verfahren auch für die Post-Quantum Zeit nicht einfach erfolgreich durchzuführen. Bei batterieversorgten Komponenten wird die Versorgung außerdem nur einen geringen Anteil der aufgrund der Kombinatorik benötigten Versuche ermöglichen, insbesondere auch auf der Funkstrecke.



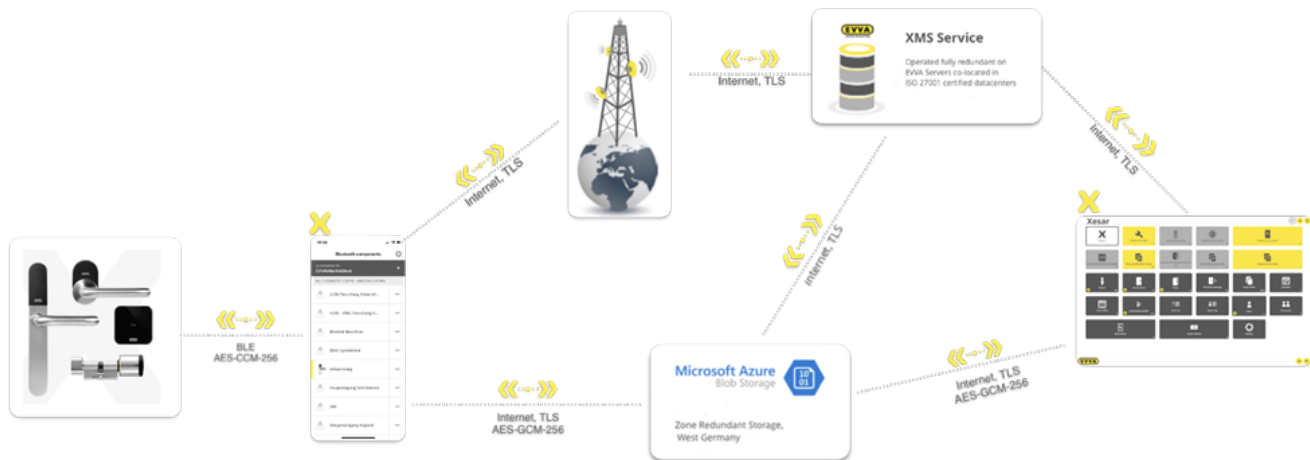
Datenspeicher

- › Schlüsselmaterial, sensitive Konfiguration und Applikationscode wird auf dem jeweiligen Mikrocontroller (MC) mit der besten MC möglichen Besicherung abgelegt (NVRAM, Interner Flashspeicher)
 - PIC24 Familie: General Segment Protection and Code Segment Protection (Family Datasheet, 29.4)
 - NRF52: Access port protection controlled by hardware (APPPROTECT)
 - Das Gehäuse schützt vor einem zerstörungsfreien Zugriff auf die MC's (siehe auch mechanische Sicherheit von Xesar-Komponenten)
- › Anlagendaten werden auf der Komponente in einem Speicher (EEPROM oder Flash) abgelegt und durch Einsatz eines kryptografischen Verfahrens mit einem 128 bit AES-Schlüssel integritätsgesichert (AES-CMAC).

Firmware und Aktualisierung

- › Die vorhandene Firmware wird mit einem ab Fabrik nicht mehr veränderbaren Bootloader geladen und kann mit entsprechender Besicherung durch den Bootloader aktualisiert werden.
- › Firmwarepakete von EVVA werden mit einem asymmetrischen Verfahren signiert (RSA-SHA256) und symmetrisch verschlüsselt an die Xesar-Verwaltung ausgeliefert. Sowohl in der Verwaltungssoftware als auch in der Wartungsapplikation wird die Zertifikatskette verifiziert.
- › Für die Aktualisierung in der Anlage wird ein AEAD-Verschlüsselungsverfahren mit 256 bit AES-Schlüsseln eingesetzt (AES-CCM). Der Firmwareupdateschlüssel wird spezifisch für die Anlage von der Xesar-Verwaltungssoftware mit einem sicheren Verfahren generiert und ist ein EVVA nicht bekanntes Kundengeheimnis.
- › Einmal in die Anlage eingebracht, kann nur mehr der Benutzer eine Aktualisierung der Firmware auf den Komponenten durchführen.
- › Im Falle der Firmware für NRF52 MC's wird zusätzlich auch:
 - die Firmware mit einem asymmetrischen Verfahren signiert (RSA-SHA256, 2048 bit Key) und direkt auf dem MC verifiziert.
 - die Firmware mit einem AEAD-Verschlüsselungsverfahren gesichert (AES-CCM) ausgeliefert bei dem ein 256 bit AES-Schlüssel zum Einsatz kommt.
- › Die Firmware von Komponenten, die neu in eine Anlage eingebracht werden, wird automatisch auf die letzte der Verwaltungssoftware oder der Wartungsapplikation bekannte Firmware-Version aktualisiert.
- › Hinweise und Überprüfung der von EVVA verfügbaren Aktualisierungen werden vom Xesar-Installation Manager und der Xesar- Wartungsapplikation unterstützt und ermöglicht.

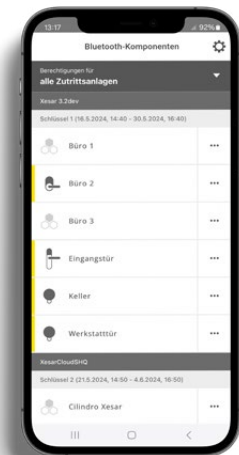
Überblick Mobiles Sperren



Xesar-Mobilapplikation (Xesar-App)

Schnittstellen und Kommunikation

- › Jede Kommunikation mit dem XMS oder den Cloud Speichern ist TLS gesichert.
- › Alle Transaktionen zwischen einer Xesar-Anlage und der Xesar-App werden auf Basis eines Schlüsselaustauschprotokolls (X25519), Schlüsselableitungsfunktion und Nachrichtenauthentifizierungscodes (HKDF-SHA256) End-to-End authentifiziert.
- › Jede Kommunikation zwischen einer Xesar-Komponente und der Mobilapplikation für die Übertragung der Zutrittsdaten ist wiedergabegeschützt und innerhalb einer Sitzung verschlüsselt
- › Datenspeicherung
- › Soweit vom Endgerät unterstützt, wird sensibles Schlüsselmaterial auf von der Hardware zur Verfügung gestellten sicheren Speichern abgelegt
 - Android: StrongBox wenn verfügbar, dem Gerät zugeordnet, Cloud Backup durch Manifest deaktiviert
 - iOS: CryptoKit Schlüsselbund, ausschließlich auf dem Gerät verwendbar, iCloud Synchronisation mit dem Provisionierungsprofil deaktiviert
- › Alle Daten werden in einer noch einmal zusätzlich verschlüsselten Datenbank am mobilen Endgerät abgelegt
- › Zutrittsdaten einer Xesar-Anlage sind bereits durch diese zuvor verschlüsselt und können von der Mobilapplikation nicht entschlüsselt, inspiziert oder manipuliert werden.
- › Sicherheitshinweise
- › Die Mobilapplikation sollte in ihrer von EVVA signierten ursprünglichen Form ausschließlich von einem offiziellen Store geladen werden (i.e. Google Play, Apple App Store)
- › EVVA empfiehlt allen Benutzern der Mobilapplikation
 - die Nutzung von Endgeräten mit Hardware gestützten Sicherheitsspeichern
 - Nutzung der Speicherverschlüsselung
 - Nutzung der Sicherung des Endgerätes mit einem Passwort, PIN oder biometrischem Login



Xesar Mobile Support Service (XMS)

Datacenter

- › Das Service wird auf EVVA-Servern betrieben, die mittels Colocation in ISO 27001 zertifizierten, physisch getrennten Datacentern in Österreich untergebracht sind.
- › Alle benötigten Ressourcen sind redundant ausgelegt und horizontal skalierbar
- › Alle Service-Endpunkte befinden sich hinter einer Firewall mit Schutzmechanismen am Stand der Technik (IDS, IPS und DoS).

Schnittstellen und Kommunikation

- › Jede Kommunikation mit dem XMS ist mit TLS > 1.2 gesichert.
 - MQTT Broker (mqtt://mqtt.akx.cloud:443)
 - Liste der erlaubten TLS-Zertifikate siehe MQTT-Broker
 - REST-Endpunkt (https://mss.akx.cloud)

- Für die Authentifizierung und Autorisierung der Xesar Verwaltungssoftware
 - Liste der erlaubten TLS-Algorithmen REST
- › Das XMS ist ausschließlich eine „Relaisstation“ zwischen einer Xesar-Anlage und einem registrierten Smartphone mit Xesar-App
- Alle Transaktionen zwischen einer Xesar-Anlage und einem registrierten Smartphone mit Xesar-App werden auf Basis eines Schlüsselaustauschprotokolls (X25519), Schlüsselableitungsfunktion und Nachrichtenauthentifizierungs-codes (HKDF-SHA256) End-to-End authentifiziert.
 - Die Transaktionen können daher nie durch das XMS oder andere Xesar-Anlagen angestoßen oder manipuliert werden.

Datenspeicher, Datensicherung und Notfallwiederherstellung

- › Es werden ausschließlich Daten gespeichert, die für die Funktionalität benötigt werden
- › Daten werden nur für eine beschränkte Zeit und in verschlüsselter Form für den Transit zwischen der Xesar-Anlage und einem dafür registrierten Smartphone mit Xesar-App zwischengespeichert.
- Registrierung: 48h
 - Aktualisierung von Berechtigungen: 16 Tage
- › Zutrittsdaten, die von einer Xesar-Anlage bereitgestellt werden, werden bereits vor der Übertragung On-Premises nur für das registrierte Smartphone mit Xesar-App verschlüsselt (AES-GCM-256). Diese Daten können nicht vom XMS-Service, EVVA oder anderen Xesar-Anlagen geöffnet werden.
- › Daten werden aktuell redundant in zertifizierten Cloud-Datacentern in der Zone Westdeutschland gespeichert. Die Architektur ist so ausgelegt, dass sie für eine gezielte Speicherung in andere Regionen/Zonen erweitert werden kann.
- › Im Falle einer Katastrophe, die eine gesamte Zone betrifft, kann die Speicherung umgeleitet werden und die Aktualisierung der Zutritte mit Hilfe der Xesar-Verwaltung On-Premises wieder durchführbar gemacht werden.
- › Organisatorische Maßnahmen wurden für einen eingeschränkten und ausschließlich autorisierten Zugriff auf gespeicherte Daten getroffen
- Strikt kontrollierte Zugriffsrechte für Bedienungs- und Supportpersonal bei EVVA
 - Striktes Management von Geheimnissen für die Ausrollung und Operation (SecDevOps)

Überwachung und Alarme

- › Die Operation der Service-Komponenten wird konstant überwacht und das Bedienpersonal bei Abweichungen alarmiert.
- Die dafür eingerichteten Regelwerke werden kontinuierlich überprüft und verbessert.
- › Die Service-Komponenten unterliegen einem kontinuierlichen CVE-Monitoring und werden im Falle von Bedrohungs-Szenarien zeitnah aktualisiert.

Hinweise zum Datenschutz

- › Bei der Entwicklung wurde nach dem Privacy by Design Prinzip gearbeitet
- › Es werden nie Kunden oder personenbezogene Daten einer Xesar-Anlage im Kontext vom XMS gespeichert
- › Daten, die von einer Xesar-Anlage an ein registriertes Smartphone mit Xesar-App übermittelt werden
- beinhalten keine personenbezogenen Daten
 - können allenfalls nicht vom XMS-Service, EVVA oder anderen Xesar-Anlagen eingesehen werden
 - Telefonnummern von mobilen Endgeräten werden ausschließlich für den Aufruf an den SMS-Service Provider verwendet, aber nicht vom XMS-Service gespeichert.

Mechanische Sicherheitsmerkmale von Xesar-Zutrittskomponenten

Beschlag

Überblick über die mechanischen Sicherheitsmerkmale eines Xesar-Beschlags.

Bestandene Zertifizierungen

- › EN 1634-1: 90 Minuten
- › EN 1634-3
- › EN 179
- › EN 1906
- › mit Stabilitätsplatte DIN 18257: ESO
- › ÖNORM 3859: 90 Minuten

Schutz gegen Umwelteinflüsse

- › IP 52 (IP55 mit aufgeklebter Dichtung) Schutz gegen Eindringen von schädlichem Staub und Strahlwasser im eingebauten Zustand
- › Lackierte Elektronik gegen Oxidation durch Kondenswasser
- › Einsatzbedingungen: -20°C - +55°C
- › 3 Batterien im sicheren Innenbereich



Physikalische Sicherheit

- › Mehrfachverschraubung
 - Mechanischer Manipulationsschutz
 - Freidrehender Außendrücker

Drücker

Überblick über die mechanischen Sicherheitsmerkmale eines Xesar-Drückers.

Bestandene Zertifizierungen

- › EN 1634-1: 90 Minuten
- › EN 179
- › EN 1906
- › ÖNORM 3859: 90 Minuten
- › CE-geprüft

Schutz gegen Umwelteinflüsse

- › Luftfeuchtigkeitsbereich: 90% bei 0°C
- › Umgebungstemperatur innen: +5 °C bis +50 °C
- › IP 40

Physikalische Sicherheit

- › Freidrehender Außendrücker



Zylinder

Bestandene Zertifizierungen

- › EN15684 16B30D3D
- › SKG***
- › SSF3522 für skandinavische Profile
- › EN1634 Brandschutzzertifizierung (90min)
- › EN179/1125 Anti-Panik Zertifizierung
- › ÖNORM B 5351:2011 WMZ6-BZ
- › CE-geprüft

Schutz gegen Umwelteinflüsse

- › IP65 Schutz gegen schädliches Eindringen von Staub und Strahlwasser bei Einbau gemäß Xesar-Einbauanleitung
- › Lackierte Elektronik gegen Oxidation durch Kondenswasser
- › Luftfeuchtigkeitsbereich: 90% bei 0°C
- › Einsatzbedingungen: -20°C - +55°C
- › 2 Batterien parallel für höhere Spannungsversorgungsstabilität

Physikalische Sicherheit

- › Freidrehender Außenknauf
- › Aufbohrschutz
- › Kernziehschutz
- › Rotationsbremse gegen Angriffe mit einer Hochfrequenzspindel
- › Definierte Sollbruchstelle am Gewinde des Außenknaufs, um den Kern vor mechanischen Angriffen zu schützen und Snapping-Angriffe abzuwehren
- › Mechanisches Spezialwerkzeug zur Montage und Demontage des Zylinderknaufs

Architekturelle Sicherheit

- › Der Xesar-Zylinder besteht aus einem Zylinder-Knauf und einem Zylinder-Modul, das sich hinter dem Aufbohrschutz befindet.
- › Knauf und Modul sind durch eine kryptografische Besicherung miteinander verknüpft:
 - Die Freigabe findet ausschließlich im mechanisch „sicheren“ Bereich statt
 - ein einfacher Tausch des Knaufs ermöglicht keinen unberechtigten Zugriff



Wandleser (Online, Offline)

Bestandene Zertifizierungen

- › CE-geprüft

Schutz gegen Umwelteinflüsse

- › Luftfeuchtigkeitsbereich 90% bei 0°C
- › Umgebungstemperatur –25 °C bis +70 °C
- › Schutzart IP65

Physikalische Sicherheit

- › Echtglas Front

Architekturelle Sicherheit

- › Der Xesar-Wandleser besteht aus einer Wandleser-Leseinheit und einer Wandleser-Steuereinheit, die sich in einem sicheren Bereich befindet.
- › Der Online-Wandleser besteht aus einer Wandleser-Leseinheit und einer Online-Steuereinheit, die sich in einem sicheren Bereich befindet.
- › Die Leseinheit und die Steuereinheit sind durch eine kryptografische Besicherung miteinander verknüpft:
 - Die Freigabe findet ausschließlich im „sicheren“ Bereich statt
 - ein einfacher Tausch des Wandlesers ermöglicht keinen unberechtigten Zugriff



Weitere allgemeine Sicherheitsmerkmale

Zutrittskomponenten (Einbauorte):

- › Zuordnung von Einbauorten zu Bereichen und Berechtigung für Bereiche
- › Blockliste für gesperrten Zutrittsmedien
- › Delete-Key – Deaktivierung von gesperrten Zutrittsmedien die sich auf der Blockliste der Komponente befinden
- › Office Modes (Daueröffnungen von Komponenten)
 - Manuelle Daueröffnung von Komponenten
 - Automatische Daueröffnung, zeitgesteuert zwischen zwei festgelegten Zeitpunkten (Start und Ende)
 - Automatisches Dauerfreigabeende an festgelegten Zeitpunkten an denen auch manuelle Dauerfreigaben beendet werden (nur Ende)
 - Shop-Modus: Automatische Dauerfreigabe, erst gestartet nach berechtigtem Zutritt
- › Ereignisprotokoll für Zutritts-, Abweisungs- und Office-Mode Ereignisse
- › Zeitliche Einschränkung für Zutrittsberechtigungen

Zutrittsmedien:

- › Virtuelles Netzwerk ermöglicht den Transport von Daten über Zutrittsmedien beziehungsweise deren Nutzung durch Personen in der Anlage.

Verwaltungssoftware:

- › Definierte Berechtigungsprofile für Benutzer mit unterschiedlichen Benutzerrechten (Benutzergruppe)
- › Definierte Dashboard-Ansichten für Benutzer nach Benutzungsrechten (Benutzergruppe)
- › Anlagenstatus am Dashboard
 - Komponenten:
 - notwendigen Firmware Updates
 - notwendige Konfigurationsaktualisierungen
 - Batteriestatusanzeige
 - Zeitnaher Onlinestatus von Einbauorten mit Online EVVA-Komponente
 - Verbindungsstatus
 - Zustand der Türkontakte
 - Zutrittskomponenten und Medien:
 - Unsichere Einbauorte
 - Zutrittsmedien, die eine Aktualisierung benötigen
 - Unsicher gesperrte Zutrittsmedien
 - Freigaben, die mit gesperrten Zutrittsmedien erfolgten
- › Systemprotokoll für die Nachvollziehbarkeit von Änderungen der Konfiguration in der Verwaltungssoftware