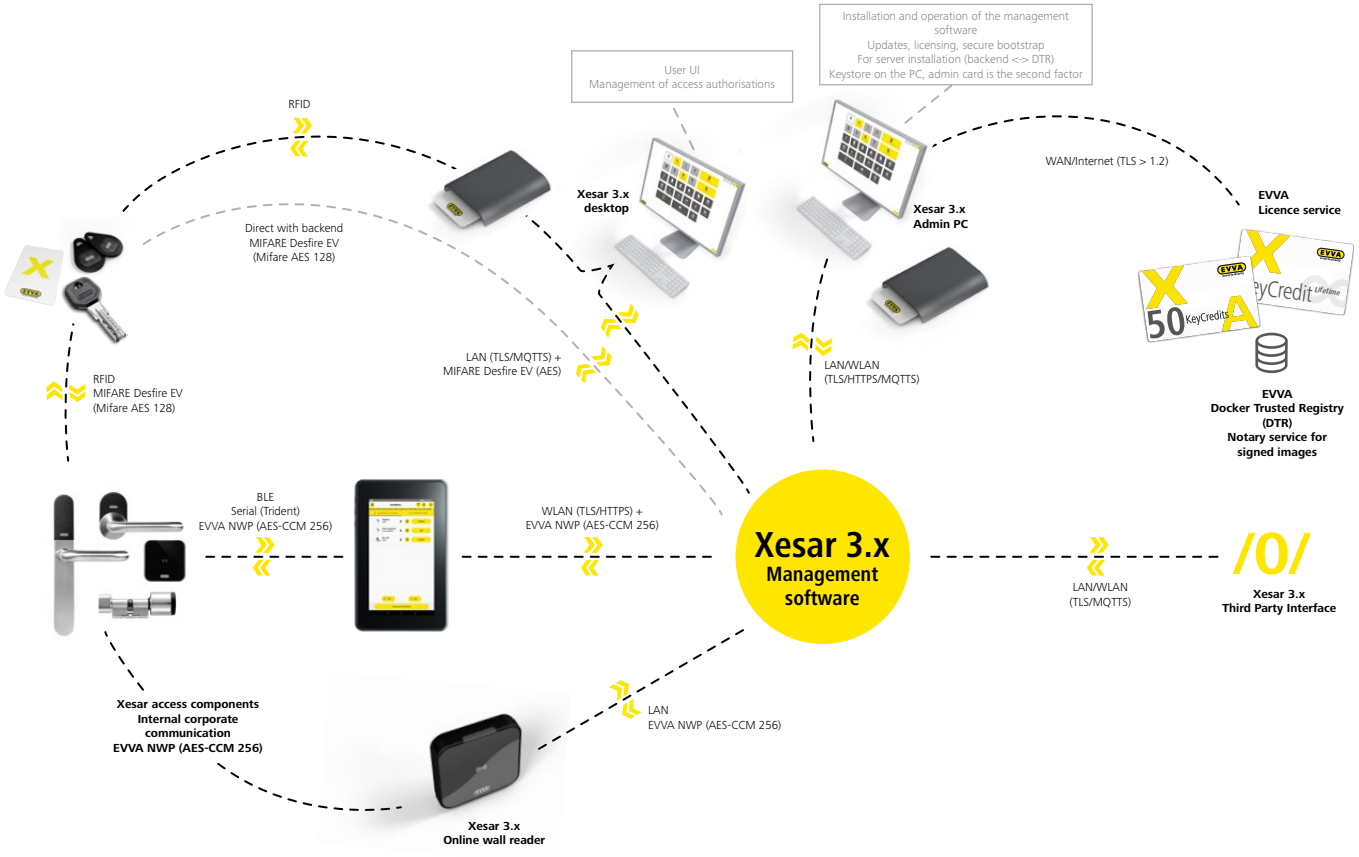
Xesar security concept

Overview of the most important security features of a Xesar access system

Xesar cyber security



Access media (Xesar 3)

Interface and communication

The MIFARE AES encryption process with 128-bit AES encryption is used in all cases for communication between access components and access media.

- The application key for access authorisation is generated during Xesar installation using a secure process. The key is a customer secret and not known to EVVA.
- It is stored exclusively in the security service installation (vault) and only in encrypted form.
- With the MIFARE process, a session with its own randomly generated key is used for each interaction.

Data storage

Xesar uses only secure access media with protected data storage

- Mifare Desfire EV1 with EAL4+ certification or
- Mifare Desfire EV2/EV3 with EAL5+ certification

Security information

- When adding an access medium to a Xesar system for the first time, this should only be done by an authorised user at a coding station in a protected location while the system is in operation so that manipulation is precluded.
- The construction site medium is the same worldwide and can be used anywhere to access Xesar access components in factory state or in construction mode. For this reason, it must not be used to carry out an access control operation.
- An access medium with a general key authorisation may only be issued to trustworthy persons in special cases. Reason: an access medium with this authorisation profile has
  - an unlimited validity duration (max. validity duration, see manual)
  - access to all access components in the installation, even if these are added/created after issuing this medium.

An access medium with general key authorisation should be stored in a secure location outside the secured installation to make it possible to access the installation in an emergency.

Management software

Delivery

- All digital components of the system delivered by EVVA are provided with a valid and time-stamped code signature.
- Interface and communication
- All communication with the Xesar administration is secured with TLS > 1.2; a list of permitted TLS algorithms can be found on Cipher Suites.
  - for managing the installation by several users via browser access
  - for connecting the Periphery Manager (distributed coding station),
  - for the interaction of the services that are part of the installation
  - for interaction with the third-party system interface

Authentication

The OWASP guidelines were generally followed here, where reasonably applicable.

- The authentication required for managing the installation via browser access is password-protected:
  - The first administrator password is generated randomly during the installation (no defaults)
  - All newly created passwords must have a minimum length. An indicator shows the strength of the password (zxcvbn: Low-Budget Password Strength Estimation)
  - Passwords are never stored in plain text (BCrypt)
  - If the authentication is unsuccessful, the response is deliberately generic
- Authentication for service interfaces is certificate-based with mTLS:
  - for connecting the Periphery Manager
  - where internal connection of services is part of the installation
  - where the connection to the interface of the third-party system is created via the MQTT broker; a token is also available for internal authorisation.

Authorisation
- User authorisation rights can be defined via user groups in the Xesar administration. These rights can then be assigned to the respective users
- The respective actions of a user are logged in the system
- Authorisation and logging also function for interface users

Data storage
- All sensitive data (e.g. key material, passwords) is stored exclusively in the security service installation (vault) and only in encrypted form.
- During the bootstrap of the installation, two factors (admin card and encrypted keystore stored on the admin PC) are used "to open" the vault for operation.
  - Non-sensitive installation and configuration data is stored in a database that is not encrypted (see security information).
  - The architecture of the management software separates the read and write models and stores all changes as a sequence of events (CQRS-ES). This increases traceability and makes it more difficult to manipulate the data sets.

Security information
- Only unmodified artefacts supplied by EVVA should be used for the installation of the system. The authenticity and integrity of all artefacts delivered by EVVA can be verified by means of a signature.
- The customer is responsible for the secure operation of the Xesar management software;
  - Access (authentication and authorisation) to the server environment must be secured to ensure that the non-sensitive installation and configuration data cannot be manipulated
  - Only those users who are unambiguously authenticated and appropriately authorised should have access to the installation management.
  - The set-up installation accounts should only be used during installation and afterwards only in exceptional cases (e.g. password resets, recovery).
- The installation security sheet, which is generated for recovery cases during installation, should only be kept in printed form in a safe place (e.g. safe).

Data protection notes
- Where the recording of person-related access data is activated, country-specific data protection regulations must be known and complied with.
- An automatic dissolution of the person-related access data can be configured via the management software. Please refer to the software manual for options and procedures.

Maintenance component (Xesar tablet)

Interface and communication
- When a new Xesar component is added to a Xesar system, the installation key is transported in encrypted form using the AEAD encryption process and a 128-bit AES key. This key is derived from a PIN - the second factor - not stored on the device - using a cryptographic key derivation function (KDF, AES-CMAC-PRF-128).
- Configuration data for components in the installation are transported in encrypted form using the AEAD encryption process and the component-specific 256-bit AES key (see also Cybersecurity Xesar components).

Security information
- The maintenance tablet supplied by EVVA should only be used for system maintenance purposes.
- No other applications should be installed on this tablet.
- A PIN is required to access the configuration data for the integration of new Xesar components. This should be:
  - After installation, system settings must be configured to allow the use of a password other than the system default (i.e. 0000).
  - This information may only be passed on to known and trusted persons
- Registration with Google is not required for Xesar operation.
- Network communication (WLAN) should only be activated when necessary and a secure private network should be used (i.e. not the Internet)
- Only system updates recommended and tested by EVVA should be installed.

Access components

Interface and communication

- In all cases (radio and serial), the AEAD encryption process with 256-bit AES keys (AES-CCM) is used for communication with the component.
- A unique communication key is generated for each component by the Xesar management software using a secure process. This key is a customer secret unknown to EVVA.
- Once the user has been added to the installation, the user can make changes to the status or configuration of the components
- Key material can be updated on the component using appropriate security (authentication, encrypted transmission)
- Because of the large key size, brute force attacks are not easy to carry out successfully with symetrical methods, even in the post-quantum era. Moreover, where battery-powered components are used, the power supply will only facilitate a small proportion of the tests required due to the combinatorics, especially on the radio link.

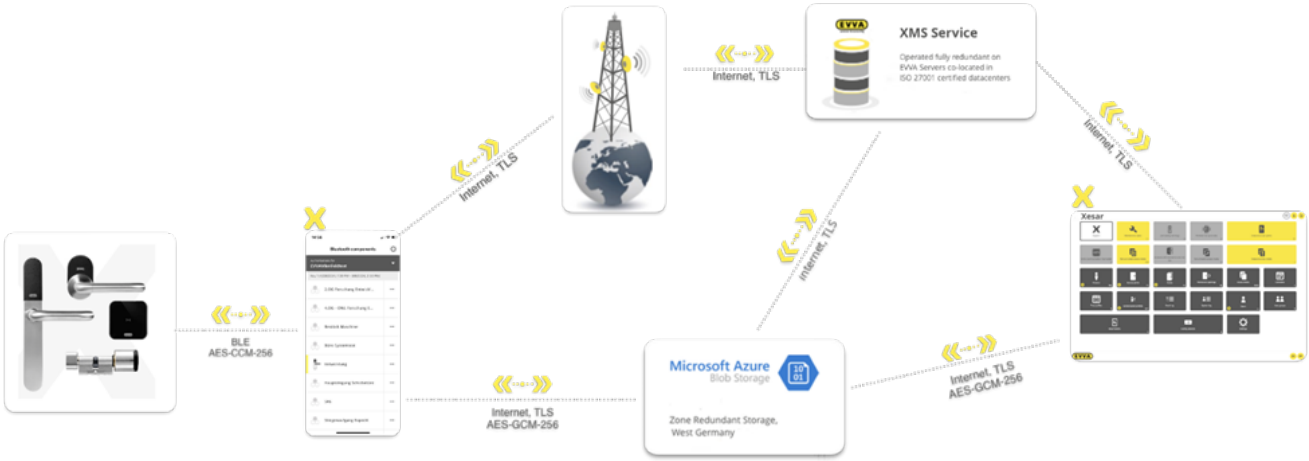
Data storage

- Key material, sensitive configurations and application code are stored on the microcontroller (MC) with the best possible MC protection (NVRAM, internal flash memory)
  - PIC24 family: General Segment Protection and Code Segment Protection (Family Datasheet, 29.4)
  - NRF52: Access port protection controlled by hardware (APPPROTECT)
  - The body protects against non-destructive access to the MCs (see also mechanical security of Xesar components)
- System data is stored on the component within a memory (EEPROM or flash) and its integrity is protected by a cryptographic procedure with a 128 bit AES key (AES-CMAC).

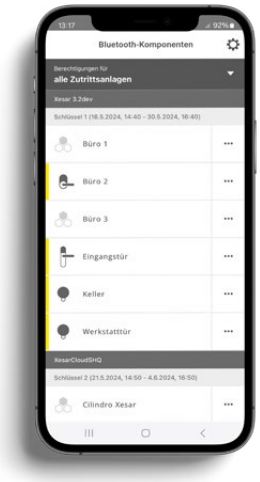
Firmware and update

- The existing firmware is loaded with a bootloader that cannot be changed ex works. The firmware may be updated by the bootloader subject to appropriate security.
- Firmware packages from EVVA are signed using an asymmetric procedure (RSA-SHA256) and delivered to the Xesar management system in symmetrically encrypted form. The certificate chain is verified both in the management software and in the maintenance application.
- An AEAD encryption process with 256-bit AES keys (AES-CCM) is used for updates in the installation. The firmware update key is generated specifically for the installation by the Xesar management software using a secure process. The key is a customer secret and not known to EVVA.
- Once installed in the installation, only the user can update the firmware on the components.
- In the case of the firmware for NRF52 MCs, additionally:
  - the firmware is signed using an asymmetric process (RSA-SHA256, 2048 bit key) and verified directly on the MC.
  - the firmware is delivered secured by an AEAD encryption process (AES-CCM) using a 256-bit AES key.
- The firmware of components that are newly added to an installation is automatically updated to the latest firmware version known to the management software or maintenance application.
- Instructions and verification of updates available from EVVA are supported and facilitated by the Xesar Installation Manager and the Xesar Maintenance Application.

Overview of mobile locking



Xesar mobile application (Xesar app)



Interfaces and communication

- All communication with the XMS or the cloud storage is TLS secured.
- All transactions between an Xesar device and the Xesar app are authenticated end-to-end based on a key exchange protocol (X25519), key derivation function, and message authentication codes (HKDF-SHA256).
- All communication between an Xesar component and the mobile application relating to the transfer of access data is protected and encrypted within a session
- Data storage
- Where supported by the end device, sensitive key material is stored on secure storage provided by the hardware
  - Android: Strongbox if available, assigned to device; cloud backup disabled by manifest
  - iOS: CryptoKit key ring can be used exclusively with the device; iCloud synchronisation with the provisioning profile is deactivated
- All data is stored in an additionally encrypted database on the mobile device
- Access data for a Xesar system is already encrypted by it and cannot be decrypted, inspected or manipulated by the mobile application.
- Security information
- The mobile application should only be downloaded from an official store (i.e. Google Play, Apple App Store) in its original EVVA-signed form
- EVVA recommends that all user of mobile applications
  - should only use end devices with hardware-supported secure storage
  - should use memory encryption
  - should use a password, PIN or biometric login to secure the end device

Xesar Mobile Support Service (XMS)

Data centre

- The service is operated on EVVA servers, which are co-located in ISO 27001-certified, physically separated data centres in Austria.
- All required resources are configured redundantly and are horizontally scalable
- All service endpoints are located behind a firewall with state-of-the-art protection mechanisms (IDS, IPS and DoS).

Interfaces and communication

- All communication with the XMS is secured using TLS > 1.2.
  - MQTT Broker (mqtts://mqtt.akx.cloud:443)
    - For a list of permitted TLS certificates, see MQTT broker
  - REST endpoint (https://mss.akx.cloud)
    - For authentication and authorisation of the Xesar management software
    - List of supported TLS algorithms REST

- The XMS is exclusively a “relay station” between a Xesar system and a registered smartphone with the Xesar app
  - All transactions between a Xesar system and a registered smartphone with the Xesar app are continuously authenticated based on a key exchange protocol (X25519), a key derivation function and message authentication codes (HKDF-SHA256).
  - Thus, at no point may transactions be initiated or manipulated by the XMS or other Xesar systems.

Data storage, data protection and emergency recovery

- Only data required for functionality is stored
- Data is only stored temporarily and in encrypted form for a limited period for transmission between the Xesar system and a smartphone registered with the Xesar app for this purpose.
  - Registration: 48h
  - Update of authorisations 16 days
- Access data provided by a Xesar system is already encrypted (AES-GCM-256) before being transmitted on-premises only for the registered smartphone with the Xesar app. XMS Service, EVVA or other Xesar systems are unable to open this data.
- Data is currently stored redundantly in certified cloud data centres in the West German region. The architecture is configured in such a way that it may be extended for targeted storage in other regions/zones.
- In the event of a disaster affecting an entire zone, storage may be rerouted and the updating of accesses made possible again on-premises using Xesar management.
- Organisational measures have been taken to ensure limited and exclusively authorised access to stored data
  - Strictly controlled access rights for operating and support personnel at EVVA
  - Strict management of secrets for deployment and operation (SecDevOps)

Monitoring and alarms

- The operation of the service components is constantly monitored and the operating personnel are alerted where deviations are detected.
  - The rules and regulations set up for this purpose are continuously reviewed and improved.
- The service components are subject to continuous CVE monitoring and are updated promptly in the event of threat scenarios.

Data protection notes

- The privacy by design principle was applied during development
- Customer or personal data from a Xesar installation are never stored in the context of XMS
- Data transmitted from a Xesar system to a registered smartphone with the Xesar app
  - do not contain any person-related data
  - cannot be viewed by XMS Service, EVVA or other Xesar systems
  - Telephone numbers from mobile devices are used exclusively for calling the SMS service provider, and are not stored by the XMS service.

Mechanical security features of Xesar access components

Escutcheon

Overview of the mechanical security features of a Xesar escutcheon.

Completed Certifications

- EN 1634-1 90 minutes
- EN 1634-3
- EN 179
- EN 1906
- with stability plate DIN 18257: ES0
- Austrian Standard 3859: 90 minutes

Protection against impacts on the environment

- IP 52 (IP 55 with adhesive seal) protection of the installed unit against the ingress of harmful dust and sprayed water
- Coated electronics to protect against oxidisation caused by condensation
- Operating conditions: -20°C - +55°C
- 3 batteries in a secure indoor area

Physical security

- Connection with several screws
  - Mechanical protection against tampering
  - Freely rotating outside handle

Handle

Overview of the mechanical security features of a Xesar handle.

Completed Certifications
- EN 1634-1 90 minutes
- EN 179
- EN 1906
- Austrian Standard 3859: 90 minutes
- CE approved

Protection against impacts on the environment
- Relative humidity range 90% at 0°C
- Ambient temperature inside: +5°C to +50°C
- IP40

Physical security
- Freely rotating outside handle

Cylinder

Completed Certifications
- EN15684 16B30D3D
- SKG***
- SSF3522 for Scandinavian profiles
- EN1634 fire resistance certification (90 min)
- EN179/1125 anti-panic certification
- Austrian standard B 5351:2011 WMZ6-BZ
- CE approved

Protection against impacts on the environment
- IP65 protection against ingress of harmful dust and powerful water jets from any direction when installed
- Coated electronics to protect against oxidisation caused by condensation
- Relative humidity range 90% at 0°C
- Operating conditions: -20°C - +55°C
- 2 lithium batteries in parallel for greater power supply stability

Physical security
- Freely rotating outside thumb turn
- Drilling protection
- Plug pulling protection
- Rotary damper to protect against attacks with a high frequency spindle
- Defined rated breaking point on the thread of the outside thumb turn to protect the plug from mechanical attacks and defend against snapping attacks
- Special mechanical tool for assembly and disassembly of the cylinder thumb turn

Architectural security
- The Xesar cylinder consists of a cylinder thumb turn and a cylinder module located behind the drilling protection.
- The thumb turn and module are linked by means of cryptographic security:
  - The approval takes place exclusively in the mechanically “secure” area
  - simple replacement of the thumb turn prevents unauthorised access

Wall reader (online, offline)

Completed Certifications
› CE approved

Protection against impacts on the environment
› Relative humidity 90% at 0°C
› Ambient temperature –25°C to +70°C
› Ingress protection rating IP65

Physical security
› Real glass front

Architectural security
› The Xesar wall reader consists of a wall reader reading unit and a wall reader control unit, which is located in a secure area.
› The online wall reader consists of a wall reader reading unit and an online control unit, which is located in a secure area.
› The reader unit and the control unit are linked to each other using cryptographic security:
  • Release takes place exclusively in the “secure” area
  • Unauthorised access remains unaffected if the wall reader is simply replaced

Other general security features

Access components (access points):
› Assignment of access points to areas and authorisation for areas
› List of blocked access media
› Delete key - deactivation of blocked access media contained in the component's block list
› Office modes (permanent opening of components)
  • Manual permanent opening of components
  • Automatic permanent opening, time-controlled between two specified times (start and end)
  • Automatic end of permanent release at specified times at which manual permanent releases are also ended (end only)
  • Shop mode: Automatic permanent release, only started after authorised access
› Event log for access, rejection and office mode events
› Time restriction for access authorisations

Access media
› The virtual network enables the transport of data via access media or their use by persons in the installation.

Management software:
› Defined authorisation profiles for users with different user rights (user group)
› Defined dashboard views for users by user rights (user group)
› Asset status on dashboard
  • Components:
    - necessary firmware updates
    - necessary configuration updates
    - battery status display
    - up-to-date online status of installation access points with Online EVVA component
    - connection status
    - status of door contacts
  • Access components and media:
    - insecure access points
    - access media that require an update
    - insecure blocked access medium
    - releases made with blocked access media
› System log for traceability of configuration changes in the management software