

Axessor Apexx Series Software

System Architecture & IT Security Guide for Axessor Apexx IP/CIT, and CenconX



Table of Contents

Apexx System Architecture	3
Overview.....	3
Axessor Apexx Lock System	3
CenconX Lock System.....	3
API/Software Components	4
Mobile Devices	3
Apexx API.....	4
Apexx Client Software.....	4
Apexx Database.....	4
MQTT Broker/Server.....	4
SMTP	5
SSO.....	5
User Configuration – Axessor Apexx.....	5
User Configuration – CenconX	6
User Configuration – Software Users	6
Software Users – Axessor Apexx	6
Software Users - CenconX.....	6
Licenses.....	6
Firmware Update Methods.....	7
Firmware Updates – Axessor Apexx Lock System.....	7
Firmware Updates – CenconX Lock System	7
Data Transit	8
Security & Data Encryption	10
Public Key Infrastructure (PKI).....	11

Computer Hardware Configurations	13
Single Computer Setup (USB Connection).....	13
Single Computer Setup (TCP/IP).....	14
Multiple Computer Setups.....	15
Database Considerations.....	17
Apexx Minimum Recommended Computer Specifications	17
Apexx Mobile Device Specifications.....	17
Apexx IT Security Guide	18
Local Software Notes.....	18
Pairing of Local Software with eBox (Axessor Apexx)	18
Disaster Recovery	19
Viewing and Exporting Apexx Event Logs.....	19
Key Takeaways	20

Apexx System Architecture

Overview

Apexx Series Software can be used to remotely manage and configure various aspects of Axessor Apexx and CenconX lock systems. This document describes aspects of the system architecture, computer infrastructure and requirements for using Apexx Series Software to support and manage Axessor Apexx and CenconX lock systems.

Axessor Apexx Lock System

Axessor Apexx locking systems consist of 2 secure communication networks: **The Lock System Can Bus** and **API/Software Network**

The Lock System CAN Bus supports the following components:

- **Apexx Series Keypads** (Maximum = 2, Minimum/Required = 1)
 - Used as a User interface for lock system access and configuration
- **Apexx Series Locks** (Maximum = 16, Minimum/Required = 1)
 - Physical electromechanical lock which controls user access to the safe
- **Apexx eBox** (Required for Networked / IP Connected Mode)
 - Functions as a protocol converter (IP to CAN bus) between the Axessor Apexx Lock System and the API/Software
 - Also functions as in I/O (input/output) box

CenconX Lock System

CenconX locking systems consist of 2 secure communication networks: **The Lock System** and **API/Software Network**

The Lock System supports the following components:

- **CenconX Series Keypads** (1)
 - Used as a User interface for lock system access and configuration
- **CenconX Series Locks** (1)
 - Physical electromechanical lock which controls user access to the safe

Mobile Devices

dormakaba's Safe Lock's Mobile App can be used to interface with Axessor Apexx and CenconX lock systems. It is available for free download at Google Play and the Apple Store, but is not functional until it is registered using Apexx Series Software. For information about using the mobile app and how to register a mobile device, refer to the CenconX System User Guide (Document #CX003.0524) and the Apexx Series Software help menu.

- **Axessor Apexx Lock Systems** > Axessor Apexx devices with firmware version 2.1.x.x or above can incorporate mobile devices via the dormakaba **Safe Locks Mobile app**.
- **CenconX Lock Systems** > dormakaba's **Safe Locks Mobile app** functions as a bridge between the CenconX Lock System and the API/Software, serving as a way to authenticate and open CenconX locks.

API/Software Components

The **API/Software** consists of 4 major components:

- Apexx API
- Apexx Client Software
- Apexx Database – Microsoft SQL Server 2019 Express
- MQTT Broker/Server

Note: The Apexx server/client must be set up using a publicly accessible IP to facilitate communication with the mobile devices.

Apexx API

The Application Programming Interface, or API, acts as both publisher and subscriber in the MQTT architecture.

Apexx Client Software

The Apexx Client Software ("Apexx Series Software") is a graphical user interface (GUI) that allows Software Users to use the API to perform actions in the Apexx/CenconX system (change system settings, store/retrieve data, etc.)

The Apexx Client supports multiple users but doesn't support multiuser simultaneously on a single client. Only one person can be logged into a single client instance at any given moment.

Apexx Database

The Apexx Database serves as the main location for data storage in the Apexx system. The Apexx Database uses Microsoft's proprietary relational database management system, Microsoft SQL Server 2019 Express, as a means of storing and retrieving system data.

MQTT Broker/Server

Message Queuing Telemetry Transport, or MQTT, is a messaging protocol that utilizes a publish-subscribe model to facilitate communication between devices. The MQTT Broker/Server acts as a centralized messaging hub and utilizes the MQTT protocol to manage communication between devices. Specifically, MQTT passes messages between the Windows client software and the eBox.

SMTP

Apexx Series Software utilizes Simple Mail Transport Protocol (SMTP) to send the following: Active alerts, Scheduled Reports, and Mobile Device Configuration info.

- Active alerts are sent to recipients based on the occurrence of one or more software user selected Audit Events.
- Scheduled Reports can be emailed to recipients based on a user defined schedule also using SMTP.
- When adding a new Mobile Device in Apexx Series Software, you have the option of using the generated QR code for mobile device configuration. When you use the Safe Locks mobile app to scan the QR code, the system employs SMTP to send the configuration information to the mobile device.
- Refer to Apexx Series Software's help menu for information regarding how to configure the SMTP settings.

SSO

Apexx Series Software utilizes Single Sign-On, ensuring that a Software User can use their credentials to log into the API using a single set of credentials.

User Configuration – Axessor Apexx

Axessor Apexx System Users fall into two distinct categories: **Safe Lock Users**, and **Software Users**

Safe Lock Users are users who will be utilizing the Axessor Apexx Lock System (consisting of the physical Keypads, Locks, and eBox), and will have unique credentials and roles with permissions that dictate their lock system access.

Safe Lock Users use numeric User IDs and PINs to access the lock system using the Apexx Series Keypad. This mode of operation is known as Bank Mode (aka Static Mode).

The three default Safe Lock User types (Administrator, Manager, and User) constitute a hierarchy of users each with pre-defined roles and privileges within the Locking System. In addition to these user types, additional Safe Lock User Roles can be created using Apexx Series Software's administrative tools that have permissions defined by a Software User. These additional user roles are created using a framework of the initial 3 user types, thus allowing new user types to meet the customization needs of the customer.

Axessor Apexx devices with firmware versions 2.1.x.x or higher introduce additional user types (a Primary Administrator and a Tenant Administrator), as well as two additional User Modes (OTC Mode, and ICS Mode) that incorporate the use of mobile devices for lock access. Refer to the Apexx Series Keypad System User Guide (Document #802.0622) for further details regarding Safe Lock User types and User Modes.

User Configuration – CenconX

Axessor Apexx System Users fall into two distinct categories: **Safe Lock Users**, and **Software Users**

Safe Lock Users are users who will be utilizing the CenconX Lock System (consisting of the physical Keypads, Locks etc.), and will have unique credentials and roles with permissions that define their lock system access.

Safe Lock User types in CenconX systems include Administrators, Managers, Static PIN (Bank Mode) Users, and OTC (One Time Code) Users. Refer to the CenconX System User Guide (Document #CX003.0524) for further information on the user types and their permissions.

User Configuration – Software Users

Software Users refers to users who run the Apexx Series Software and use the software tools to perform management and administrative tasks. Unlike Safe Lock Users, Software Users do not directly access the physical Lock System (open/close safe doors) but perform administrative/managerial tasks via software (adding lock users, reset lock user passwords).

Software Users use credentials to gain access to the Apexx Series Software using Single sign-on (SSO). Other authentication types for Apexx Series Software Users includes Windows Authentication (with the exception of Entra ID), Windows Domain Authentication, and Google OAuth 2.0.

Software Users who have a Software User “Write” permission can add new Software Users and configure the read/write permissions.

Software Users – Axessor Apexx

Software User types in Axessor Apexx systems include Administrators, Managers. For Cash In Transit applications, Dispatchers, and Audit Only Users also have a role to play (**Note:** device firmware 2.1.x.x and higher required).

Refer to the Apexx Series Software help menu for further details regarding Software User types and permissions.

Software Users - CenconX

Software User types in CenconX systems include Administrators, Managers, Dispatchers, and Audit Only Users. Refer to the CenconX System User Guide (Document #CX003.0524) for further information on the user types and their permissions.

When setting up your CenconX lock system, you have the ability to configure a single client/database setup for a single Owner (Primary Dispatcher), or you can introduce a second client/database to allow for a Secondary Dispatcher to have shared control over system management and access. Refer to the CenconX System User Guide for further information (Document #CX003.0524).

Licenses

Apexx Series Software has multiple license types available, each of which unlocks different software functions and features. Consult the Axessor Apexx IP and CenconX Price Books for more information.

Firmware Update Methods

The process of updating your Axessor Apexx device firmware varies depending on which license you've purchased.

For more information on the firmware update process, consult the Axessor Apexx System User Guide (Document #802.0622), the CenconX User Guide (Document #CX003.0524), and the Apexx Series Software's help menu.

Firmware Updates – Axessor Apexx Lock System

Local Firmware Updates can be done by establishing a temporary USB connection between the computer hosting the Apexx Series Software and the Keypad of your lock system.

Remote Firmware Updates can be done over a network connection via the eBox. This is a three-step process:

1. A Software User initiates the remote firmware update process, pushing the firmware from the API/Software to the locking system over the eBox.
2. The firmware is downloaded and stored on the locking system. A message will appear on the Keypad display informing Safe Lock Users that there is a pending firmware update.
3. A Safe Lock User enters valid credentials (User ID and PIN) at the Keypad, then initiates the firmware update.

Firmware Updates – CenconX Lock System

Local Firmware Updates can be done by establishing a temporary USB connection between the computer hosting the Apexx Series Software and the Keypad of your lock system.

CenconX mobile users also have the option of **Mobile Firmware Updates**, wherein dormakaba's Safe Locks mobile app can be used to receive firmware updates. The process involves using Apexx Series Software to dispatch the firmware update files to a user's mobile device. The mobile user can then log into the Safe Locks app, download the required files, then initiate the firmware update process using a BLE connection between the mobile device and CenconX keypad.

Data Transit

Figure 1 and its accompanying chart show data flow between the various hardware and software components of the Axessor Apexx lock system.

Communication Port	Description
443	This port is used for outbound TCP/IP traffic.
587	This port is used to communicate with the SMTP host. It is required and is defaulted to 587.
5001	This is the default port used for commissioning an Apexx lock system.
8883	This is the default port used by the MQTT Broker.

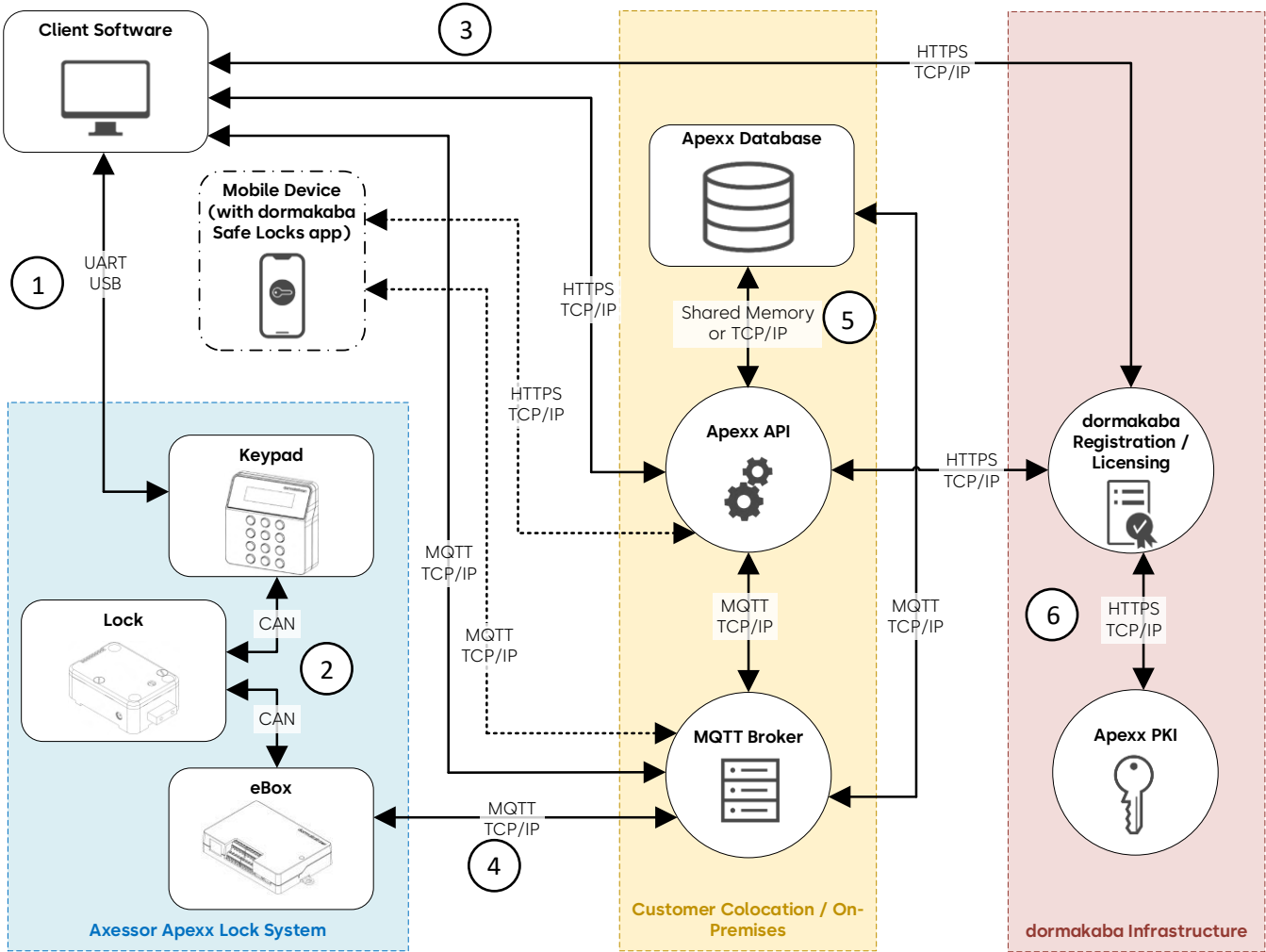


Figure 1 - Apexx System Architecture w Axessor Apexx Lock System - System Components and Data Transit

	Communication Protocols	Data flow	Description / Purpose
1	UART over USB	Bidirectional path: Client Software to Keypad	Direct configuration and audit retrieval
2	CAN	Bidirectional path: - Keypad to Lock - Lock to eBox	Device-to-device communication
3	HTTPS over TCP/IP	Bidirectional path: Client Software to dormakaba Registration/Licensing	Online licensing and registration
4	MQTT over TCP/IP	Bidirectional path: - Client Software to MQTT Broker Bidirectional path: - eBox to MQTT Broker Bidirectional path: - Device with dormakaba Safe Locks mobile app to MQTT Broker	Networked configuration and audit retrieval
5	Shared memory or TCP/IP	Bidirectional path: Apexx API to Apexx Database	Persistent data storage with SQL Server
6	HTTPS over TCP/IP	Bidirectional path: - Client Software to Apexx API - Apexx API to dormakaba Registration/Licensing - dormakaba Registration/Licensing to Apexx PKI - Device with dormakaba Safe Locks Mobile App to Apexx API	x.509 certificate issuance

Figure 2 shows a similar diagram to the one outlined in Figure 1, but with a CenconX lock system in place of the Axessor Apexx lock system. In this instance, the mobile device acts as the conduit for communication between the CenconX lock system and the software infrastructure.

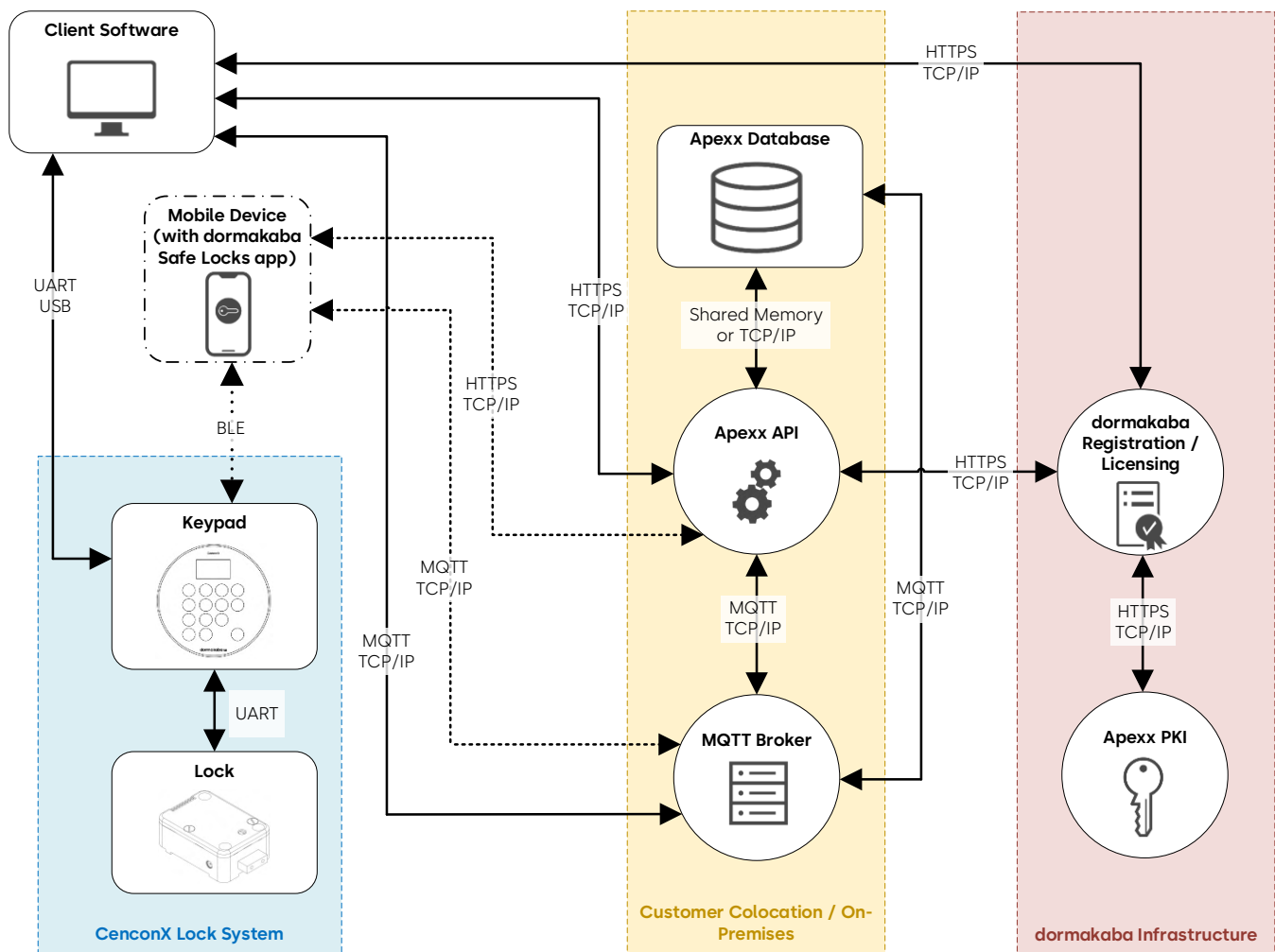


Figure 2 - Apexx System Architecture w CenconX Lock System - System Components and Data Transit

Security & Data Encryption

The Apexx Series Software, CenconX lock systems, Axessor Apexx Lock Systems, and commissioned mobile devices employ multiple encryption methods, including AES256, PBKDF2, and TLS certificates to ensure the safe and secure communication and storage of data.

Public Key Infrastructure (PKI)

The Apexx Series Software, CenconX lock systems, Axessor Apexx Lock Systems, and commissioned mobile devices utilize a Public Key Infrastructure to create, store, and distribute digital certificates to Apexx devices via certificate authorities.

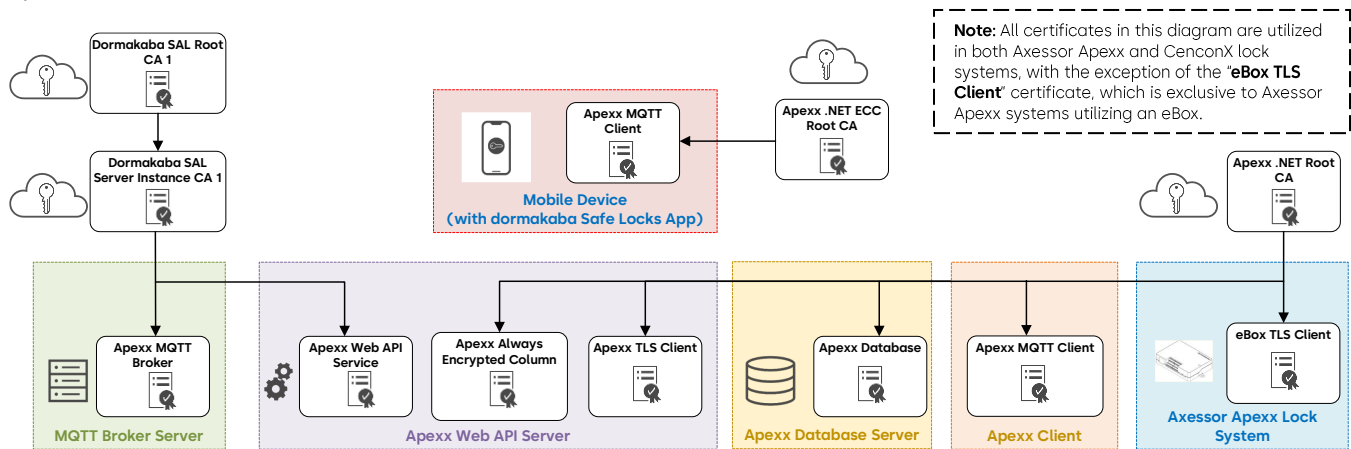


Figure 3 – Public Key Infrastructure

Certificate Type	Description
Dormakaba SAL Root CA	- This certificate is preloaded on the devices at the factory and replaced via firmware update - During installation of Apexx Series Software, this certificate also gets installed when running the Prerequisites Installer file on the Client and Server Machines (stored in the Trusted Root Certification Authorities folder)
Dormakaba SAL Server Instance CA	- Servers running local software services for Apexx require certificates signed by the dormakaba SAL PKI for devices to trust them - This certificate must be deployed to all servers running local software services - During installation of Apexx Series Software, this certificate also gets installed when running the Prerequisites Installer file on the Client and Server Machines (stored in the Intermediate Certification Authorities folder)
Apexx MQTT Broker	- Created during software installation - Used for TLS connections and authentication
Apexx Web API Service	- Created during software installation - Contains the server's name (computer where this service is installed), the trusted certificate authority, and the server's public encryption key
Apexx TLS Client	- Used for authentication of the Apexx Client - The certificate is a verified user if the issuer matches the installed Apexx .NET Root CA installed on the broker server
Apexx Database	- SQL Server on Windows is the only supported database engine - The following settings are enabled on the instance/database: - Windows Authentication - Role-based access control (RBAC) is used within, along with Windows Authentication to control permissions
eBox TLS Client	- Used for authentication of the eBox - The certificate is a verified user if the issuer matches the installed Apexx .NET Root CA installed on the broker server
Apexx .NET Root CA	- Created during software installation and is stored in the Local Machine certificate store in the Trusted Root Certification Authorities folder - During the API installation process, it gets stored in the Local Machine's Personal Certificates folder (LM\Personal\Certificates)

Certificate Type	Description
	- Any computer running the software (client, server, database, etc.) requires a copy of this certificate for security/identification purposes - The local software PKI signs certificate requests for all clients of the MQTT broker. - Those certificates are used for both establishing mutual trust Transport Layer Security (TLS) connections and authentication with the MQTT broker. - It can also sign the certificates used by SQL Server for TLS. - Uses RSA for signatures
Apexx .NET ECC Root CA	- Created during software installation and is stored in the Local Machine certificate store in the Trusted Root Certification Authorities folder - During the API installation process, it gets stored in the Local Machine's Personal Certificates folder (LM\Personal\Certificates) - Any computer running the software (client, server, database, etc.) requires a copy of this certificate for security/identification purposes - The local software PKI signs certificate requests for all clients of the MQTT broker. - Those certificates are used for both establishing mutual trust Transport Layer Security (TLS) connections and authentication with the MQTT broker. - It can also sign the certificates used by SQL Server for TLS. - Uses ECDSA for signatures
Apexx MQTT Client	- Created during software client login - Used for TLS connections and authentication
Apexx Always Encrypted Column	- Encrypting data at the API that goes to the encrypted column in the database - During the API installation process, it gets stored in the Local Machine's Personal Certificates folder (LM\Personal\Certificates)

Note: Certificates can be renewed 60 days prior to expiration by renewing your license using Apexx Series Software's online registration tool.

Computer Hardware Configurations

The Computer Hardware/API/Software portion of the Apexx System can be configured in a number of ways depending on the complexity of your system (number of Apexx Locking Systems, their locations, etc.). This section outlines only a few of the several possible set-ups. Refer to the Axessor Apexx or CenconX Price Books for more information on the license requirements for the various computer/hardware configurations.

Note: If desired, any of the software components (Client, Database, API, or MQTT) can be hosted on a virtual machine.

Single Computer Setup (USB Connection)

Figure 4 illustrates a basic setup involving just a single computer and one Axessor Apexx Locking System and/or a CenconX Locking System. In this setup, all API/Software elements are hosted on a single computer with a USB connection being used to temporarily connect to the Axessor Apexx or CenconX Locking System for programming/system configuration purposes.

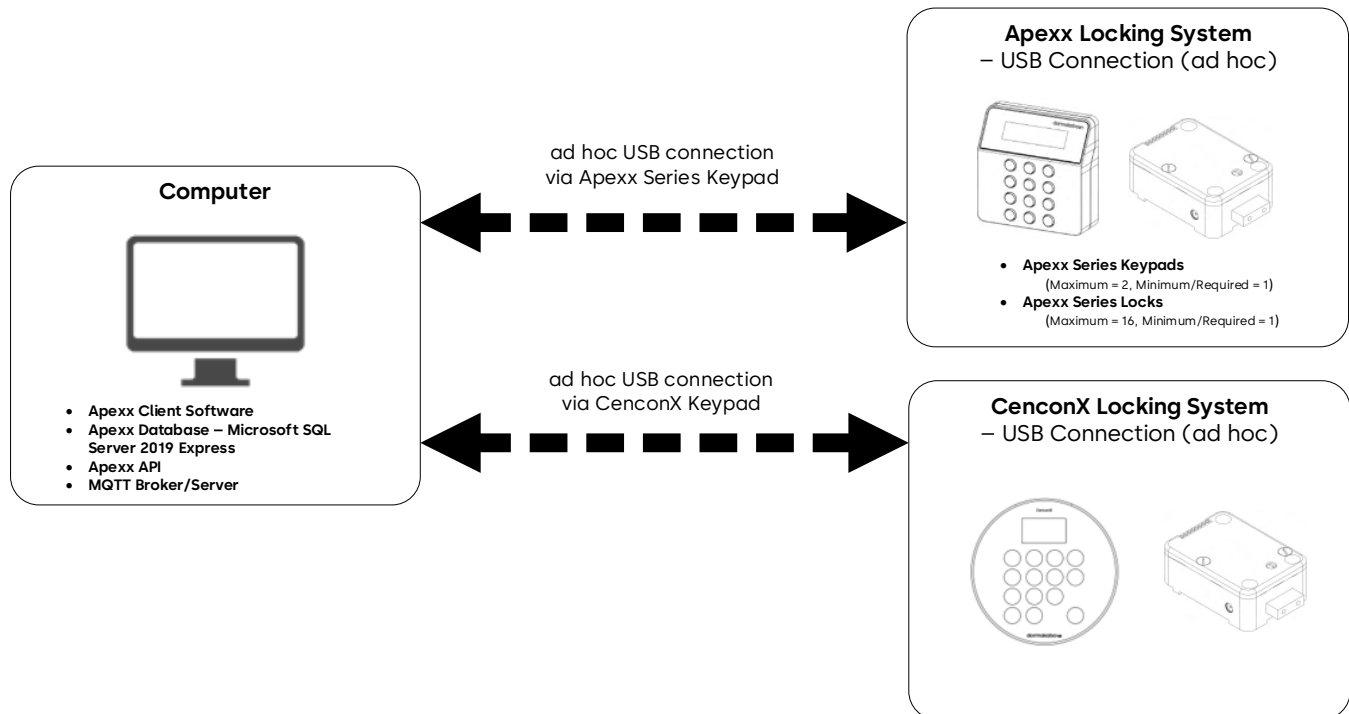


Figure 4 – Single Computer Setup - ad hoc USB connection

Axessor Apexx Lock Systems – USB Connection

For Axessor Apexx, this setup works well for small sites where the computer and all Locking System components (Keypads and Locks) are at the same physical location, but lacks the versatility and convenience offered by the networked setups utilizing the Apexx eBox.

CenconX Lock Systems – USB Connection

For CenconX, USB only connections are not recommended for CenconX systems using OTC functionality.

Single Computer Setup (TCP/IP)

Figure 5 shows another simple setup involving just one computer and one Axessor Apexx Locking System and/or a CenconX Locking System.

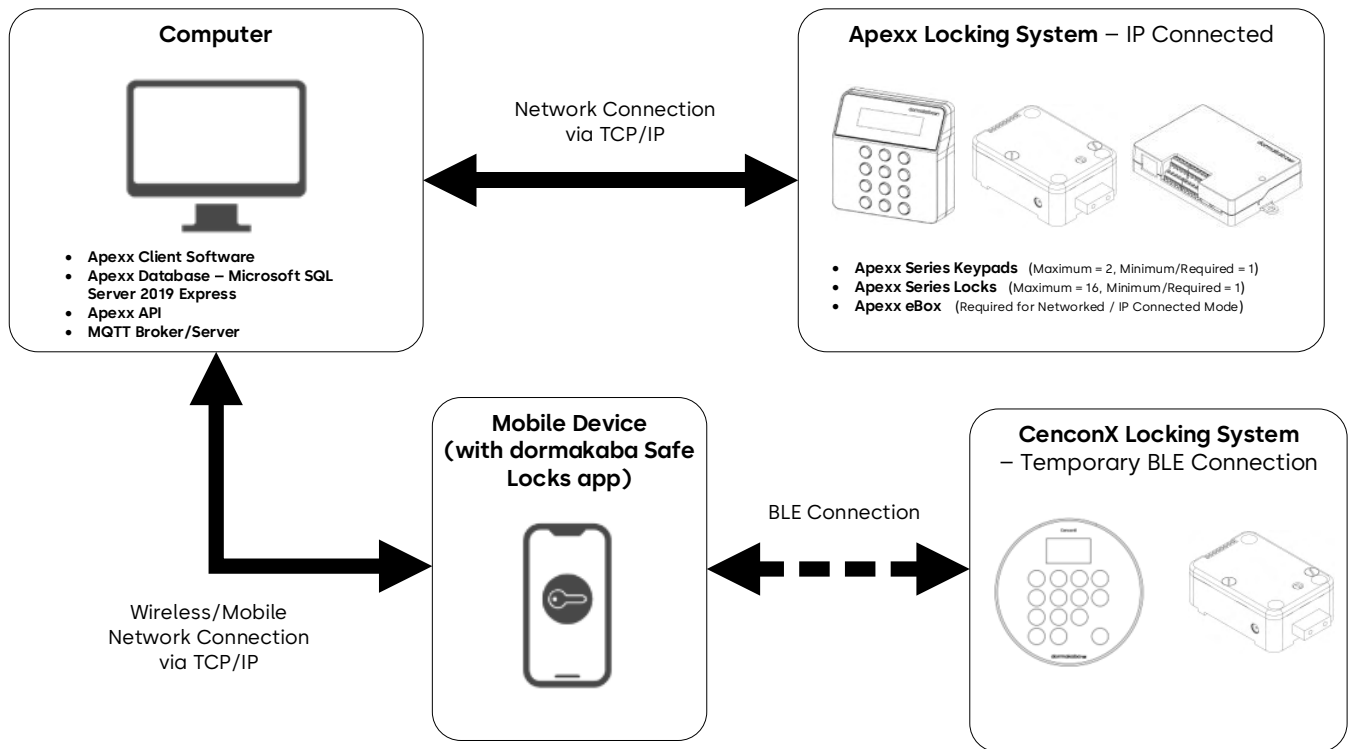


Figure 5 – Single Computer setup - Network via eBox (TCP/IP) and mobile

Axessor Apexx Lock Systems – Single Computer Setup (TCP/IP)

The Apexx eBox is used to provide a network/IP connection for continuous/live communication between the computer and Axessor Apexx locking system.

For Axessor Apexx Locking systems, this setup is also useful for smaller setups where all the equipment is at the same physical location, but the inclusion of the eBox allows the system administrator to take advantage of all the features that an active IP connection provides (live audits, active system monitoring, remote firmware updates, and other additional Hardware/Software features)

CenconX Lock Systems – Single Computer Setup (TCP/IP)

For the CenconX Locking System, the Mobile Device connects to the computer server/client via a network/IP connection and a temporary BLE "bridge" connection connects the mobile device to the CenconX locking system.

Multiple Computer Setups

For larger sites involving bigger buildings and/or multiple Locking Systems, the multiple-computer setup shown in Figure 6 offers additional flexibility.

Note: Only one API, MQTT Broker, and SQL Server database are allowed in the system.

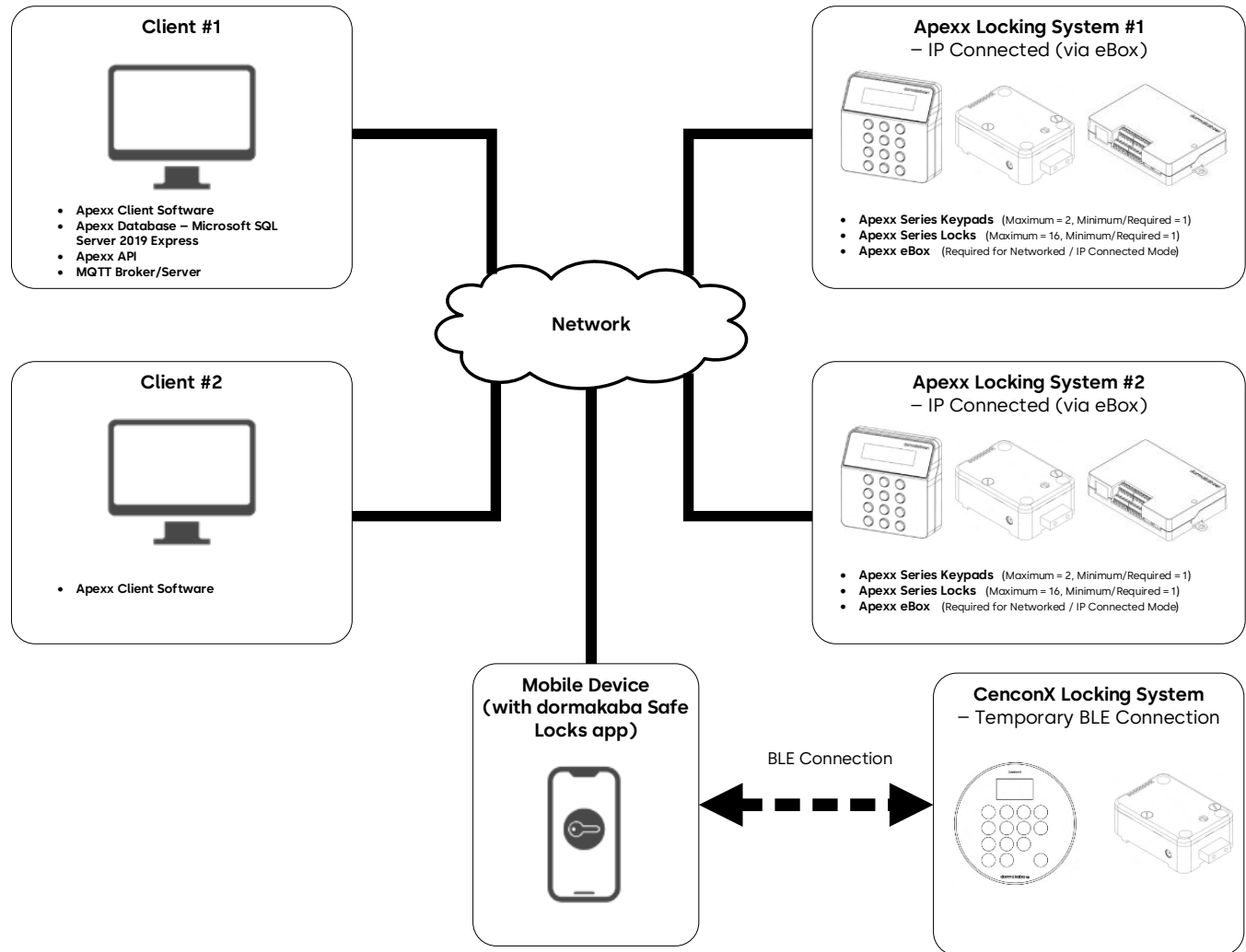


Figure 6 – Multiple Computer Setup with Multiple Locking Systems

In such a setup, any or all of the software components could be installed on one or more computers (or virtual machines), allowing for added convenience and flexibility when it comes to running and configuring your lock systems. Note that each Axessor Apexx locking system connects to the network via an Apexx eBox.

This concept is expanded further in the system shown in Figure 7, which includes multiple computers and lock systems spread out over multiple buildings.

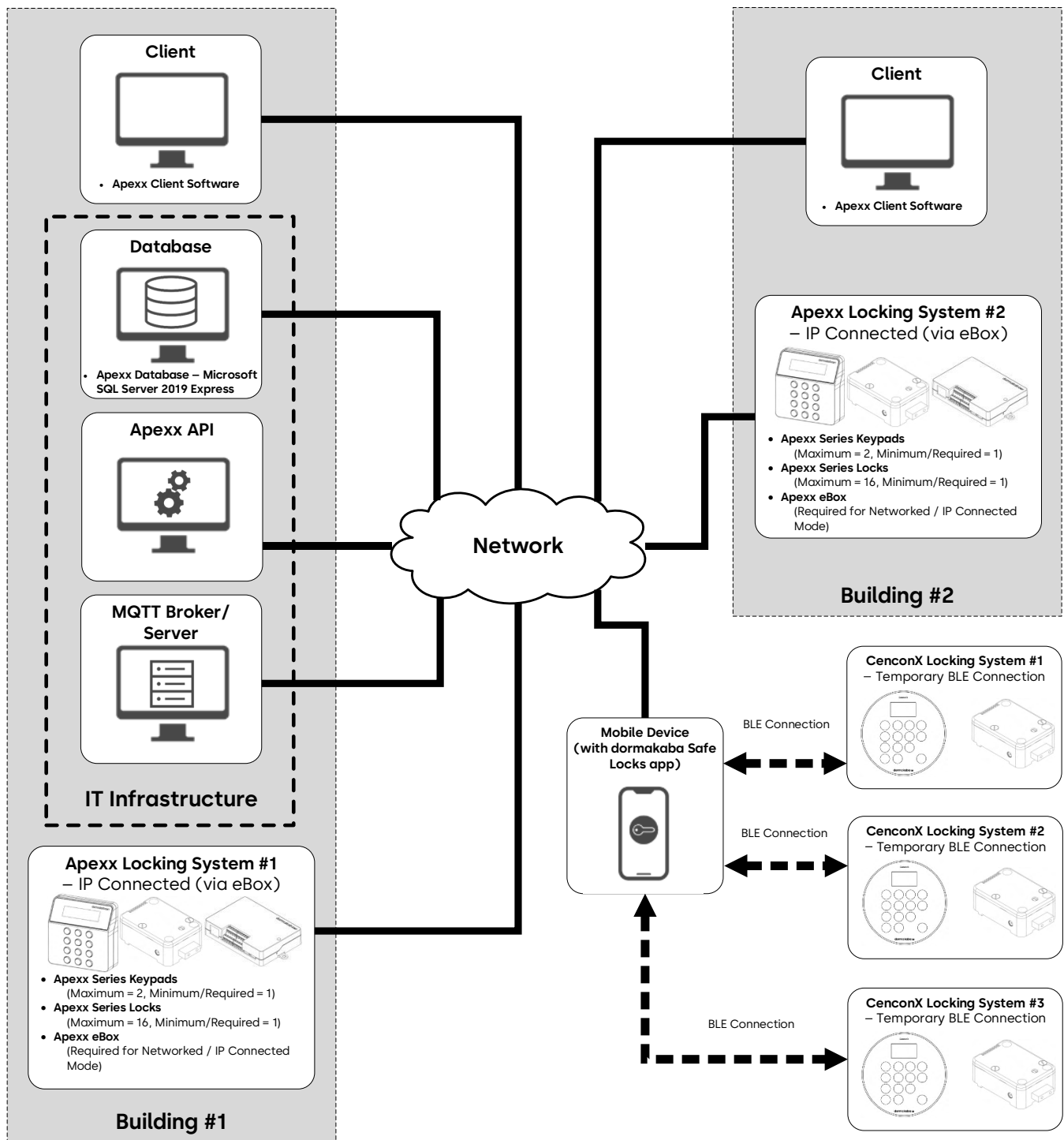


Figure 7 – Multiple Computer/Locking System Setup with multi-server setup

One notable difference between this setup and all the others is that it includes multiple computers hosting different software components. Note how two of the computers in Building #1 host the Apexx API and Apexx Database respectively. These two computers can be configured to be used as the API and Database for the Locking Systems in Building #1, Building #2, and/or any other Lock System on the entire network.

This final example illustrates that many different setups are possible depending on your organizational needs and IT infrastructure setup.

Database Considerations

Apexx Series Software includes Microsoft SQL Server 2019 Express as its dedicated internal database engine.

	Microsoft SQL Server 2019 Express (64-bit)
Database Limit	10 GB
Number of CPUs	1 physical processor
RAM	1 GB
Supported Operating Systems	Windows 10, Windows Server 2016, Windows Server 2019

Apexx Minimum Recommended Computer Specifications

*Consider doubling for larger installations

Apexx Client Workstation

- 2.0 GHz processor with 4 cores*
- 16GB RAM
- 500GB Hard Drive
- Windows 10 Professional 64bit

Apexx Broker Server

- 2.0 GHz processor with 4 cores*
- 16GB RAM
- 500GB Hard Drive
- Windows 2019 Server Standard 64bit

Apexx Database Server & Apexx API

- 2.0 GHz processor with 6 cores*
- 32GB RAM*
- 1TB Hard Drive
- Windows 2019 Server Standard 64bit
- Microsoft SQL Server Standard or Enterprise

Note: If desired, any of the software components (Client, Database, API, or MQTT Broker) can be hosted on a virtual machine.

Apexx Mobile Device Specifications

(As of document publication date)

- Mobile Operating system: Android 8+ or iOS 15+
- Must be BLE compatible

Note: Check Google Play and Apple Store for latest versions of the dormakaba Safe Locks mobile app and device/OS compatibility information.

Apexx IT Security Guide

Local Software Notes

- All parts of the Software (MQTT, client and API) are designed as Windows applications. To be able to use them in a cloud environment, one must be able to manage the communication channels between them.
- The communication channels are established during installation – These rely on DNS (or static IP addresses). Once the installation is completed, certificates will be established for the purpose of security. These certificates need to be properly managed to prevent any attack paths.
- The communication to-and from the locking system is MQTT over SSL, so the standard ports need to be reachable.
- Software requires Windows certificates subsystem and an SQL19 database to run.
- Software is not supported on Mac or Linux systems.
- Cloud environments tested are Azure and AWS.
- The same user cannot be logged into multiple clients at the same time.

Pairing of Local Software with eBox (Axessor Apexx)

The local software and Apexx eBox need to be paired before a connection can be established. When a brand-new eBox needs to be installed:

1. The eBox is physically installed on the CAN bus.
2. An authorized user needs to log in into the keypad and commission the eBox on the CAN bus (no unauthorized devices can listen to the CAN bus)
3. After commissioning of the eBox, the eBox will be able to obtain the encryption keys to the CAN bus (AES-256 with system specific keys).
4. Once the eBox is on the CAN bus, connection needs to be made to the Local Software. The IP address can be viewed and changed in the network settings in the advanced menu of the keypad. If there is a setting, it will be used. Otherwise, the eBox will assume DHCP to obtain IP address.
5. Once valid Ethernet setting exist, the eBox will attempt to connect to the MQTT server in the Local Software (either through direct IP communication based on the settings, or broadcast on local network in case of DHCP). This is done over TLS.
6. If Local Software detects a new eBox, it needs to be authorized in the Software before successful log-in using the claim code. Once eBox is authorized on the Software, the software will produce a verification PIN that needs to be validated on the keypad (Verification of Software to the eBox, and eBox to Software).
7. After the system is verified, a secure channel is established. This is done using pre-installed factory signed certificates (PKI infrastructure). Any communication afterwards is encrypted using TLS.

8. TLS 1.2. eBox also initially communicates over TCP port 5001 (API) to verify software is activated, then over port 8883 (default) for communication.
9. Software needs to be activated and have proper certificates in order for eBox to activate properly. Inactivated software will result in denial of service.

For further information on installing, connecting, and configuring the Apexx eBox, refer to the Axessor Apexx Installation guide (Document #801.0622), Apexx Series Keypad System User Guide (Document #802.0622), and the Apexx Series Software's help menu.

Disaster Recovery

Local Software connects to SQL19 database for data storage (SQL19 Express by Microsoft - Reference: <https://www.microsoft.com/en-ca/sql-server/sql-server-2019-pricing>). The configuration of the database needs to be input into the Local Software in the form of a config file. The encryption/protection and data recovery will then follow the path of the SQL19 database. It is expected that the database is managed by the local IT department.

The recovery path will then be to re-install the API, MQTT and client either with fresh copy from dormakaba or utilize a local backup. All data is at rest in the SQL database. API, MQTT and client don't store any lock or user data, only connection and configuration settings.

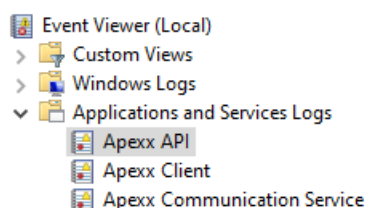
Database is created automatically by the API service for the first time. Database utilizes default service specific (API or BROKER) NT Service logins and authenticates via Kerberos channels. Default DB settings are Windows Authentication, Encrypted columns. We recommend but do not require encryption at the engine level.

Viewing and Exporting Apexx Event Logs



Windows "Event Viewer" can be used to help view and troubleshoot issues related to Apexx applications and services.

1. Open event viewer > type **"Event Viewer"** in the windows search bar, then open the program.
2. Click the arrow next to >  **"Applications and Services Logs"** to expand the list.
3. Click the Apexx application/service to view all events related to that application or service (Apexx API, Apexx Client, Apexx Communication Service).



4. From here, you can sort events by time, event id, etc. to assist in viewing and troubleshooting issues with your Apexx setup.
5. Export Apexx Event Logs > Under **"Actions"**, you can choose  **"Save All Events As..."** to export the event logs of the selected application/service and save it in one of several formats (.evtx, .xml, .txt, .csv).

Key Takeaways

1. Only servers with Local Software needs to be IP addressable - eBox doesn't.
2. Communication between eBox and Local Software (traffic over intranet/Internet) is encrypted using TLS.
3. Please include the SQL server in your disaster recovery plan. This database is crucial to the function of the system.



Access Automation Solutions

Entrance Automation
Entrance Security



Access Control Solutions

Electronic Access & Data
Escape and Rescue Systems
Lodging Systems



Access Hardware Solutions

Door Closers
Architectural Hardware
Mechanical Key Systems



Services

Technical Support
Installation and commissioning
Maintenance and Repair



Key & Wall Solutions

Key Systems
Movable / Sliding Walls



Safe Locks

Electronic Safe Locks
Mechanical Safe Locks
Boltworks and Accessories



Glass systems

Manual door systems
Glass fittings
Horizontal Sliding Walls

Our Sustainability Commitment

We are committed to foster a sustainable development along our entire value chain in line with our economic, environmental and social responsibilities toward current and future generations. Sustainability at product level is an important, future-oriented approach in the field of construction. In order to give quantified disclosures of a product's environmental impact through its entire life cycle, dormakaba provides Environmental Product Declarations (EPD), based on holistic life cycle assessments.

<https://www.dormakabagroup.com/en/sustainability/product-declarations>.

Axessor Apexx System Architecture & IT Security Guide - RevB
Subject to change without notice

Dormakaba SAL GmbH

Siemensstrasse 33
42551 Velbert
safelocks.de@dormakaba.com
T +49 2051 9111 0

dormakaba USA Inc.

1525 Bull Lea Road, Suite 100
Lexington, KY 460511
sales.safelocks.us@dormakaba.com
1-800-950-4744



AXESSOR APEXX IP
INSTALLATION AND
OPERATION GUIDES

dk.world/AxessorApexxIP

Axessor Apexx-Serie Software

Systemarchitektur- und IT-Sicherheitshandbuch für Axessor Apexx IP/CIT und CenconX



Inhalt

Apexx-Systemarchitektur	3
Übersicht	3
Axessor Apexx-Schlosssystem.....	3
CenconX-Schlosssystem.....	3
Mobile Geräte.....	4
API/Software – Komponenten	4
Apexx-API	4
Apexx-Client-Software	4
Apexx-Datenbank	4
MQTT-Broker/Server	5
SMTP	5
SSO.....	5
Benutzerkonfiguration – Axessor Apexx	5
Benutzerkonfiguration – CenconX.....	6
Benutzerkonfiguration – Softwarebenutzer.....	6
Softwarebenutzer – Axessor Apexx	6
Softwarebenutzer – CenconX.....	6
Lizenzen	7
Methoden zur Firmware-Aktualisierung.....	7
Firmware-Aktualisierungen – Axessor Apexx-Schlosssystem.....	7
Firmware-Aktualisierungen – CenconX Schlosssystem.....	7
Datenübertragung	8
Sicherheits- und Datenverschlüsselung	10
Public Key-Infrastruktur (PKI)	11

Computer-Hardware-Konfigurationen.....	13
Konfiguration mit einem Computer (USB-Verbindung)	13
Konfiguration mit einem Computer (TCP/IP).....	14
Konfiguration mit mehreren Computern.....	15
Besondere Hinweise zur Datenbank.....	17
Empfohlene Mindestanforderungen an Apexx-Computer	17
Spezifikationen des Apexx-Mobilgeräts	17
Apexx IT-Sicherheitsleitfaden	18
Hinweise zur lokalen Software	18
Kopplung der lokalen Software mit der eBox (Axessor Apexx).....	18
Notfallwiederherstellung	19
Anzeigen und Exportieren von Apexx-Ereignisprotokollen	20
Quintessenz	21

Apexx-Systemarchitektur

Übersicht

Die **Software der Apexx-Serie** ermöglicht die Verwaltung und Konfiguration verschiedener Aspekte der Axessor Apexx- und CenconX-Schlosssysteme über Fernzugriff. In diesem Dokument werden Aspekte der Systemarchitektur und der Computerinfrastruktur sowie die Anforderungen für die Verwendung der Software der Apexx-Serie zur Unterstützung und Verwaltung der Axessor Apexx- und CenconX-Schlosssysteme beschrieben.

Axessor Apexx-Schlosssystem

Axessor Apexx-Schlosssysteme bestehen aus 2 sicheren Kommunikationsnetzwerken: **CAN-Bus des Schlosssystems** und **API/Software-Netzwerk**

Der **CAN-Bus des Schlosssystems** unterstützt die folgenden Komponenten:

- **Tastaturen der Apexx-Serie** (maximal = 2, minimal/erforderlich = 1)
 - Wird als Benutzeroberfläche für den Zugriff auf das Schlosssystem und die Konfiguration verwendet
- **Schlösser der Apexx-Serie** (maximal = 16, minimal/erforderlich = 1)
 - Physisches elektromechanisches Schloss, das den Zugang des Benutzers zum Tresor steuert
- **Apexx eBox** (für Modus mit Netzwerk/IP-Verbindung erforderlich)
 - Funktioniert als Protokollkonverter (IP zu CAN-Bus) zwischen dem Axessor Apexx-Schlosssystem und der API/Software
 - Funktioniert auch als I/O-Box (Eingang/Ausgang)

CenconX-Schlosssystem

Die CenconX-Schlosssysteme bestehen aus 2 sicheren Kommunikationsnetzwerken: **Schlosssystem** und **API/Software-Netzwerk**

Das **Schlosssystem** unterstützt die folgenden Komponenten:

- **Tastaturen der CenconX-Serie** (1)
 - Wird als Benutzeroberfläche für den Zugriff auf das Schlosssystem und die Konfiguration verwendet
- **Schlösser der CenconX-Serie** (1)
 - Physisches elektromechanisches Schloss, das den Zugang des Benutzers zum Tresor steuert

Mobile Geräte

Die Safe Locks Mobile App von dormakaba dient als Schnittstelle zu den Schlosssystemen Axessor Apexx und CenconX. Die App ist bei Google Play und im Apple Store kostenlos zum Download verfügbar, ist aber erst nach der Registrierung mit der Software der Apexx-Serie funktionsfähig. Informationen zur Verwendung der mobilen App und zur Registrierung eines mobilen Geräts finden Sie im CenconX System User Guide (Dokumentnummer CX003.0524) und im Hilfemenü der Software der Apexx-Serie.

- **Axessor Apexx-Schlosssysteme** > Axessor Apexx-Geräte mit Firmware-Version 2.1.x.x oder höher können mobile Geräte über die dormakaba **Safe Locks Mobile App** einbinden.
- **CenconX-Schlosssysteme** > Die **Safe Locks Mobile App** von dormakaba fungiert als Brücke zwischen dem CenconX-Schlosssystem und der API/Software und dient zur Authentifizierung und Öffnung von CenconX-Schlössern.

API/Software – Komponenten

Die **API/Software** besteht aus 4 Hauptkomponenten:

- Apexx-API
- Apexx-Client-Software
- Apexx-Datenbank – Microsoft SQL Server 2019 Express
- MQTT-Broker/Server

Hinweis: Der Apexx-Server/-Client muss zur Kommunikation mit den mobilen Geräten mit einer öffentlich zugänglichen IP eingerichtet werden.

Apexx-API

Die Anwendungsprogrammierschnittstelle (API) fungiert in der MQTT-Architektur sowohl als Herausgeber (Publisher) als auch als Teilnehmer (Subscriber).

Apexx-Client-Software

Die Apexx-Client-Software („Software der Apexx-Serie“) ist eine grafische Benutzeroberfläche (GUI), die es den Softwarebenutzern ermöglicht, die API zu verwenden, um Aktionen im Apexx-/CenconX-System auszuführen (Systemeinstellungen ändern, Daten speichern/abrufen usw.).

Der Apexx-Client unterstützt mehrere Benutzer, aber nicht gleichzeitig auf einem Client. Es kann immer nur eine Person bei einer einzigen Client-Instanz angemeldet sein.

Apexx-Datenbank

Die Apexx-Datenbank dient als Hauptspeicherort für Daten im Apexx-System. Die Apexx-Datenbank verwendet Microsoft SQL Server 2019 Express, das proprietäre relationale Datenbankmanagementsystem von Microsoft, als Mittel zum Speichern und Abrufen von Systemdaten.

MQTT-Broker/Server

Message Queuing Telemetry Transport, kurz MQTT, ist ein Messaging-Protokoll, das ein Publish-Subscribe-Modell zur Erleichterung der Kommunikation zwischen Geräten verwendet. Der MQTT-Broker/Server fungiert als zentraler Messaging-Hub und nutzt das MQTT-Protokoll zur Verwaltung der Kommunikation zwischen Geräten. MQTT überträgt Nachrichten zwischen der Windows-Client-Software und der eBox.

SMTP

Die Software der Apexx-Serie verwendet das Simple Mail Transport Protocol (SMTP), um Folgendes zu senden: aktive Warnmeldungen, geplante Berichte und Informationen zur Konfiguration von mobilen Geräten.

- Aktive Alarmer werden an Empfänger gesendet, wenn ein oder mehrere vom Softwarebenutzer ausgewählte Prüfereignisse auftreten.
- Geplante Berichte können nach einem benutzerdefinierten Zeitplan auch über SMTP per E-Mail an die Empfänger gesendet werden.
- Beim Hinzufügen eines neuen Mobilgeräts in der Software der Apexx-Serie haben Sie die Möglichkeit, den generierten QR-Code für die Konfiguration des mobilen Geräts zu verwenden. Wenn Sie den QR-Code mit der Safe Locks Mobile App scannen, sendet das System die Konfigurationsinformationen über SMTP an das mobile Gerät.
- Informationen zur Konfiguration der SMTP-Einstellungen finden Sie im Hilfemenü der Software der Apexx-Serie.

SSO

Die Software der Apexx-Serie nutzt Single Sign-On, um sicherzustellen, dass sich ein Softwarebenutzer mit seinen Anmeldeinformationen bei der API anmelden kann.

Benutzerkonfiguration – Axessor Apexx

Die Axessor Apexx-Systembenutzer lassen sich in zwei verschiedene Kategorien einteilen:

Tresorschlossbenutzer und **Softwarebenutzer**

Tresorschlossbenutzer sind Benutzer, die das Axessor Apexx-Schlosssystem (bestehend aus den physischen Tastaturen, den Schlössern und der eBox) verwenden und über eindeutige Anmeldeinformationen und Rollen mit Berechtigungen verfügen, die ihren Zugang zum Schlosssystem bestimmen.

Tresorschlossbenutzer verwenden numerische Benutzer-IDs und PINs, um über die Tastatur der Apexx-Serie auf das Schlosssystem zuzugreifen. Diese Betriebsart wird als Bankmodus (auch statischer Modus) bezeichnet.

Die drei Standardtypen der Tresorschlossbenutzer (Administrator, Manager und Benutzer) bilden eine Hierarchie aus Benutzern mit jeweils vordefinierten Rollen und Berechtigungen innerhalb des Schlosssystems. Zusätzlich zu diesen Benutzertypen können mit den administrativen Tools der Software der Apexx-Serie weitere Tresorschlossbenutzerrollen erstellt werden, deren Berechtigungen durch einen Softwarebenutzer definiert werden. Diese zusätzlichen Benutzerrollen werden auf der Grundlage der drei Standardbenutzertypen erstellt, sodass die neuen Benutzertypen die Anpassungsanforderungen des Kunden erfüllen.

Bei Axessor Apexx-Geräten mit Firmware-Versionen 2.1.x.x oder höher sind zusätzliche Benutzertypen (ein primärer Administrator und ein Mieter-Administrator) sowie zwei zusätzliche Benutzermodi (OTC-Modus und ICS-Modus) verfügbar, welche die Verwendung mobiler Geräte für den Schlosszugang ermöglichen. Weitere Informationen zu den Tresorschlossbenutzertypen und Benutzermodi finden Sie in der Tastaturbedienungsanleitung der Apexx-Serie (Dokumentnummer 802.0622).

Benutzerkonfiguration – CenconX

Die Axessor Apexx-Systembenutzer lassen sich in zwei verschiedene Kategorien einteilen:

Tresorschlossbenutzer und **Softwarebenutzer**

Tresorschlossbenutzer sind Benutzer, die das CenconX-Schlosssystem (bestehend aus den physischen Tastaturen, den Schlössern usw.) verwenden und über eindeutige Anmeldeinformationen und Rollen mit Berechtigungen verfügen, die ihren Zugang zum Schlosssystem bestimmen.

Zu den Tresorschlossbenutzertypen in CenconX-Systemen gehören Administratoren, Manager, Benutzer mit statischer PIN (Bankmodus) und OTC-Benutzer (Einmalcode). Weitere Informationen zu den Benutzertypen und deren Berechtigungen finden Sie im CenconX System User Guide (Dokumentnummer CX003.0524).

Benutzerkonfiguration – Softwarebenutzer

Softwarebenutzer sind Benutzer, die die Software der Apexx-Serie ausführen und die Software-Tools verwenden, um Management- und Administratöraufgaben durchzuführen. Im Gegensatz zu Tresorschlossbenutzern haben Softwarebenutzer keinen direkten Zugang zum physischen Schlosssystem (Tresortüren öffnen/schließen), sondern führen Administrator-/Managementaufgaben über die Software aus (Hinzufügen von Schlossbenutzern, Passwörter von Schlossbenutzern zurücksetzen).

Softwarebenutzer verwenden Anmeldeinformationen, um über Single Sign-On (SSO) den Zugriff auf die Software der Apexx-Serie zu erhalten. Andere Authentifizierungsmethoden für Benutzer der Software der Apexx-Serie umfassen die Windows-Authentifizierung (mit Ausnahme von Entra ID), die Windows-Domänen-Authentifizierung und Google OAuth 2.0.

Softwarebenutzer, die über eine Softwarebenutzer-Schreibberechtigung verfügen, können neue Softwarebenutzer hinzufügen und die Lese-/Schreibberechtigungen konfigurieren.

Softwarebenutzer – Axessor Apexx

Zu den Softwarebenutzertypen in Axessor Apexx-Systemen gehören Administratoren und Manager. Bei Geldtransporten spielen auch Dispatcher und Audit-Benutzer eine Rolle (**Hinweis:** Gerätefirmware 2.1.x.x und höher erforderlich).

Weitere Details zu den Softwarebenutzertypen und Berechtigungen finden Sie im Hilfemenü der Software der Apexx-Serie.

Softwarebenutzer – CenconX

Zu den Softwarebenutzertypen in CenconX-Systemen gehören Administratoren, Manager, Dispatcher und Audit-Benutzer. Weitere Informationen zu den Benutzertypen und deren Berechtigungen finden Sie im CenconX System User Guide (Dokumentnummer CX003.0524).

Bei der Einrichtung Ihres CenconX-Schlosssystems haben Sie die Möglichkeit, einen Client/eine Datenbank für einen einzigen Eigentümer (primärer Dispatcher) zu konfigurieren, oder Sie richten einen zweiten Client/eine zweite Datenbank ein, um einem sekundären Dispatcher die gemeinsame Kontrolle über die Systemverwaltung und den Zugriff zu ermöglichen. Weitere Informationen finden Sie im CenconX System User Guide (Dokumentnummer CX003.0524).

Lizenzen

Für die Software der Apexx-Serie sind mehrere Lizenztypen verfügbar, die jeweils unterschiedliche Softwarefunktionen und -Features freischalten. Weitere Informationen finden Sie in den Preislisten für Axessor Apexx IP und CenconX.

Methoden zur Firmware-Aktualisierung

Der Prozess der Aktualisierung der Firmware Ihrer Axessor Apexx-Geräte hängt davon ab, welche Lizenz Sie erworben haben.

Weitere Informationen zum Prozess der Firmware-Aktualisierung finden Sie im Axessor Apexx System User Guide (Dokumentnummer 802.0622), im CenconX User Guide (Dokumentnummer CX003.0524) und im Hilfemenü der Software der Apexx-Serie.

Firmware-Aktualisierungen – Axessor Apexx-Schlosssystem

Lokale Firmware-Aktualisierungen lassen sich durch den Aufbau einer temporären USB-Verbindung zwischen dem Computer, auf dem die Software der Apexx-Serie installiert ist, und der Tastatur Ihres Schlosssystems durchführen.

Remote-Firmware-Aktualisierungen können über eine Netzwerkverbindung über die eBox durchgeführt werden. Dies ist ein dreistufiger Prozess:

1. Ein Softwarebenutzer initiiert den Prozess der Remote-Firmware-Aktualisierung, indem er die Firmware von der API/Software über die eBox an das Schlosssystem überträgt.
2. Die Firmware wird heruntergeladen und im Schlosssystem gespeichert. Auf dem Display der Tastatur erscheint eine Meldung, die den Tresorschlossbenutzer darüber informiert, dass eine Firmware-Aktualisierung ansteht.
3. Ein Tresorschlossbenutzer gibt über die Tastatur gültige Anmeldeinformationen (Benutzer-ID und PIN) ein und startet dann die Firmware-Aktualisierung.

Firmware-Aktualisierungen – CenconX Schlosssystem

Lokale Firmware-Aktualisierungen lassen sich durch den Aufbau einer temporären USB-Verbindung zwischen dem Computer, auf dem die Software der Apexx-Serie installiert ist, und der Tastatur Ihres Schlosssystems durchführen.

Mobile Benutzer von CenconX haben zudem die Möglichkeit, mithilfe der Safe Locks Mobile App von dormakaba **mobile Firmware-Aktualisierungen** zu erhalten. Dabei werden die Dateien für die Firmware-Aktualisierung über die Software der Apexx-Serie an das mobile Gerät des Benutzers gesendet. Der mobile Benutzer kann sich dann bei der Safe Locks App anmelden, die erforderlichen Dateien herunterladen und dann den Aktualisierungsprozess über eine BLE-Verbindung zwischen dem mobilen Gerät und der CenconX-Tastatur einleiten.

Datenübertragung

Abbildung 1 und die dazugehörige Tabelle zeigen den Datenfluss zwischen den verschiedenen Hardware- und Softwarekomponenten des Axessor Apexx-Schlosssystems.

Kommunikationsport	Beschreibung
443	Dieser Port wird für den ausgehenden TCP/IP-Verkehr verwendet.
587	Dieser Port wird für die Kommunikation mit dem SMTP-Host verwendet. Er ist erforderlich und standardmäßig auf 587 eingestellt.
5001	Dies ist der Standardport für die Inbetriebnahme eines Apexx-Schlosssystems.
8883	Dies ist der vom MQTT-Broker verwendete Standardport.

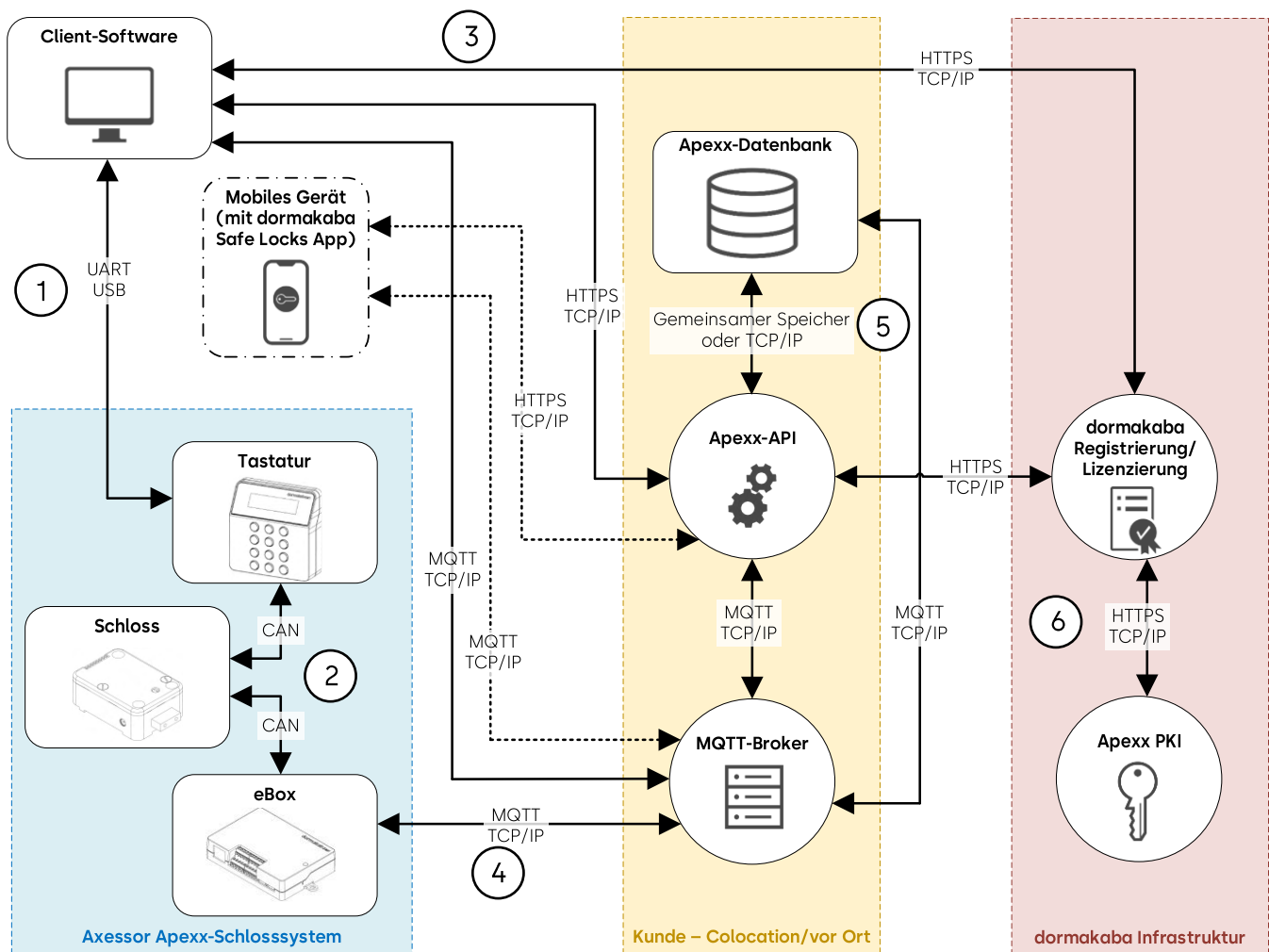


Abbildung 1: Apexx-Systemarchitektur mit Axessor Apexx-Schlosssystem – Systemkomponenten und Datenübertragung

	Kommunikationsprotokolle	Datenfluss	Beschreibung/Zweck
1	UART over USB	Bidirektionaler Pfad: Client-Software zu Tastatur	Direkter Abruf von Konfigurationen und von Prüfberichten
2	CAN	Bidirektionaler Pfad: - Tastatur zu Schloss - Schloss zu eBox	Kommunikation zwischen Geräten
3	HTTPS over TCP/IP	Bidirektionaler Pfad: Client-Software zu dormakaba Registrierung/Lizenzierung	Online-Lizenzierung und -Registrierung
4	MQTT over TCP/IP	Bidirektionaler Pfad: - Client-Software zu MQTT-Broker Bidirektionaler Pfad: - eBox zu MQTT-Broker Bidirektionaler Pfad: - Gerät mit dormakaba Safe Locks Mobile App zu MQTT-Broker	Abruf von Konfigurationen und von Prüfberichten im Netzwerkbetrieb
5	Gemeinsamer Speicher oder TCP/IP	Bidirektionaler Pfad: Apexx-API zu Apexx-Datenbank	Persistente Datenspeicherung mit SQL-Server
6	HTTPS over TCP/IP	Bidirektionaler Pfad: - Client-Software zu Apexx-API - Apexx-API zu dormakaba Registrierung/Lizenzierung - dormakaba Registrierung/Lizenzierung zu Apexx-PKI - Gerät mit dormakaba Safe Locks Mobile App zu Apexx-API	Ausstellung von x.509-Zertifikaten

Abbildung 2 zeigt ein ähnliches Schema wie in Abbildung 1, jedoch mit einem CenconX-Schlosssystem anstelle des Axessor Apexx-Schlosssystems. In diesem Fall dient das mobile Gerät als Kommunikationskanal zwischen dem CenconX-Schlosssystem und der Softwareinfrastruktur.

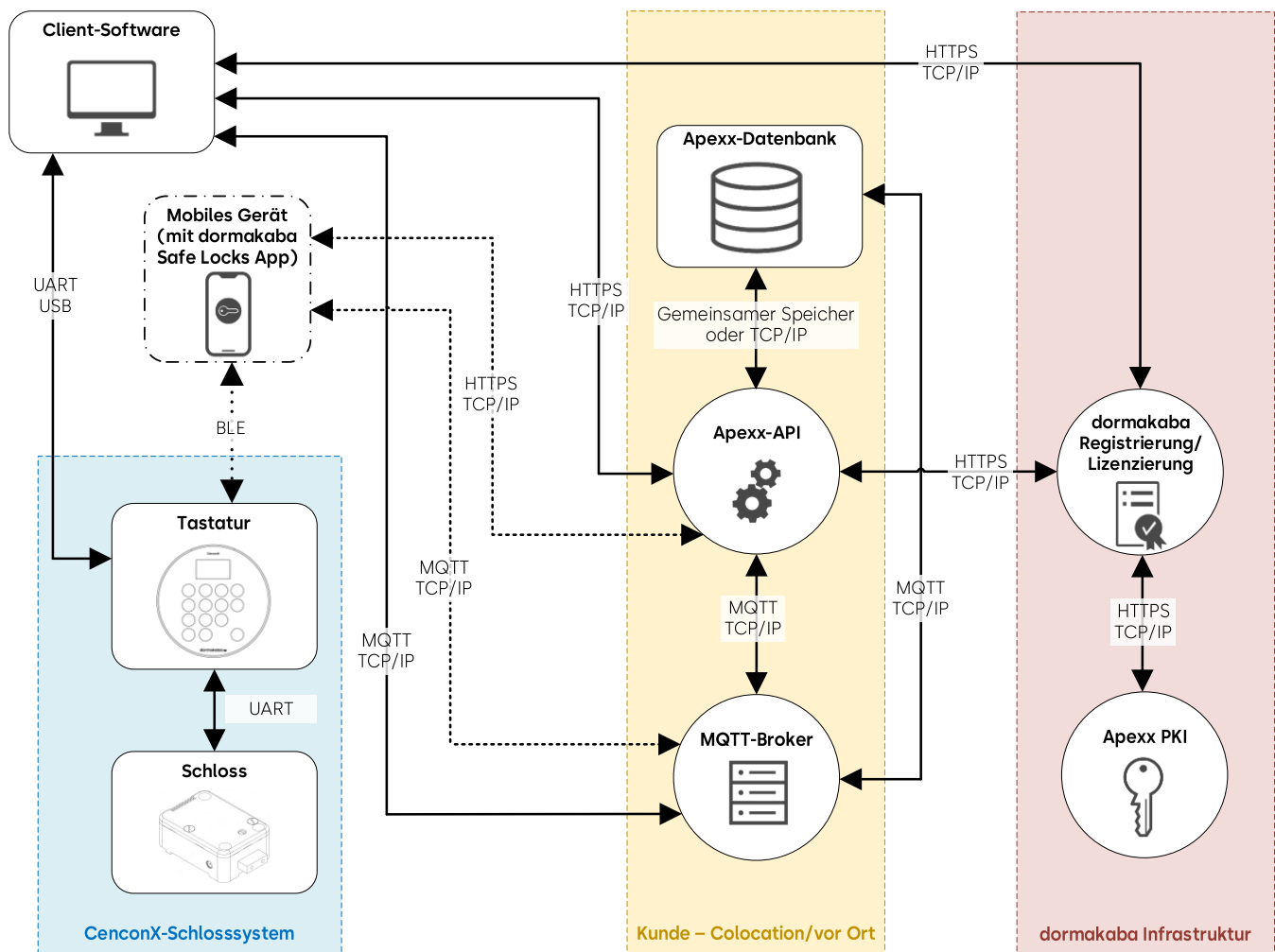


Abbildung 2: Apexx-Systemarchitektur mit CenconX-Schlosssystem – Systemkomponenten und Datenübertragung

Sicherheits- und Datenverschlüsselung

Die Software der Apexx-Serie, die CenconX-Schlosssysteme, die Axessor Apexx-Schlosssysteme und die in Betrieb genommenen mobilen Geräte verwenden mehrere Verschlüsselungsmethoden, darunter AES256, PBKDF2 und TLS-Zertifikate, um die sichere Kommunikation und Speicherung von Daten zu gewährleisten.

Public Key-Infrastruktur (PKI)

Die Software der Apexx-Serie, die CenconX-Schlosssysteme, die Axessor Apexx-Schlosssysteme und die in Betrieb genommenen mobilen Geräte nutzen eine Public Key-Infrastruktur, um digitale Zertifikate zu erstellen, zu speichern und über Zertifizierungsstellen an Apexx-Geräte zu verteilen.

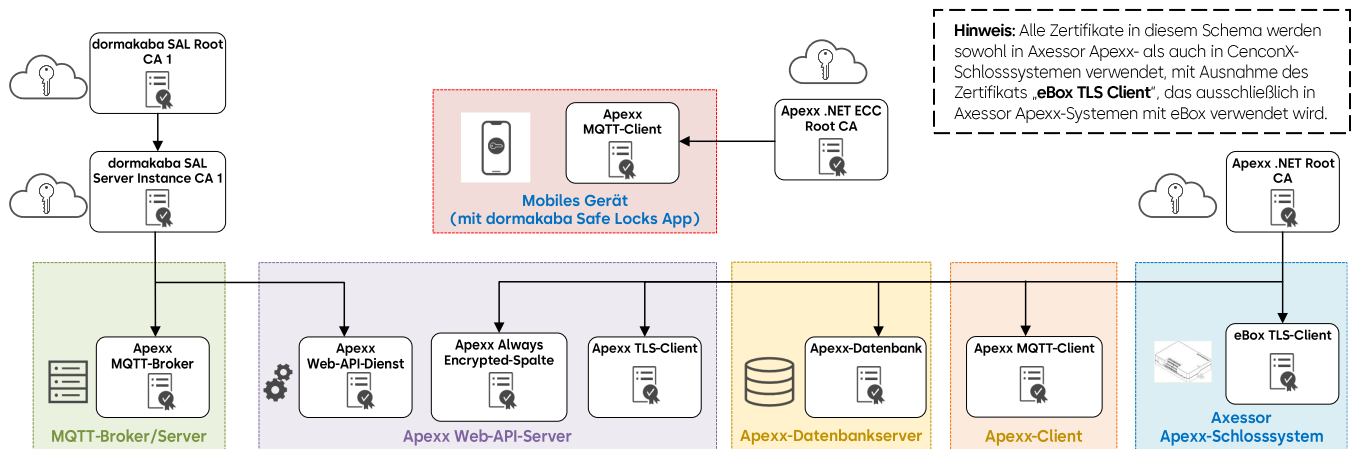


Abbildung 3: Public Key-Infrastruktur

Zertifikatstyp	Beschreibung
dormakaba SAL Root CA	- Dieses Zertifikat wird vor ihrer Auslieferung auf die Geräte geladen und wird per Firmware-Aktualisierung ersetzt. - Während der Installation der Software der Apexx-Serie wird dieses Zertifikat beim Ausführen der Prerequisites Installer-Datei auf den Client- und Serverrechnern (gespeichert im Ordner „Vertrauenswürdige Stammzertifizierungsstellen“) auch installiert.
dormakaba SAL Server Instance CA	- Server, auf denen lokale Softwaredienste für Apexx ausgeführt werden, benötigen von der dormakaba SAL-PKI signierte Zertifikate, damit die Geräte ihnen vertrauen. - Dieses Zertifikat muss auf allen Servern bereitgestellt werden, auf denen lokale Softwaredienste ausgeführt werden. - Während der Installation der Software der Apexx-Serie wird dieses Zertifikat beim Ausführen der Prerequisites Installer-Datei auf den Client- und Serverrechnern (gespeichert im Ordner „Zwischenzertifizierungsstellen“) auch installiert.
Apexx MQTT-Broker	- Wird während der Softwareinstallation erstellt. - Wird für TLS-Verbindungen und die Authentifizierung verwendet.
Apexx Web-API-Dienst	- Wird während der Softwareinstallation erstellt. - Enthält den Namen des Servers (Computer, auf dem dieser Dienst installiert ist), die vertrauenswürdige Zertifizierungsstelle und den öffentlichen Verschlüsselungsschlüssel des Servers.
Apexx TLS-Client	- Wird für die Authentifizierung des Apexx-Clients verwendet. - Das Zertifikat ist dann ein verifizierter Benutzer, wenn der Aussteller mit der installierten Apexx .NET Root CA auf dem Broker-Server übereinstimmt.
Apexx-Datenbank	- SQL Server unter Windows ist die einzige unterstützte Datenbank-Engine. - In der Instanz/Datenbank sind die folgenden Einstellungen aktiviert: - Windows-Authentifizierung - Die rollenbasierte Zugriffssteuerung (RBAC) wird zusammen mit der Windows-Authentifizierung zur Steuerung der Berechtigungen verwendet.
eBox TLS-Client	- Wird für die Authentifizierung der eBox verwendet. - Das Zertifikat ist dann ein verifizierter Benutzer, wenn der Aussteller mit der installierten Apexx .NET Root CA auf dem Broker-Server übereinstimmt.

Zertifikatstyp	Beschreibung
Apexx .NET Root CA	• Wird während der Softwareinstallation erstellt und im Zertifikatspeicher des lokalen Rechners im Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ gespeichert. • Während der API-Installation wird es im Ordner „Persönliche Zertifikate“ des lokalen Rechners gespeichert (LM\Personal\Certificates). • Jeder Computer, auf dem die Software ausgeführt wird (Client, Server, Datenbank usw.), benötigt für die Zwecke der Sicherheit/Identifizierung eine Kopie dieses Zertifikats. • Die lokale Software-PKI signiert Zertifikatsanforderungen für alle Clients des MQTT-Brokers. • Diese Zertifikate werden sowohl für den Aufbau vertrauenswürdiger TLS-Verbindungen (Transport Layer Security) als auch für die Authentifizierung beim MQTT-Broker verwendet. • Damit können auch die von SQL Server für TLS verwendeten Zertifikate signiert werden. • Verwendet RSA für Signaturen.
Apexx .NET ECC Root CA	• Wird während der Softwareinstallation erstellt und im Zertifikatspeicher des lokalen Rechners im Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ gespeichert. • Während der API-Installation wird es im Ordner „Persönliche Zertifikate“ des lokalen Rechners gespeichert (LM\Personal\Certificates). • Jeder Computer, auf dem die Software ausgeführt wird (Client, Server, Datenbank usw.), benötigt für die Zwecke der Sicherheit/Identifizierung eine Kopie dieses Zertifikats. • Die lokale Software-PKI signiert Zertifikatsanforderungen für alle Clients des MQTT-Brokers. • Diese Zertifikate werden sowohl für den Aufbau vertrauenswürdiger TLS-Verbindungen (Transport Layer Security) als auch für die Authentifizierung beim MQTT-Broker verwendet. • Damit können auch die von SQL Server für TLS verwendeten Zertifikate signiert werden. • Verwendet ECDSA für Signaturen.
Apexx MQTT-Client	• Wird bei der Software-Client-Anmeldung erstellt. • Wird für TLS-Verbindungen und die Authentifizierung verwendet.
Apexx Always Encrypted-Spalte	• Verschlüsselung von Daten in der API, die an die verschlüsselte Spalte in der Datenbank gehen. • Während der API-Installation wird es im Ordner „Persönliche Zertifikate“ des lokalen Rechners gespeichert (LM\Personal\Certificates).

Hinweis: Zertifikate können 60 Tage vor Ablauf erneuert werden, indem Sie Ihre Lizenz über das Online-Registrierungstool der Software der Apexx-Serie erneuern.

Computer-Hardware-Konfigurationen

Der Computer-Hardware/API/Software-Teil des Apexx-Systems kann in Abhängigkeit von der Komplexität Ihres Systems (Anzahl der Apexx-Schlosssysteme, deren Standorte usw.) auf verschiedene Weise konfiguriert werden. In diesem Abschnitt werden nur einige der möglichen Konfigurationen beschrieben. Weitere Informationen zu den Lizenzanforderungen für die verschiedenen Computer-/Hardware-Konfigurationen finden Sie in den Preislisten zu Axessor Apexx oder CenconX.

Hinweis: Falls gewünscht, kann jede der Softwarekomponenten (Client, Datenbank, API oder MQTT) auf einer virtuellen Maschine gehostet werden.

Konfiguration mit einem Computer (USB-Verbindung)

Abbildung 4 zeigt eine Basiskonfiguration mit nur einem Computer und einem Axessor Apexx-Schlosssystem und/oder einem CenconX-Schlosssystem. In dieser Konfiguration werden alle API-/Software-Elemente auf einem einzigen Computer gehostet, wobei eine USB-Verbindung verwendet wird, um vorübergehend eine Verbindung zum Axessor Apexx- oder CenconX-Schlosssystem für die Programmierung/Systemkonfiguration herzustellen.

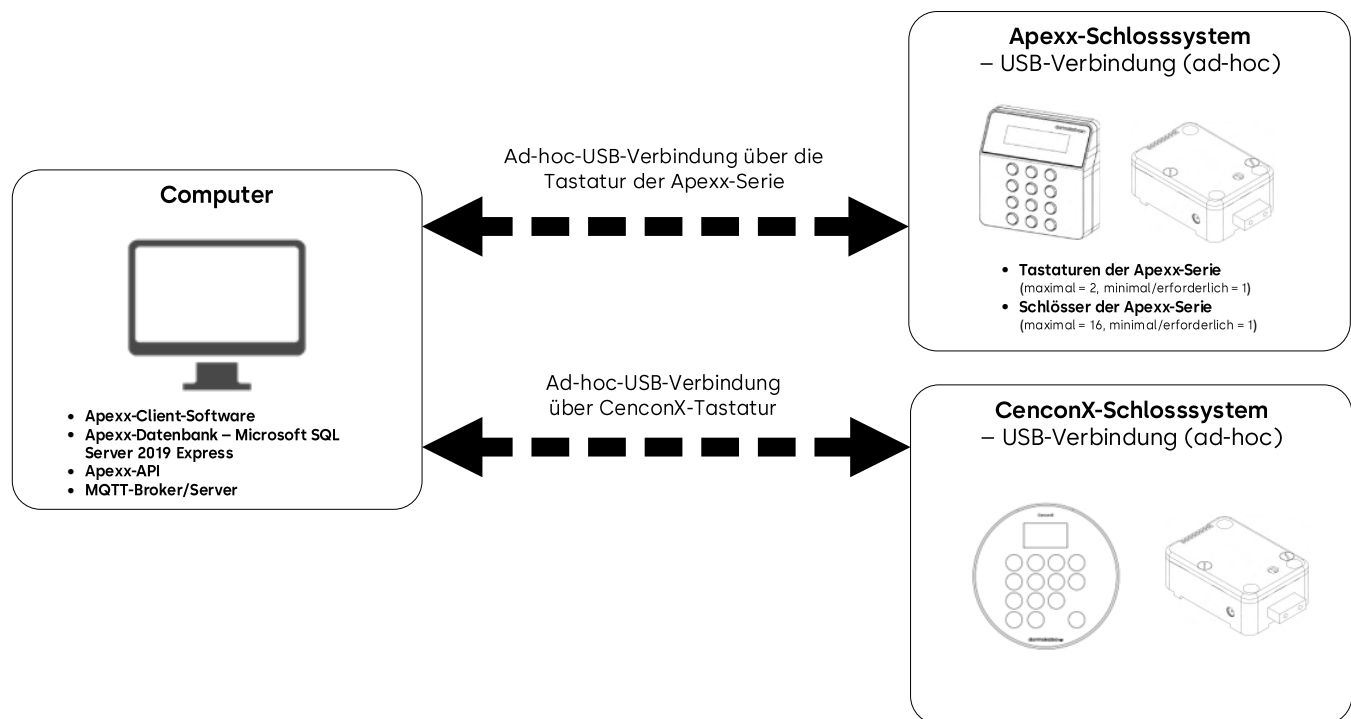


Abbildung 4: Konfiguration mit einem Computer – Ad-hoc-USB-Verbindung

Axessor Apexx-Schlosssysteme – Verbindung über USB

Diese Konfiguration eignet sich im Falle von Axessor Apexx gut für kleine Standorte, an denen sich der Computer und alle Komponenten des Schlosssystems (Tastaturen und Schlösser) am selben Ort befinden, bietet aber nicht die Vielseitigkeit und den Komfort, den die Netzwerkkonfigurationen mit der Apexx eBox bieten.

CenconX-Schlosssysteme – Verbindung über USB

Verbindungen nur über USB werden für CenconX-Systeme mit OTC-Funktionalität nicht empfohlen.

Konfiguration mit einem Computer (TCP/IP)

Abbildung 5 zeigt eine weitere einfache Konfiguration mit nur einem Computer und einem Axessor Apexx-Schlosssystem und/oder einem CenconX-Schlosssystem.

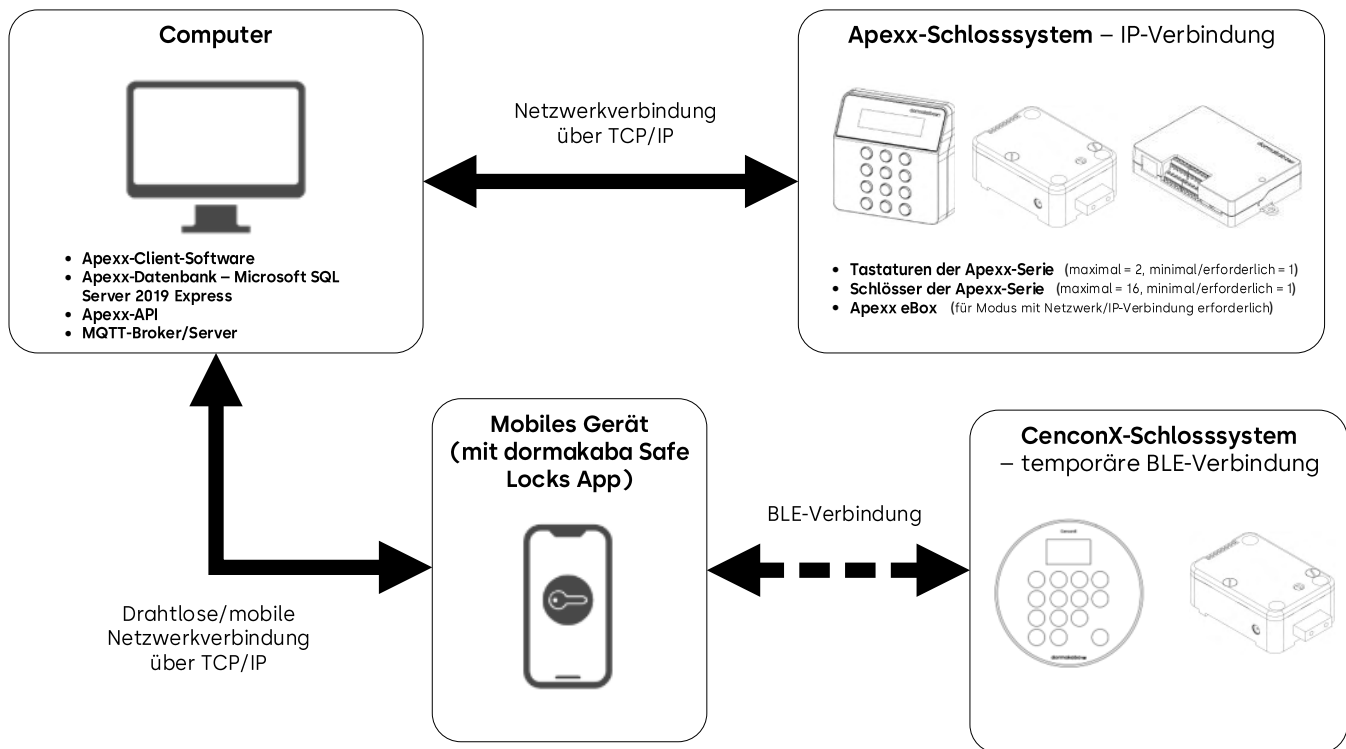


Abbildung 5: Konfiguration mit einem Computer – Netzwerk über eBox (TCP/IP) und Mobilfunk

Axessor Apexx-Schlosssysteme – Konfiguration mit einem Computer (TCP/IP)

Die Apexx eBox dient zur Herstellung einer Netzwerk-/IP-Verbindung für die kontinuierliche/Live-Kommunikation zwischen dem Computer und dem Axessor Apexx-Schlosssystem.

Bei Axessor Apexx-Schlosssystemen ist die Konfiguration auch für kleinere Konfigurationen geeignet, bei denen sich alle Geräte am selben Ort befinden. Durch die eBox kann der Systemadministrator jedoch alle Funktionen nutzen, die eine aktive IP-Verbindung bietet (Live-Audits, aktive Systemüberwachung, Remote-Firmware-Aktualisierungen und andere zusätzliche Hardware-/Softwarefunktionen).

CenconX-Schlosssysteme – Konfiguration mit einem Computer (TCP/IP)

Bei dem CenconX-Schlosssystem verbindet sich das mobile Gerät über eine Netzwerk-/IP-Verbindung mit dem Computer-Server/-Client und eine temporäre BLE-„Brückenverbindung“ verbindet das mobile Gerät mit dem CenconX-Schlosssystem.

Konfiguration mit mehreren Computern

Für größere Standorte mit größeren Gebäuden und/oder mehreren Schlosssystemen bietet die in Abbildung 6 gezeigte Konfiguration mit mehreren Computern zusätzliche Flexibilität.

Hinweis: Im System sind nur eine API, ein MQTT-Broker und eine SQL-Server-Datenbank zulässig.

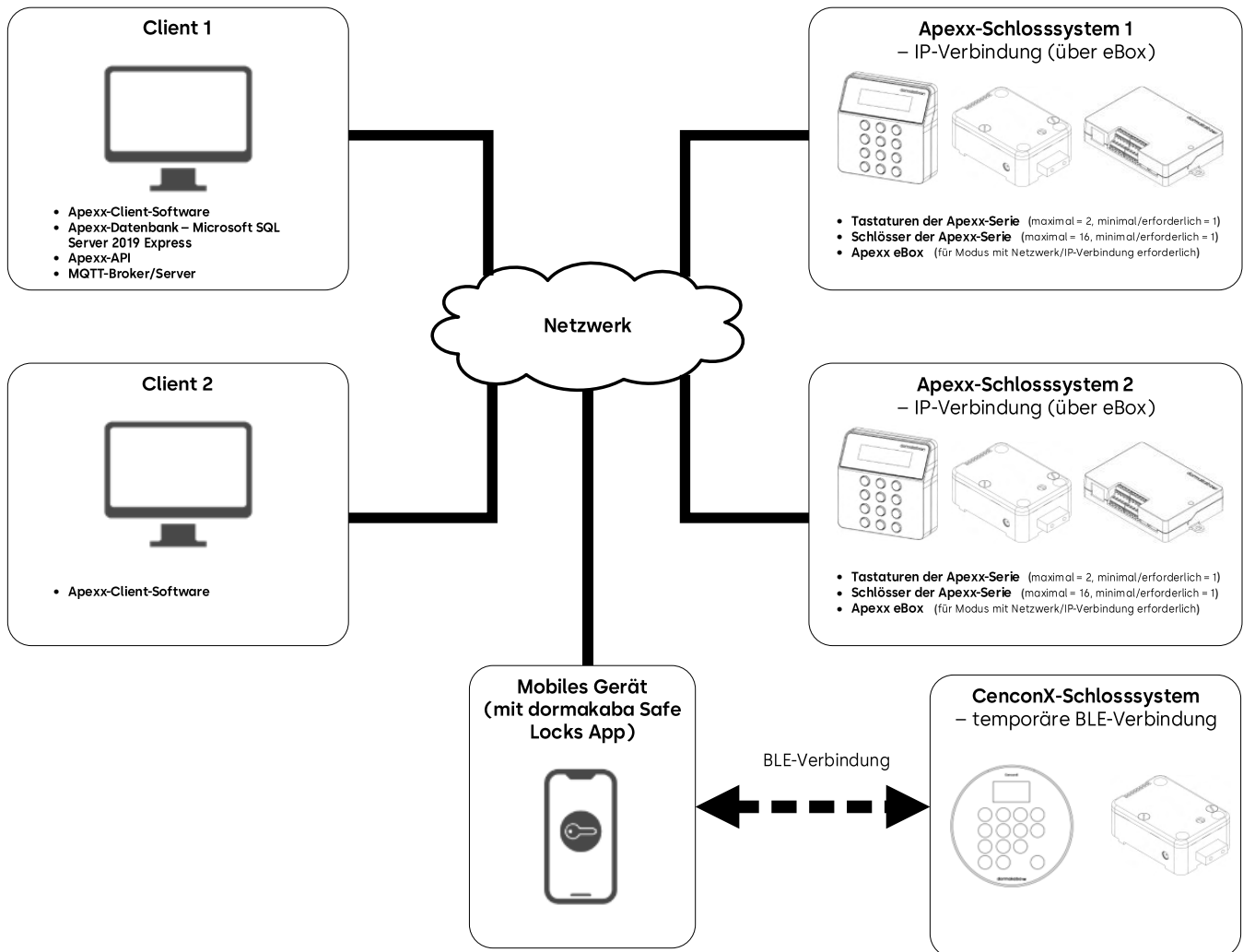


Abbildung 6: Konfiguration mit mehreren Computern und mehreren Schlosssystemen

In einer solchen Konfiguration können einzelne oder alle Softwarekomponenten auf einem oder mehreren Computern (oder virtuellen Maschinen) installiert werden, was zusätzlichen Komfort und Flexibilität bei der Ausführung und Konfiguration Ihrer Schlosssysteme bietet. Beachten Sie, dass jedes Axessor Apexx-Schlosssystem über eine Apexx eBox mit dem Netzwerk verbunden ist.

Dieses Konzept wird in dem in Abbildung 7 gezeigten System mit mehreren Computern und Schlosssystemen, die über mehrere Gebäude verteilt sind, noch erweitert.

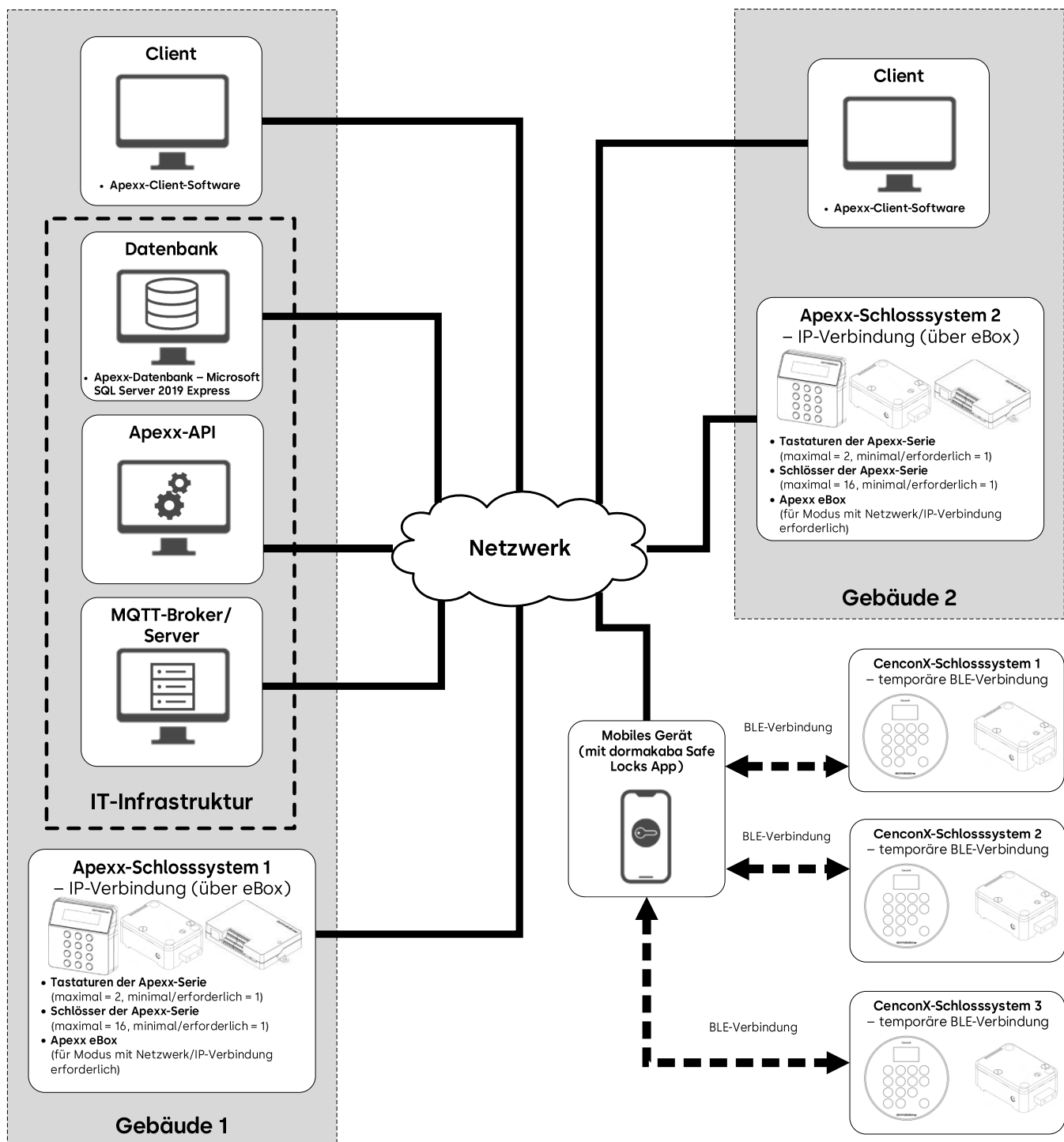


Abbildung 7: Konfiguration mit mehreren Computern/Schlosssystemen und mehreren Servern

Ein bemerkenswerter Unterschied zwischen dieser Konfiguration und allen anderen Konfigurationen besteht darin, dass mehrere Computer, auf denen verschiedene Softwarekomponenten gehostet werden, vorhanden sind. Beachten Sie, dass zwei der Computer in Gebäude 1 die Apexx-API bzw. die Apexx-Datenbank hosten. Diese beiden Computer können so konfiguriert werden, dass sie als API und Datenbank für die Schlosssysteme in Gebäude 1, Gebäude 2 und/oder jedes andere Schlosssystem im gesamten Netzwerk verwendet werden.

Dieses letzte Beispiel veranschaulicht, dass je nach den Anforderungen Ihres Unternehmens und Ihrer IT-Infrastruktur viele verschiedene Konfigurationen möglich sind.

Besondere Hinweise zur Datenbank

Die Software der Apexx-Serie enthält Microsoft SQL Server 2019 Express als dedizierte interne Datenbank-Engine.

	Microsoft SQL Server 2019 Express (64-Bit)
Datenbank-Limit	10 GB
Anzahl der CPUs	1 physischer Prozessor
RAM	1 GB
Unterstützte Betriebssysteme	Windows 10, Windows Server 2016, Windows Server 2019

Empfohlene Mindestanforderungen an Apexx-Computer

*Bei größeren Installationen Verdoppelung in Betracht ziehen

Apexx-Client-Workstation

- 2,0-GHz-Prozessor mit 4 Kernen*
- 16 GB RAM
- 500 GB Festplatte
- Windows 10 Professional 64-Bit

Apexx-Broker-Server

- 2,0-GHz-Prozessor mit 4 Kernen*
- 16 GB RAM
- 500 GB Festplatte
- Windows 2019 Server Standard 64-Bit

Apexx-Datenbank-Server und Apexx-API

- 2,0-GHz-Prozessor mit 6 Kernen*
- 32 GB RAM*
- 1 TB Festplatte
- Windows 2019 Server Standard 64-Bit
- Microsoft SQL Server Standard oder Enterprise

Hinweis: Falls gewünscht, kann jede der Softwarekomponenten (Client, Datenbank, API oder MQTT-Broker) auf einer virtuellen Maschine gehostet werden.

Spezifikationen des Apexx-Mobilgeräts

(Stand: Zeitpunkt der Veröffentlichung des Dokuments)

- Betriebssystem des mobilen Geräts: Android 8+ oder iOS 15+
- Muss BLE-kompatibel sein

Hinweis: Bei Google Play und im Apple Store finden Sie die neuesten Versionen der dormakaba Safe Locks Mobile App und Informationen zur Kompatibilität von Geräten/Betriebssystemen.

Apexx IT-Sicherheitsleitfaden

Hinweise zur lokalen Software

- Alle Teile der Software (MQTT, Client und API) sind als Windows-Anwendungen konzipiert. Um sie in einer Cloud-Umgebung nutzen zu können, muss man in der Lage sein, die Kommunikationskanäle zwischen ihnen zu verwalten.
- Die Kommunikationskanäle werden während der Installation eingerichtet. Diese basieren auf DNS (oder statischen IP-Adressen). Sobald die Installation abgeschlossen ist, werden aus Sicherheitsgründen Zertifikate eingerichtet. Diese Zertifikate müssen ordnungsgemäß verwaltet werden, um Angriffswege zu verhindern.
- Da die Kommunikation zum und vom Schlosssystem über MQTT over SSL erfolgt, müssen die Standardports erreichbar sein.
- Die Software erfordert die Ausführung eines Windows-Zertifikatssubsystems und einer SQL19-Datenbank.
- Die Software wird auf Mac- oder Linux-Systemen nicht unterstützt.
- Die getesteten Cloud-Umgebungen sind Azure und AWS.
- Ein und derselbe Benutzer kann nicht bei mehreren Clients gleichzeitig angemeldet sein.

Kopplung der lokalen Software mit der eBox (Axessor Apexx)

Die lokale Software und die Apexx eBox müssen gekoppelt werden, bevor eine Verbindung hergestellt werden kann. Wenn eine brandneue eBox installiert werden muss:

1. Die eBox wird am CAN-Bus angeschlossen.
2. Ein berechtigter Benutzer muss sich bei der Tastatur anmelden und die eBox am CAN-Bus in Betrieb nehmen (den CAN-Bus können keine nicht autorisierten Geräte überwachen).
3. Nach der Inbetriebnahme der eBox kann die eBox die Verschlüsselungsschlüssel für den CAN-Bus abrufen (AES-256 mit systemspezifischen Schlüsseln).
4. Sobald die eBox am CAN-Bus angeschlossen ist, muss eine Verbindung zur lokalen Software hergestellt werden. Die IP-Adresse kann in den Netzwerkeinstellungen im erweiterten Menü der Tastatur abgerufen und geändert werden. Wenn eine Einstellung vorhanden ist, wird sie verwendet. Andernfalls geht die eBox davon aus, dass DHCP zum Abrufen einer IP-Adresse verwendet wird.
5. Sobald eine gültige Etherneteinstellung vorhanden ist, versucht die eBox, sich mit dem MQTT-Server in der lokalen Software zu verbinden (entweder durch direkte IP-Kommunikation basierend auf den Einstellungen oder durch Broadcast im lokalen Netzwerk im Falle von DHCP). Dies erfolgt über TLS.

6. Wenn die lokale Software eine neue eBox erkennt, dann muss diese in der Software vor der erfolgreichen Anmeldung mit dem Anforderungscode autorisiert werden. Sobald die eBox in der Software autorisiert ist, erstellt die Software eine Verifizierungs-PIN, die auf der Tastatur validiert werden muss (Verifizierung der Software gegenüber der eBox und der eBox gegenüber der Software).
7. Nachdem das System verifiziert wurde, wird ein sicherer Kanal eingerichtet. Dies erfolgt über vorinstallierte, werkseitig signierte Zertifikate (PKI-Infrastruktur). Jede weitere Kommunikation wird mit TLS verschlüsselt.
8. TLS 1.2. Die eBox kommuniziert auch zunächst über den TCP-Port 5001 (API), um zu überprüfen, ob die Software aktiviert ist, und dann über Port 8883 (Standard) für die Kommunikation.
9. Die Software muss aktiviert sein und über die entsprechenden Zertifikate verfügen, damit die eBox ordnungsgemäß aktiviert wird. Deaktivierte Software führt zu einem Denial-of-Service.

Weitere Informationen zur Installation, zum Verbinden und zur Konfiguration der Apexx eBox finden Sie in der Axessor Apexx-Installationsanleitung (Dokumentnummer 801.0622), in der Tastaturbedienungsanleitung der Apexx-Serie (Dokumentnummer 802.0622) und im Hilfemenü der Software der Apexx-Serie.

Notfallwiederherstellung

Die lokale Software stellt zur Datenspeicherung eine Verbindung zur SQL19-Datenbank her (SQL19 Express von Microsoft – Referenz: <https://www.microsoft.com/en-ca/sql-server/sql-server-2019-pricing>). Die Konfiguration der Datenbank muss in der lokalen Software in Form einer Konfigurationsdatei eingegeben werden. Die Verschlüsselung/der Schutz und die Datenwiederherstellung folgen dann dem Pfad der SQL19-Datenbank. Es wird erwartet, dass die Datenbank von der lokalen IT-Abteilung verwaltet wird.

Der Wiederherstellungspfad besteht dann darin, die API, MQTT und den Client entweder mit einer neuen Kopie von dormakaba neu zu installieren oder eine lokale Sicherungskopie zu verwenden. Alle Daten ruhen in der SQL-Datenbank. API, MQTT und Client speichern keine Schloss- oder Benutzerdaten, sondern nur die Verbindungs- und Konfigurationseinstellungen.

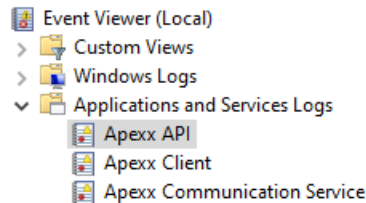
Die Datenbank wird zunächst automatisch vom API-Dienst erstellt. Die Datenbank verwendet standardmäßige dienstspezifische (API oder BROKER) NT-Dienstanmeldungen und authentifiziert sich über Kerberos-Kanäle. Die Standard-Datenbankeinstellungen sind Windows-Authentifizierung, verschlüsselte Spalten. Eine Verschlüsselung auf der Engine-Ebene wird empfohlen, ist aber nicht erforderlich.

Anzeigen und Exportieren von Apexx-Ereignisprotokollen



Über die Windows-Ereignisanzeige lassen sich Probleme im Zusammenhang mit Apexx-Anwendungen und -Dienstern anzeigen und beheben.

1. Ereignisanzeige öffnen > Geben Sie **„Ereignisanzeige“** in die Windows-Suchleiste ein und öffnen Sie das Programm.
2. Klicken Sie auf den Pfeil neben >  **„Anwendungs- und Dienstprotokolle“**, um die Liste zu erweitern.
3. Klicken Sie auf die Apexx-Anwendung/den Apexx-Dienst, um alle Ereignisse in Bezug auf diese Anwendung oder diesen Dienst (Apexx API, Apexx Client, Apexx Communication Service) anzuzeigen.



4. Von hier aus können Sie die Ereignisse nach Zeit, Ereignis-ID usw. sortieren, um die Anzeige und Fehlersuche bei Ihrer Apexx-Konfiguration zu erleichtern.
5. Apexx-Ereignisprotokolle exportieren > Unter **„Aktionen“** können Sie  **„Alle Ereignisse speichern unter...“** wählen, um die Ereignisprotokolle der ausgewählten Anwendung/des ausgewählten Dienstes zu exportieren und in einem von mehreren Formaten (.evtx, .xml, .txt, .csv) zu speichern.

Quintessenz

1. Nur Server mit lokaler Software müssen über IP-Adressen erreichbar sein – die eBox nicht.
2. Die Kommunikation zwischen eBox und lokaler Software (Datenverkehr über Intranet/Internet) wird mit TLS verschlüsselt.
3. Den SQL-Server sollten Sie in Ihren Notfallwiederherstellungsplan einbeziehen. Diese Datenbank ist für das Funktionieren des Systems von entscheidender Bedeutung.



Access Automation Solutions

Entrance Automation
Entrance Security



Access Control Solutions

Electronic Access & Data
Escape and Rescue Systems
Lodging Systems



Access Hardware Solutions

Door Closers
Architectural Hardware
Mechanical Key Systems



Services

Technical Support
Installation and commissioning
Maintenance and Repair



Key & Wall Solutions

Key Systems
Movable / Sliding Walls



Safe Locks

Electronic Safe Locks
Mechanical Safe Locks
Boltworks and Accessories



Glass systems

Manual door systems
Glass fittings
Horizontal Sliding Walls

Unser Nachhaltigkeitsversprechen

Wir engagieren uns für eine nachhaltige Entwicklung entlang unserer gesamten Wertschöpfungskette im Einklang mit unserer wirtschaftlichen, ökologischen und sozialen Verantwortung gegenüber heutigen und zukünftigen Generationen. Nachhaltigkeit auf Produktebene ist ein wichtiger, zukunftsweisender Ansatz im Bauwesen. Um die Umweltauswirkungen eines Produkts über seinen gesamten Lebenszyklus quantifizierbar darzustellen, erstellt dormakaba Umweltproduktdeklarationen (EPD), die auf ganzheitlichen Ökobilanzen basieren.

<https://www.dormakabagroup.com/en/sustainability/product-declarations>.

Dormakaba SAL GmbH

Siemensstrasse 33
42551 Velbert
safelocks.de@dormakaba.com
T +49 2051 9111 0

dormakaba USA Inc.

1525 Bull Lea Road, Suite 100
Lexington, KY 460511
sales.safelocks.us@dormakaba.com
1-800-950-4744



AXESSOR APEXX IP
INSTALLATION AND
OPERATION GUIDES

Software de la serie- Axessor Apexx

Guía de arquitectura de sistemas y seguridad de TI para Axessor Apexx IP/CIT y CenconX



Índice

Arquitectura del sistema Apexx	3
Resumen.....	3
Sistema de cerraduras Axessor Apexx	3
Sistema de cerradura CenconX.....	3
Dispositivos móviles	4
Componentes de API/software	4
API Apexx.....	4
Software de cliente Apexx.....	4
Base de datos Apexx.....	4
Bróker/Servidor MQTT	5
SMTP	5
SSO.....	5
Configuración de usuario - Axessor Apexx	5
Configuración de usuarios - CenconX.....	6
Configuración de usuarios - Usuarios de software	6
Usuarios del software - Axessor Apexx.....	6
Usuarios de software - CenconX.....	6
Licencias.....	7
Métodos de actualización del firmware	7
Actualizaciones de firmware - Sistema de cerraduras Axessor Apexx.....	7
Actualizaciones del firmware - Sistema de cerraduras CenconX	7
Tránsito de datos.....	8
Seguridad y cifrado de datos	10
Infraestructura de clave pública (PKI).....	11

Configuraciones del hardware informático.....	13
Configuración para un solo ordenador (conexión USB)	13
Configuración de un solo ordenador (TCP/IP)	14
Configuraciones de varios ordenadores	15
Consideraciones sobre la base de datos	17
Especificaciones mínimas del ordenador recomendadas para Apexx	17
Especificaciones del dispositivo móvil Apexx.....	17
Guía de seguridad informática de Apexx	18
Notas sobre el software local	18
Emparejamiento del software local con eBox (Axessor Apexx).....	18
Recuperación en caso de catástrofe	19
Visualización y exportación de registros de eventos de Apexx.....	19
Principales conclusiones.....	20

Arquitectura del sistema Apexx

Resumen

El **software de la serie Apexx** puede utilizarse para gestionar y configurar de forma remota diversos aspectos de los sistemas de cerraduras Axessor Apexx y CenconX. Este documento describe aspectos de la arquitectura del sistema, la infraestructura informática y los requisitos para utilizar el software de la serie Apexx para dar soporte y gestionar los sistemas de cerraduras Axessor Apexx y CenconX.

Sistema de cerraduras Axessor Apexx

Los sistemas de bloqueo Axessor Apexx constan de 2 redes de comunicación seguras: **el bus CAN del sistema de cerraduras** y **la red de API/software**

El **bus CAN del sistema de cerraduras** admite los siguientes componentes:

- **Teclados numéricos de la serie Apexx** (máximo = 2, mínimo/requerido = 1)
 - Se utiliza como una interfaz de usuario para acceder al sistema de bloqueo y configurarlo
- **Cerraduras de la serie Apexx** (máximo = 16, mínimo/requerido = 1)
 - Cerradura electromecánica física que controla el acceso del usuario a la caja fuerte
- **eBox de Apexx** (obligatoria para el modo en red/conectado por IP)
 - Funciona como convertidor de protocolo (IP a bus CAN) entre el sistema de cerraduras Axessor Apexx y la API/software
 - También funciona como en el cuadro de E/S (entrada/salida)

Sistema de cerradura CenconX

Los sistemas de bloqueo CenconX constan de 2 redes de comunicación seguras: **el sistema de cerradura** y **la red API/software**

El **sistema de cerradura** admite los siguientes componentes:

- **Teclados numéricos de la serie CenconX** (1)
 - Se utiliza como una interfaz de usuario para acceder al sistema de bloqueo y configurarlo
- **Cerraduras de la serie CenconX** (1)
 - Cerradura electromecánica física que controla el acceso del usuario a la caja fuerte

Dispositivos móviles

La aplicación móvil Safe Lock de dormakaba puede utilizarse como interfaz para los sistemas de cerraduras Axessor Apexx y CenconX. Está disponible para su descarga gratuita en Google Play y Apple Store, pero no es funcional hasta que se registra mediante el software de la serie Apexx. Para obtener información sobre el uso de la aplicación móvil y cómo registrar un dispositivo móvil, consulte la Guía del usuario del sistema CenconX (Documento n.º CX003.0524) y el menú de ayuda del software de la serie Apexx.

- **Sistemas de cerraduras Axessor Apexx** > Los dispositivos Axessor Apexx con versión de firmware 2.1.x.x o superior pueden incorporar dispositivos móviles a través de la **aplicación móvil Safe Locks** de dormakaba.
- **Sistemas de cerraduras CenconX** > La **aplicación móvil Safe Locks** de dormakaba funciona como puente entre el sistema de cerraduras CenconX y la API/software, sirviendo como medio para autenticar y abrir cerraduras CenconX.

Componentes de API/software

La **API/software** consta de 4 componentes principales:

- API Apexx
- Software de cliente Apexx
- Base de datos Apexx: Microsoft SQL Server 2019 Express
- Bróker/Servidor MQTT

Nota: el servidor/cliente Apexx debe configurarse utilizando una IP de acceso público para facilitar la comunicación con los dispositivos móviles.

API Apexx

La interfaz de programación de aplicaciones (API) actúa como editor y suscriptor en la arquitectura MQTT.

Software de cliente Apexx

El software de cliente Apexx ("Apexx Series Software") es una interfaz gráfica de usuario (GUI) que permite a los usuarios del software utilizar la API para realizar acciones en el sistema Apexx/CenconX (cambiar la configuración del sistema, almacenar/recuperar datos, etc.).

Este software admite varios usuarios, pero no es capaz de gestionar varios usuarios simultáneamente en un solo cliente: solo puede haber una persona conectada en una instancia de cliente al mismo tiempo.

Base de datos Apexx

La base de datos Apexx sirve como ubicación principal para el almacenamiento de datos en el sistema Apexx. La base de datos Apexx utiliza el sistema de gestión de bases de datos relacional propiedad de Microsoft, Microsoft SQL Server 2019 Express, como medio de almacenamiento y recuperación de datos del sistema.

Bróker/Servidor MQTT

Message Queuing Telemetry Transport (MQTT) es un protocolo de mensajería que utiliza un modelo de publicación-suscripción para facilitar la comunicación entre dispositivos. El bróker/servidor MQTT actúa como un núcleo de mensajería centralizado y utiliza el protocolo MQTT para gestionar la comunicación entre dispositivos. En concreto, MQTT transmite mensajes entre el software cliente de Windows y la eBox.

SMTP

El software de la serie Apexx utiliza el protocolo simple de transferencia de correo (SMTP) para enviar lo siguiente: alertas activas, informes programados e información sobre la configuración de dispositivos móviles.

- Las alertas activas se envían a los destinatarios en función de la aparición de uno o varios eventos de auditoría seleccionados por el usuario del software.
- Los informes programados pueden enviarse por correo electrónico a los destinatarios según un calendario definido por el usuario, también mediante SMTP.
- Al añadir un nuevo dispositivo móvil en el software de la serie Apexx, tiene la opción de utilizar el código QR generado para la configuración del dispositivo móvil. Cuando se utiliza la aplicación móvil Safe Locks para escanear el código QR, el sistema emplea SMTP para enviar la información de configuración al dispositivo móvil.
- Consulte el menú de ayuda del software de la serie Apexx para obtener información sobre cómo configurar los ajustes SMTP.

SSO

El software de la serie Apexx utiliza el inicio de sesión único, lo que garantiza que un usuario del software pueda utilizar sus credenciales para iniciar sesión en la API utilizando un único conjunto de credenciales.

Configuración de usuario - Axessor Apexx

Los usuarios del sistema Axessor Apexx se dividen en dos categorías distintas: ***usuarios de cerradura de caja fuerte*** y ***usuarios de software***

Los **usuarios de cerradura de caja fuerte** son usuarios que utilizarán el sistema de cerraduras Axessor Apexx (compuesto por los teclados numéricos físicos, las cerraduras y la eBox) y tendrán credenciales y funciones exclusivas con permisos que determinarán su acceso al sistema de cerraduras.

Los usuarios de cerradura de caja fuerte utilizan identificadores de usuario numéricos y PIN para acceder al sistema de bloqueo mediante el teclado numérico de la serie Apexx. Este modo de funcionamiento se conoce como Modo Banco (también conocido como Modo Estático).

Los tres tipos de usuario predeterminados de caja fuerte (administrador, gestor y usuario) constituyen una jerarquía de usuarios, cada uno con funciones y privilegios predefinidos dentro del sistema de bloqueo. Además de estos tipos de usuario, se pueden crear funciones de usuario de caja fuerte adicionales mediante las herramientas administrativas del software de la serie Apexx que tienen permisos definidos por un usuario de software. Estos roles de usuario adicionales se crean utilizando un marco de los 3 tipos de usuario iniciales, permitiendo así nuevos tipos de usuario para satisfacer las necesidades de personalización del cliente.

Los dispositivos Axessor Apexx con versiones de firmware 2.1.x.x o superiores introducen tipos de usuario adicionales (un Administrador Principal y un Administrador de Inquilinos), así como dos Modos de Usuario adicionales (Modo OTC y Modo ICS) que incorporan el uso de dispositivos móviles para el acceso a la cerradura. Consulte la Guía del usuario del sistema de teclado numérico de la serie Apexx (Documento n.º 802.0622) para obtener más información sobre los tipos de usuario de cerraduras de caja fuerte y los modos de usuario.

Configuración de usuarios - CenconX

Los usuarios del sistema Axessor Apexx se dividen en dos categorías distintas: **usuarios de cerradura de caja fuerte** y **usuarios de software**

Los **usuarios de cerradura de caja fuerte** son usuarios que utilizarán el sistema de cerraduras CenconX (compuesto por los teclados numéricos físicos, las cerraduras, etc.) y tendrán credenciales y funciones exclusivas con permisos que determinarán su acceso al sistema de cerraduras.

Los tipos de usuario de cerraduras de caja fuerte en los sistemas CenconX incluyen Administradores, Gerentes, Usuarios de PIN estático (Modo Banco) y Usuarios de OTC (código de un solo uso). Consulte la Guía del usuario del sistema CenconX (Documento n.º CX003.0524) para obtener más información sobre los tipos de usuario y sus permisos.

Configuración de usuarios - Usuarios de software

Los **usuarios de software** son aquellos que ejecutan el software de la serie Apexx y utilizan las herramientas de software para realizar tareas de gestión y administración. A diferencia de los usuarios de cerraduras de caja fuerte, los usuarios de software no acceden directamente al sistema físico de cerraduras (abrir/cerrar puertas de cajas fuertes), sino que realizan tareas administrativas/de gestión a través del software (añadir usuarios de cerraduras de caja fuerte o restablecer contraseñas de usuarios de cerraduras de caja fuerte).

Los usuarios de software utilizan credenciales para acceder al software de la serie Apexx mediante el inicio de sesión único (SSO). Otros tipos de autenticación para los usuarios del software de la serie Apexx incluyen la autenticación de Windows (con la excepción de Entra ID), la autenticación de dominio de Windows y Google OAuth 2.0.

Los usuarios de software que tienen permiso de "escritura" pueden añadir nuevos usuarios de software y configurar los permisos de lectura/escritura.

Usuarios del software - Axessor Apexx

Los tipos de usuario de software en los sistemas Axessor Apexx incluyen Administradores y Gerentes. Para las aplicaciones de efectivo en tránsito, los despachadores y los usuarios de solo auditoría también tienen una función que desempeñar (**nota:** se requiere un firmware de dispositivo 2.1.x.x y superior).

Consulte el menú de ayuda del software de la serie Apexx para obtener más información sobre los tipos de usuario de software y sus permisos.

Usuarios de software - CenconX

Los tipos de usuario de software en los sistemas CenconX incluyen Administradores, Gerentes, Despachadores y Usuarios de Solo Auditoría. Consulte la Guía del usuario del sistema CenconX (Documento n.º CX003.0524) para obtener más información sobre los tipos de usuario y sus permisos.

Al configurar su sistema de cerraduras CenconX, tiene la posibilidad de configurar un solo cliente/base de datos para un solo Propietario (Despachador Principal), o puede introducir un segundo cliente/base de datos para permitir que un Despachador Secundario tenga control compartido sobre la gestión y el acceso al sistema. Consulte la Guía del usuario del sistema CenconX para obtener más información (Documento n.º CX003.0524).

Licencias

El software de la serie Apexx dispone de varios tipos de licencia, cada uno de los cuales desbloquea diferentes funciones y características del software. Consulte el catálogo de precios de Axessor Apexx IP y CenconX para obtener más información.

Métodos de actualización del firmware

El proceso de actualización del firmware de su dispositivo Axessor Apexx varía en función de la licencia que haya adquirido.

Para obtener más información sobre el proceso de actualización del firmware, consulte la Guía del usuario del sistema Axessor Apexx (Documento n.º 802.0622), la Guía del usuario de CenconX (Documento n.º CX003.0524) y el menú de ayuda del software de la Serie Apexx.

Actualizaciones de firmware - Sistema de cerraduras Axessor Apexx

Las **actualizaciones locales del firmware** pueden realizarse estableciendo una conexión USB temporal entre el ordenador que aloja el software de la serie Apexx y el teclado numérico de su sistema de cerraduras.

Las **actualizaciones remotas del firmware** pueden realizarse a través de una conexión de red mediante la eBox. Este proceso se divide en tres etapas:

1. Un usuario de software inicia el proceso de actualización remota del firmware, enviando el firmware desde la API/software al sistema de bloqueo a través de la eBox.
2. El firmware se descarga y se almacena en el sistema de bloqueo. Aparecerá un mensaje en la pantalla del teclado numérico informando a los usuarios de las cerraduras de caja fuerte de que hay una actualización de firmware pendiente.
3. Un usuario de cerradura de caja fuerte deberá introducir sus credenciales válidas (ID de usuario y PIN) en el teclado numérico e iniciar la actualización del firmware.

Actualizaciones del firmware - Sistema de cerraduras CenconX

Las **actualizaciones locales del firmware** pueden realizarse estableciendo una conexión USB temporal entre el ordenador que aloja el software de la serie Apexx y el teclado numérico de su sistema de cerraduras.

Los usuarios móviles de CenconX también tienen la opción de realizar **actualizaciones del firmware móvil**, ya que la aplicación móvil Safe Locks de dormakaba se puede utilizar para recibir actualizaciones de firmware. El proceso consiste en utilizar el software de la serie Apexx para enviar los archivos de actualización del firmware al dispositivo móvil de un usuario. A continuación, el usuario móvil puede iniciar sesión en la aplicación Safe Locks, descargar los archivos necesarios e iniciar el proceso de actualización del firmware mediante una conexión BLE entre el dispositivo móvil y el teclado numérico CenconX.

Tránsito de datos

Figura 1 y el gráfico que lo acompaña muestran el flujo de datos entre los distintos componentes de hardware y software del sistema de cerraduras Axessor Apexx.

Puerto de comunicación	Descripción
443	Este puerto se utiliza para el tráfico TCP/IP saliente.
587	Este puerto se utiliza para comunicarse con el host SMTP. Es obligatorio y por defecto es 587.
5001	Este es el puerto por defecto utilizado para la puesta en marcha de un sistema de cerraduras Apexx.
8883	Este es el puerto por defecto utilizado por el bróker MQTT.

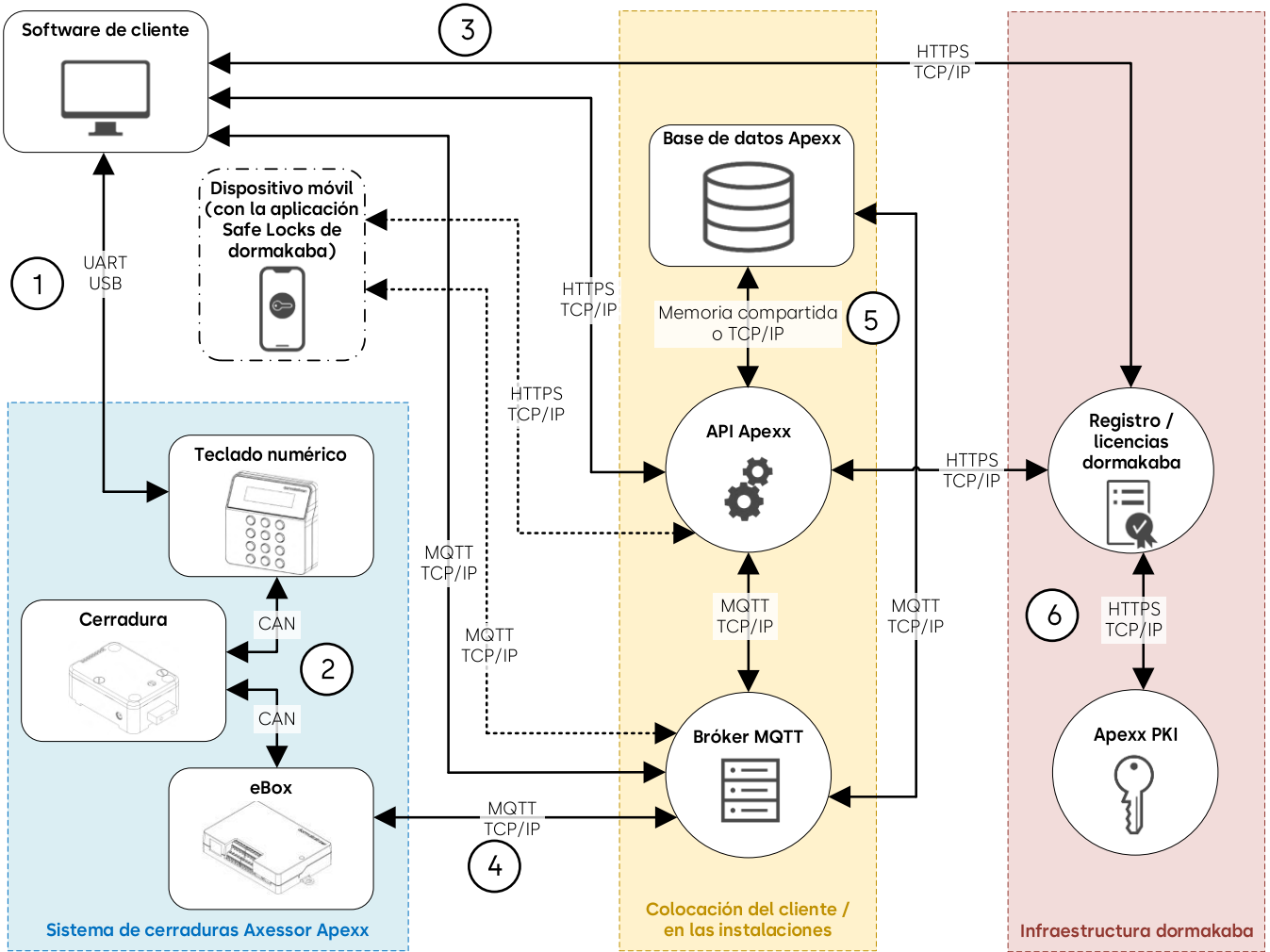


Figura 1 - Arquitectura del sistema Apexx con sistema de cerraduras Axessor Apexx - Componentes del sistema y tránsito de datos

	Protocolos de comunicación	Flujo de datos	Descripción / Finalidad
1	UART a USB	Ruta bidireccional: Software de cliente a teclado numérico	Configuración directa y recuperación de auditorías
2	CAN	Ruta bidireccional: - Teclado numérico a cerradura - Cerradura a eBox	Comunicación entre dispositivos
3	HTTPS a TCP/IP	Ruta bidireccional: Software de cliente a registro/licencias dormakaba	Licencias y registro en línea
4	MQTT a TCP/IP	Ruta bidireccional: - Software de cliente a bróker MQTT Ruta bidireccional: - eBox a bróker MQTT Ruta bidireccional: - Dispositivo con aplicación móvil Safe Locks de dormakaba a bróker MQTT	Configuración en red y recuperación de auditorías
5	Memoria compartida o TCP/IP	Ruta bidireccional: API Apexx a base de datos Apexx	Almacenamiento persistente de datos con SQL Server
6	HTTPS a TCP/IP	Ruta bidireccional: - Software de cliente a API Apexx - API Apexx a registros/licencias dormakaba - Registros/licencias dormakaba a PKI Apexx - Dispositivo con aplicación móvil Safe Locks de dormakaba a Apexx API	Emisión de certificados x.509

Figura 2 muestra un diagrama similar al esbozado en Figura 1, pero con un sistema de cerraduras CenconX en lugar del sistema de cerraduras Axessor Apexx. En este caso, el dispositivo móvil actúa como canal de comunicación entre el sistema de cerraduras CenconX y la infraestructura de software.

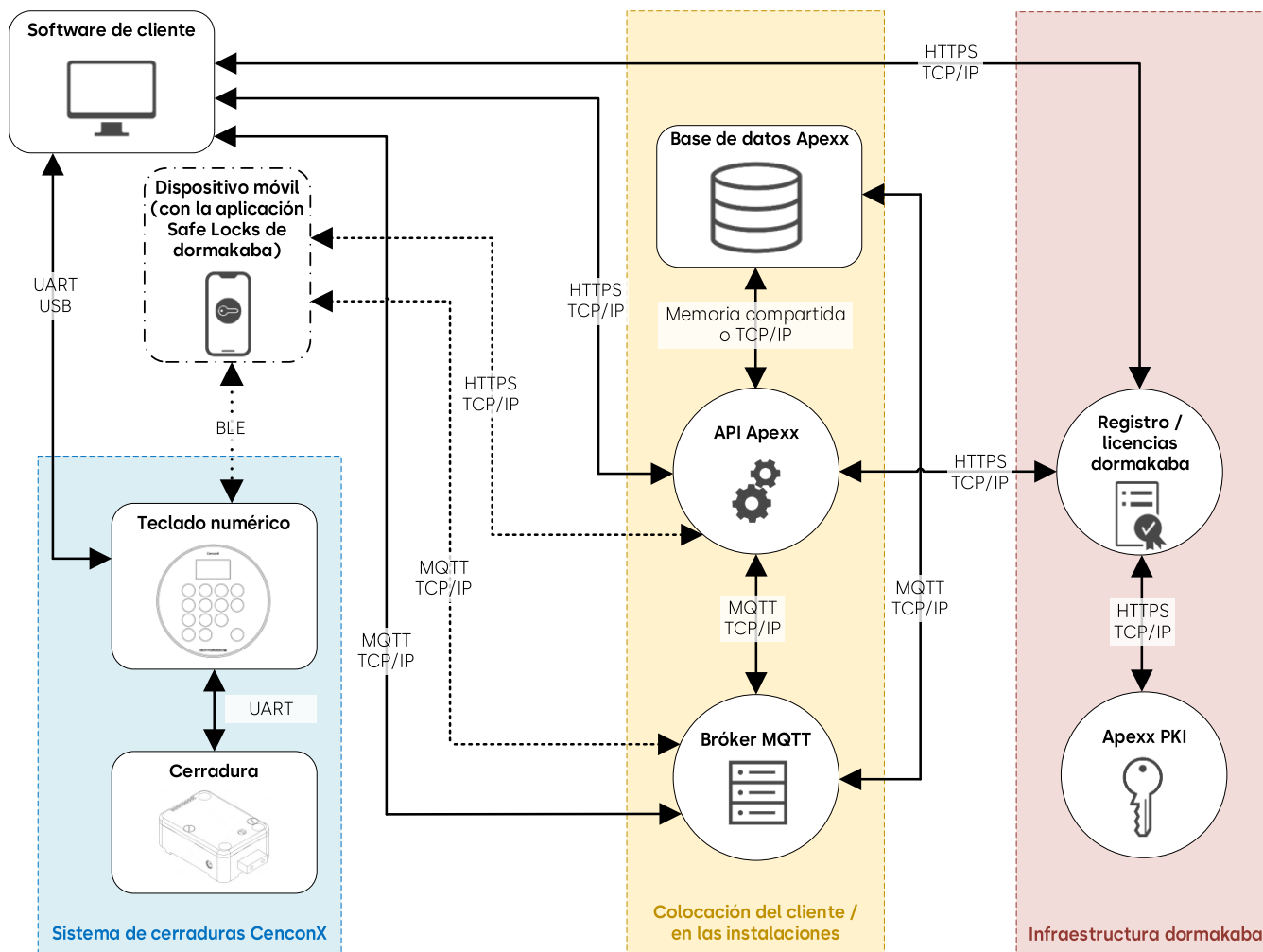


Figura 2 - Arquitectura del sistema Apexx con sistema de cerraduras CenconX - Componentes del sistema y tránsito de datos

Seguridad y cifrado de datos

El software de la serie Apexx, los sistemas de cerraduras CenconX, los sistemas de cerraduras Axessor Apexx y los dispositivos móviles puestos en marcha emplean múltiples métodos de cifrado, incluyendo AES256, PBKDF2 y certificados TLS para garantizar la seguridad de la comunicación y el almacenamiento de datos.

Infraestructura de clave pública (PKI)

El software de la serie Apexx, los sistemas de cerraduras CenconX, los sistemas de cerraduras Axessor Apexx y los dispositivos móviles puestos en marcha utilizan una infraestructura de clave pública para crear, almacenar y distribuir certificados digitales a los dispositivos Apexx a través de las autoridades de certificación.

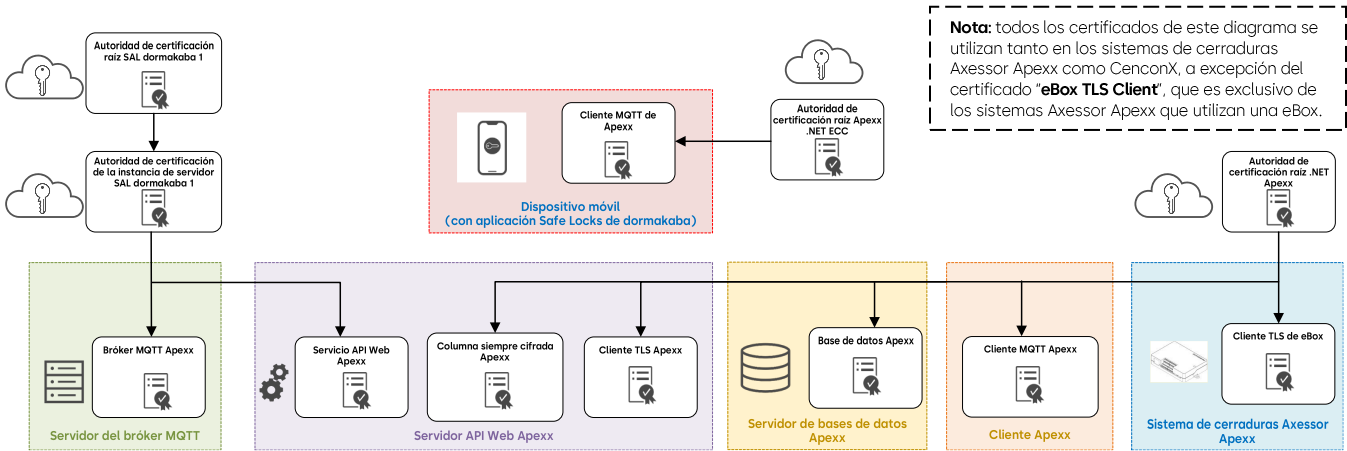


Figura 3 - Infraestructura de clave pública

Tipo de certificado	Descripción
Autoridad de certificación raíz SAL dormakaba	- Este certificado viene instalado de fábrica en los dispositivos y se sustituye mediante actualización del firmware - Durante la instalación del software de la serie Apexx, este certificado también se instala al ejecutar el archivo de instalación de requisitos previos en los equipos cliente y servidor (almacenado en la carpeta de autoridades de certificación raíz de confianza)
Autoridad de certificación de la instancia de servidor SAL dormakaba	- Los servidores que ejecutan servicios de software locales para Apexx necesitan certificados firmados por la PKI SAL de dormakaba para que los dispositivos confíen en ellos - Este certificado debe instalarse en todos los servidores que ejecuten servicios de software locales - Durante la instalación del software de la serie Apexx, este certificado también se instala al ejecutar el archivo de instalación de requisitos previos en los equipos cliente y servidor (almacenado en la carpeta de autoridades de certificación intermedias)
Bróker MQTT Apexx	- Se crea durante la instalación del software - Se utiliza para conexiones TLS y autenticación
Servicio API Web Apexx	- Se crea durante la instalación del software - Contiene el nombre del servidor (ordenador en el que está instalado este servicio), la autoridad de certificación de confianza y la clave de cifrado pública del servidor
Cliente TLS Apexx	- Se utiliza para la autenticación del cliente Apexx - El certificado es un usuario verificado si el emisor coincide con la autoridad de certificación raíz Apexx. NET instalada en el servidor bróker
Base de datos Apexx	- SQL Server en Windows es el único motor de base de datos compatible - Los siguientes ajustes están activados en la instancia/base de datos: - Autenticación de Windows - El control de acceso basado en roles (RBAC) se utiliza junto con la autenticación de Windows para controlar los permisos
Cliente TLS de eBox	- Se utiliza para la autenticación de la eBox - El certificado es un usuario verificado si el emisor coincide con la autoridad de certificación raíz Apexx. NET instalada en el servidor bróker

Tipo de certificado	Descripción
Autoridad de certificación raíz .NET Apexx	- Se crea durante la instalación del software y se almacena en el almacén de certificados del equipo local, en la carpeta de autoridades de certificación raíz de confianza - Durante el proceso de instalación de la API, se almacena en la carpeta de certificados personales del equipo local (LM\Personal\Certificates) - Cualquier ordenador que ejecute el software (cliente, servidor, base de datos, etc.) necesita una copia de este certificado por motivos de seguridad/identificación - La PKI del software local firma las solicitudes de certificados para todos los clientes del bróker MQTT - Estos certificados se utilizan tanto para establecer conexiones TLS (Transport Layer Security) de confianza mutua como para la autenticación con el bróker MQTT - También puede firmar los certificados utilizados por SQL Server para TLS - Utiliza RSA para las firmas
Autoridad de certificación raíz Apexx .NET ECC	- Se crea durante la instalación del software y se almacena en el almacén de certificados del equipo local, en la carpeta de autoridades de certificación raíz de confianza - Durante el proceso de instalación de la API, se almacena en la carpeta de certificados personales del equipo local (LM\Personal\Certificates) - Cualquier ordenador que ejecute el software (cliente, servidor, base de datos, etc.) necesita una copia de este certificado por motivos de seguridad/identificación - La PKI del software local firma las solicitudes de certificados para todos los clientes del bróker MQTT - Estos certificados se utilizan tanto para establecer conexiones TLS (Transport Layer Security) de confianza mutua como para la autenticación con el bróker MQTT - También puede firmar los certificados utilizados por SQL Server para TLS - Utiliza ECDSA para las firmas
Cliente MQTT de Apexx	- Creado durante el inicio de sesión del cliente de software - Se utiliza para conexiones TLS y autenticación
Columna siempre cifrada Apexx	- Cifrado de datos en la API que va a la columna cifrada en la base de datos - Durante el proceso de instalación de la API, se almacena en la carpeta de certificados personales del equipo local (LM\Personal\Certificates)

Nota: los certificados pueden renovarse 60 días antes de su caducidad renovando la licencia mediante la herramienta de registro en línea del software de la serie Apexx.

Configuraciones del hardware informático

La parte de hardware/API/software del sistema Apexx puede configurarse de varias maneras dependiendo de la complejidad de su sistema (número de sistemas de bloqueo Apexx, sus ubicaciones, etc.). En esta sección se describen solo algunas de las configuraciones posibles. Consulte el catálogo de precios de Axessor Apexx o CenconX para obtener más información sobre los requisitos de licencia para las distintas configuraciones de ordenador/hardware.

Nota: si lo desea, cualquiera de los componentes de software (cliente, base de datos, API o MQTT) puede alojarse en una máquina virtual.

Configuración para un solo ordenador (conexión USB)

Figura 4 ilustra una configuración básica con un solo ordenador y un sistema de bloqueo Axessor Apexx y/o un sistema de bloqueo CenconX. En esta configuración, todos los elementos de la API/software se alojan en un único ordenador y se utiliza una conexión USB para conectarse temporalmente al sistema de bloqueo Axessor Apexx o CenconX con fines de programación/configuración del sistema.

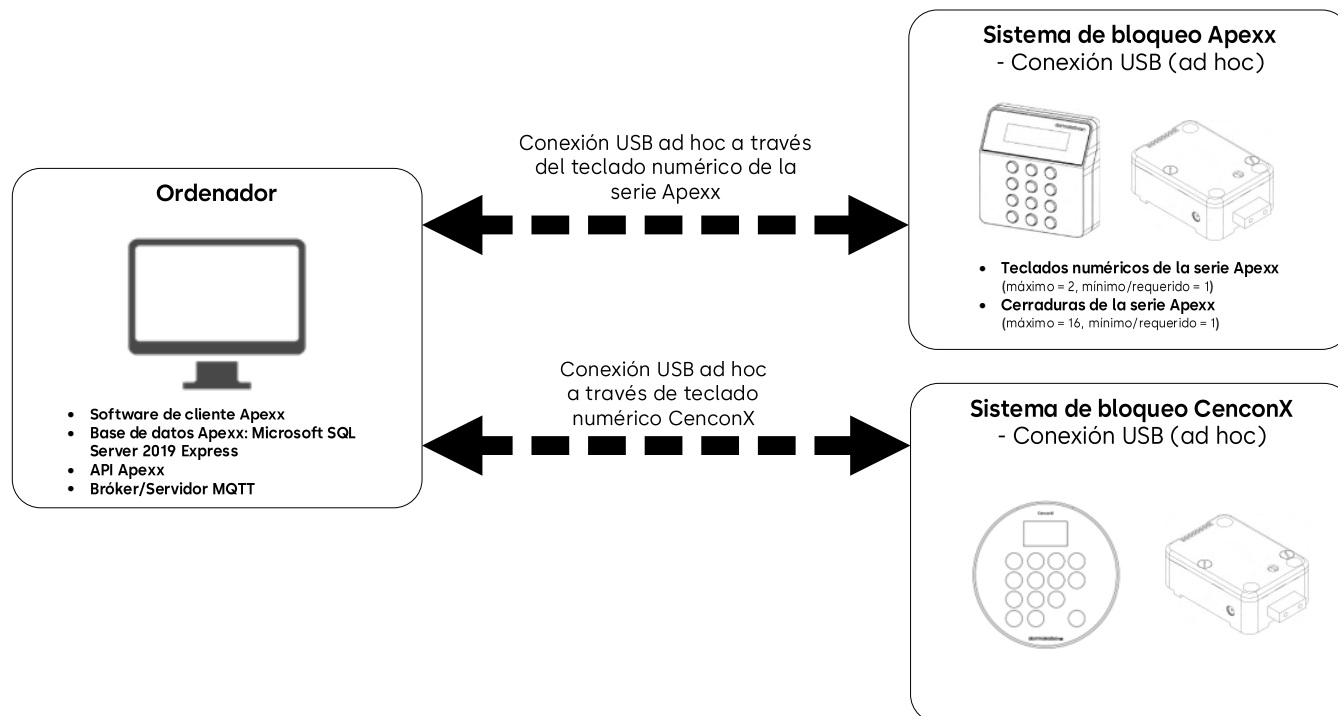


Figura 4 - Configuración de un solo ordenador - Conexión USB ad hoc

Sistemas de cerraduras Axessor Apexx - Conexión USB

En el caso de Axessor Apexx, este tipo de configuración funciona bien en lugares pequeños en los que el ordenador y todos los componentes del sistema de bloqueo (teclados numéricos y cerraduras) se encuentran en la misma ubicación física, pero carece de la versatilidad y comodidad que ofrecen las configuraciones en red que utilizan la eBox de Apexx.

Sistemas de cerraduras CenconX - Conexión USB

En el caso de CenconX, no se recomiendan las conexiones solo USB para sistemas CenconX que utilicen la funcionalidad OTC.

Configuración de un solo ordenador (TCP/IP)

Figura 5 muestra otra configuración sencilla en la que solo intervienen un ordenador y un sistema de bloqueo Axessor Apexx y/o un sistema de bloqueo CenconX.

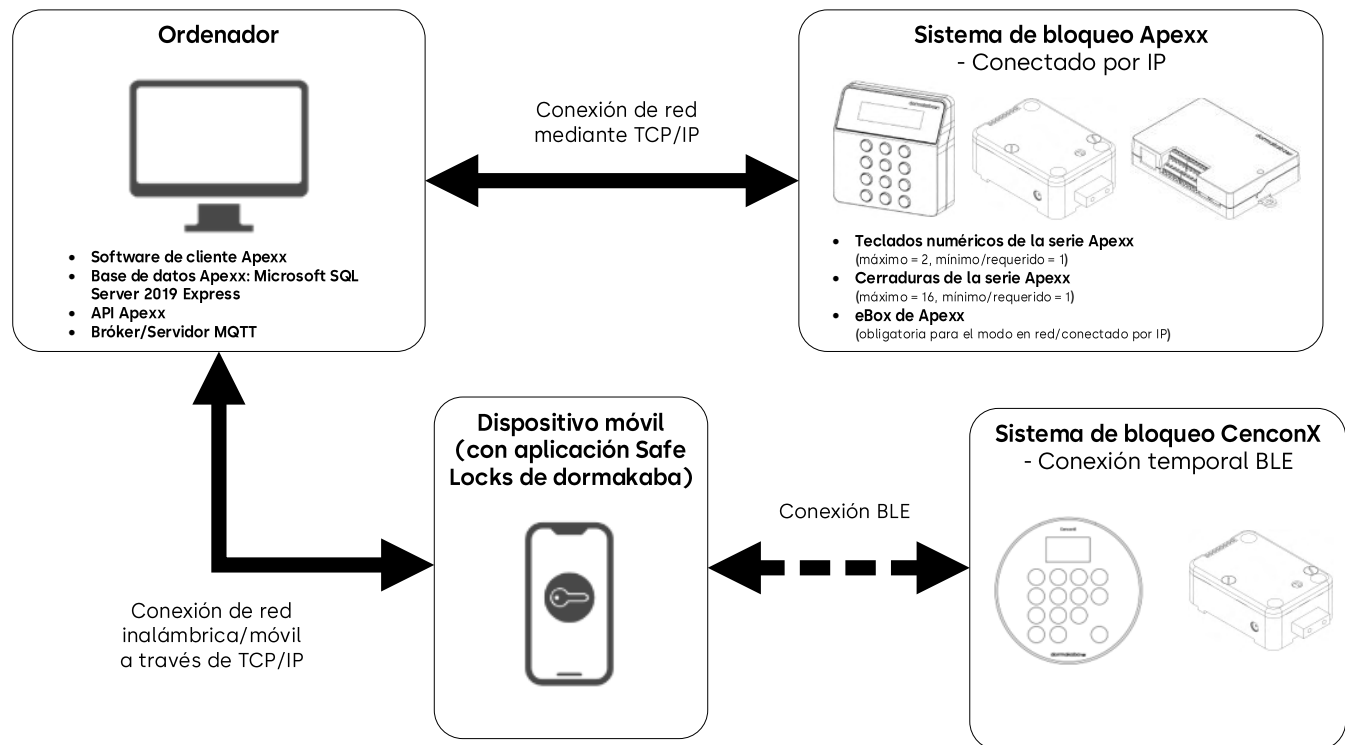


Figura 5 - Configuración de un solo ordenador - Red a través de eBox (TCP/IP) y móvil

Sistemas de cerraduras Axessor Apexx - Configuración de un solo ordenador (TCP/IP)

La eBox de Apexx se utiliza para proporcionar una conexión de red/IP para la comunicación continua/en directo entre el ordenador y el sistema de bloqueo Axessor Apexx.

En el caso de los sistemas de bloqueo Axessor Apexx, esta configuración también es útil para configuraciones más pequeñas en las que todo el equipo se encuentra en la misma ubicación física, pero la inclusión de la eBox permite al administrador del sistema aprovechar todas las funciones que proporciona una conexión IP activa (auditorías en directo, supervisión activa del sistema, actualizaciones remotas de firmware y otras funciones adicionales de hardware/software).

Sistemas de cerraduras CenconX - Configuración de un solo ordenador (TCP/IP)

En el caso del sistema de bloqueo CenconX, el dispositivo móvil se conecta al servidor/cliente del ordenador a través de una conexión de red/IP, y una conexión "puente" BLE temporal conecta el dispositivo móvil al sistema de bloqueo CenconX.

Configuraciones de varios ordenadores

Para instalaciones de mayor tamaño, con edificios más grandes y/o varios sistemas de bloqueo, la configuración de varios ordenadores que se muestra en Figura 6 ofrece una flexibilidad adicional.

Nota: solo se permite una API, un bróker MQTT y una base de datos SQL Server en el sistema.

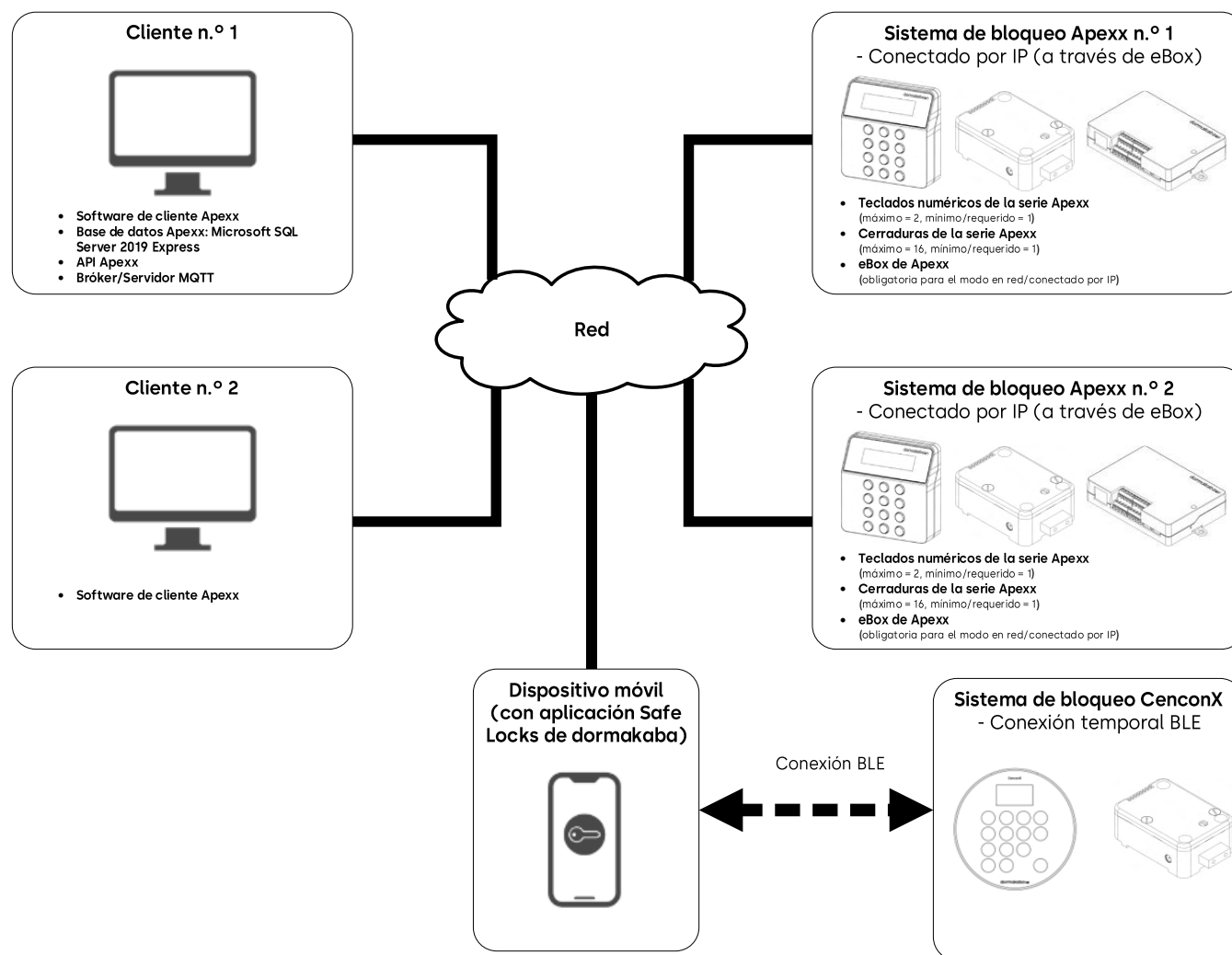


Figura 6 - Configuración de varios ordenadores con varios sistemas de bloqueo

En una configuración de este tipo, cualquiera o todos los componentes de software podrían instalarse en uno o más ordenadores (o máquinas virtuales), lo que permite una mayor comodidad y flexibilidad a la hora de ejecutar y configurar sus sistemas de bloqueo. Tenga en cuenta que cada sistema de bloqueo Axessor Apexx se conecta a la red a través de una eBox de Apexx.

Este concepto se amplía aún más en el sistema que se muestra en Figura 7, que incluye varios ordenadores y sistemas de cerraduras repartidos por varios edificios.

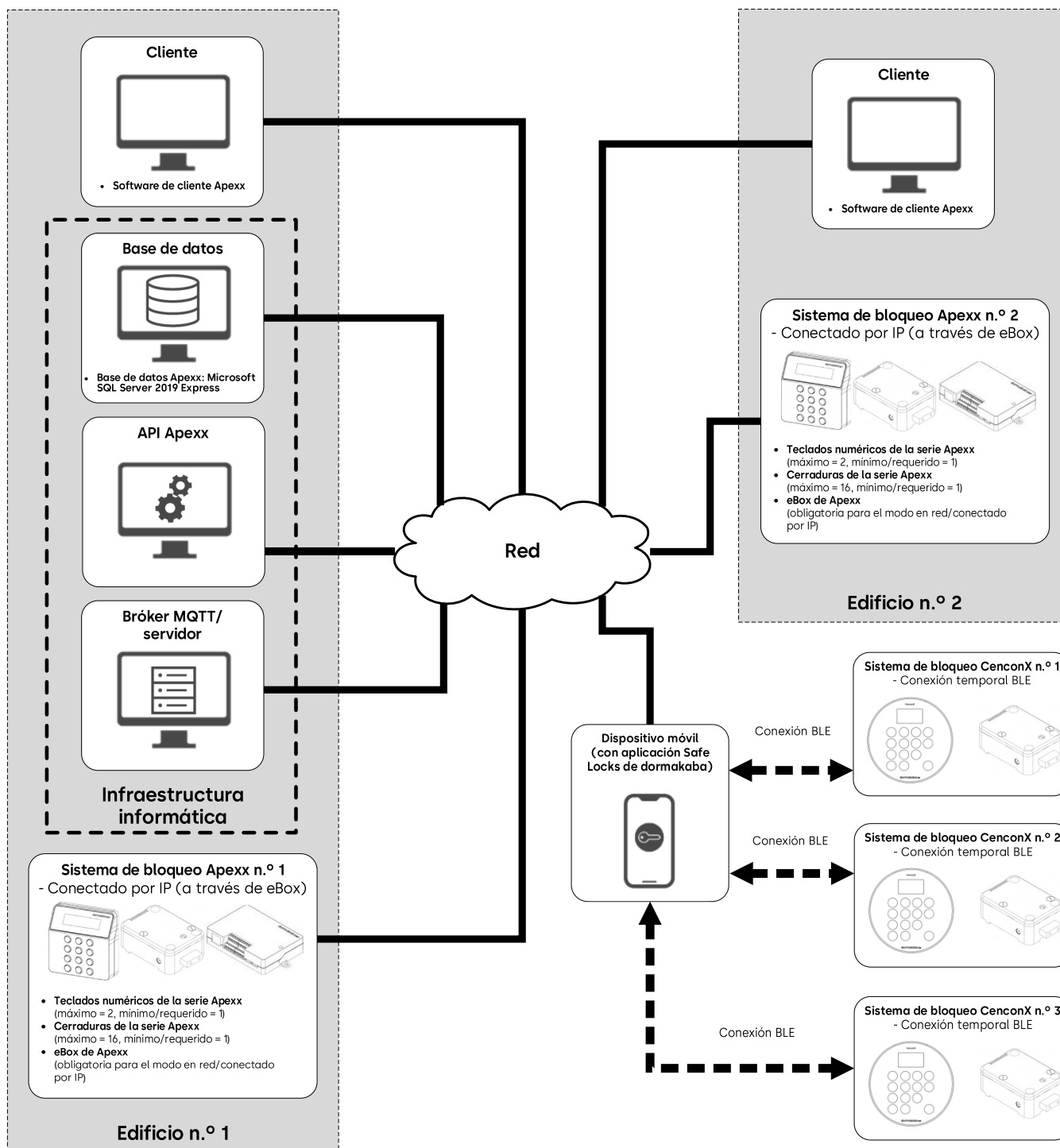


Figura 7 - Configuración de varios ordenadores/sistemas de bloqueo con configuración multiservidor

Una diferencia notable entre esta configuración y todas las demás es que incluye varios ordenadores que alojan distintos componentes de software. En este ejemplo, dos de los ordenadores del edificio n.º 1 alojan la API Apexx y la base de datos Apexx respectivamente. Estos dos ordenadores pueden configurarse para el uso como API y base de datos para los sistemas de bloqueo en el edificio n.º 1, el edificio n.º 2 y/o cualquier otro sistema de cerraduras en toda la red.

Este último ejemplo ilustra que son posibles muchas configuraciones diferentes en función de las necesidades de su organización y de la configuración de su infraestructura informática.

Consideraciones sobre la base de datos

El software de la serie Apexx incluye Microsoft SQL Server 2019 Express como motor exclusivo de la base de datos interna.

	Microsoft SQL Server 2019 Express (64 bits)
Límite de la base de datos	10 GB
Número de CPU	1 procesador físico
RAM	1 GB
Sistemas operativos compatibles	Windows 10, Windows Server 2016, Windows Server 2019

Especificaciones mínimas del ordenador recomendadas para Apexx

*Considere la posibilidad de duplicar para instalaciones más grandes

Estación de trabajo del cliente Apexx

- Procesador de 2,0 GHz con 4 núcleos*
- 16 GB DE RAM
- Disco duro de 500 GB
- Windows 10 Professional (64 bits)

Servidor del bróker Apexx

- Procesador de 2,0 GHz con 4 núcleos*
- 16 GB DE RAM
- Disco duro de 500 GB
- Windows 2019 Server Standard (64 bits)

Servidor de base de datos Apexx y API Apexx

- Procesador de 2,0 GHz con 6 núcleos*
- 32 GB DE RAM*
- Disco duro de 1 TB
- Windows 2019 Server Standard (64 bits)
- Microsoft SQL Server Standard o Enterprise

Nota: si lo desea, cualquiera de los componentes de software (cliente, base de datos, API o bróker MQTT) puede alojarse en una máquina virtual.

Especificaciones del dispositivo móvil Apexx

(A fecha de publicación del documento)

- Sistema operativo móvil: Android 8+ o iOS 15+
- Debe ser compatible con BLE

Nota: consulte en Google Play y Apple Store las últimas versiones de la aplicación móvil Safe Locks de dormakaba y la información sobre compatibilidad de dispositivos/sistemas operativos.

Guía de seguridad informática de Apexx

Notas sobre el software local

- Todas las partes del software (MQTT, cliente y API) están diseñadas como aplicaciones Windows. Para poder utilizarlas en un entorno de nube, hay que saber cómo gestionar los canales de comunicación entre ellos.
- Los canales de comunicación se establecen durante la instalación: se basan en DNS (o direcciones IP estáticas). Una vez finalizada la instalación, se establecerán certificados a efectos de seguridad. Estos certificados deben gestionarse adecuadamente para evitar cualquier vía de ataque.
- La comunicación hacia y desde el sistema de bloqueo es MQTT sobre SSL, por lo que los puertos estándar deben estar accesibles.
- El software requiere el subsistema de certificados de Windows y una base de datos SQL19 para funcionar.
- El software no es compatible con sistemas Mac o Linux.
- Los entornos de nube probados son Azure y AWS.
- Un mismo usuario no puede iniciar sesión en varios clientes al mismo tiempo.

Emparejamiento del software local con eBox (Axessor Apexx)

El software local y la eBox de Apexx deben emparejarse antes de poder establecer una conexión. Si hay que instalar una eBox totalmente nueva:

1. La eBox se instala físicamente en el bus CAN.
2. Un usuario autorizado debe iniciar sesión en el teclado numérico y poner en servicio la eBox en el bus CAN (ningún dispositivo no autorizado puede escuchar el bus CAN).
3. Tras la puesta en marcha de la eBox, esta podrá obtener las claves de cifrado del bus CAN (AES-256 con claves específicas del sistema).
4. Una vez que la eBox está en el bus CAN, hay que conectarla al software local. La dirección IP se puede ver y cambiar en los ajustes de red del menú avanzado del teclado numérico. Si la configuración existe, se utilizará. De lo contrario, la eBox utilizará DHCP para obtener la dirección IP.
5. Cuando haya una configuración Ethernet válida, la eBox intentará conectarse al servidor MQTT en el software local (ya sea a través de comunicación IP directa basada en la configuración, o difusión en la red local en caso de DHCP). Esto se hace a través del TLS.
6. Si el software local detecta una nueva eBox, esta debe autorizarse en el software antes de iniciar sesión utilizando el código de validación. Una vez autorizada la eBox en el software, este producirá un PIN de verificación que debe validarse en el teclado numérico (verificación del software a la eBox, y de la eBox al software).

7. Una vez verificado el sistema, se establecerá un canal seguro. Para ello, se utilizan certificados firmados de fábrica que han sido preinstalados (infraestructura PKI). Cualquier comunicación posterior se cifrará mediante TLS.
8. TLS 1.2. eBox también se comunica inicialmente a través del puerto TCP 5001 (API) para verificar que el software está activado y, a continuación, a través del puerto 8883 (predeterminado) para la comunicación.
9. El software debe estar activado y tener los certificados adecuados para que la eBox se active correctamente. El software desactivado provocará una denegación de servicio.

Para obtener más información sobre la instalación, conexión y configuración de la eBox de Apexx, consulte la Guía de instalación de Axessor Apexx (Documento n.º 801.0622), la Guía del usuario del sistema de teclado numérico de la serie Apexx (Documento n.º 802.0622) y el menú de ayuda del software de la serie Apexx.

Recuperación en caso de catástrofe

El software local se conecta a la base de datos SQL19 para el almacenamiento de datos (SQL19 Express de Microsoft - Referencia: <https://www.microsoft.com/en-ca/sql-server/sql-server-2019-pricing>).

La configuración de la base de datos debe introducirse en el software local en forma de un archivo de configuración. El cifrado/protección y la recuperación de datos seguirán entonces la ruta de la base de datos SQL19. La base de datos debe ser gestionada por el departamento local de IT.

La ruta de recuperación será volver a instalar la API, el MQTT y el cliente, ya sea con una copia nueva de dormakaba o con una copia de seguridad local. Todos los datos se almacenan en la base de datos SQL. API, MQTT y el cliente no almacenan ningún dato de cerradura o de usuario, solo los ajustes de conexión y configuración.

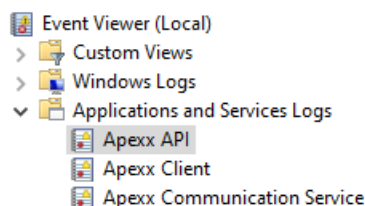
El servicio API crea automáticamente la base de datos por primera vez. La base de datos utiliza inicios de sesión específicos del servicio NT por defecto (API o BROKER) y se autentica a través de canales Kerberos. La configuración por defecto de la base de datos es Autenticación de Windows, Columnas cifradas. Recomendamos, pero no exigimos, el cifrado a nivel de motor.

Visualización y exportación de registros de eventos de Apexx



Se puede utilizar el “Visor de Eventos” de Windows para ayudar a ver y solucionar problemas relacionados con las aplicaciones y servicios de Apexx.

1. Abrir el visor de eventos > escriba “**Visor de eventos**” en la barra de búsqueda de Windows y, a continuación, abra el programa.
2. Haga clic en la flecha situada junto a > 📁 “**Registros de aplicaciones y servicios**” para ampliar la lista.
3. Haga clic en la aplicación/servicio Apexx para ver todos los eventos relacionados con esa aplicación o servicio (Apexx API, Apexx Client, Apexx Communication Service).



4. Desde aquí puede ordenar los eventos por hora, por identificador de evento, etc., para ayudar en la visualización y solución de problemas con su configuración Apexx.
5. Exportar registros de eventos de Apexx > En "**Acciones**" puede elegir  "**Guardar todos los eventos como...**" para exportar los registros de eventos de la aplicación/servicio seleccionado y guardarlos en uno de varios formatos (.evtx, .xml, .txt, .csv).

Principales conclusiones

1. Solo los servidores con software local deben ser direccionables por IP; la eBox no.
2. La comunicación entre la eBox y el software local (tráfico a través de intranet/Internet) se cifra mediante TLS.
3. Incluya el servidor SQL en su plan de recuperación en caso de desastres. Esta base de datos es crucial para el funcionamiento del sistema.



Access Automation Solutions

Entrance Automation
Entrance Security



Access Control Solutions

Electronic Access & Data
Escape and Rescue Systems
Lodging Systems



Access Hardware Solutions

Door Closers
Architectural Hardware
Mechanical Key Systems



Services

Technical Support
Installation and commissioning
Maintenance and Repair



Key & Wall Solutions

Key Systems
Movable / Sliding Walls



Safe Locks

Electronic Safe Locks
Mechanical Safe Locks
Boltworks and Accessories



Glass systems

Manual door systems
Glass fittings
Horizontal Sliding Walls

Nuestro compromiso con la sostenibilidad

Nos comprometemos a fomentar el desarrollo sostenible a lo largo de toda nuestra cadena de valor, en consonancia con nuestras responsabilidades económicas, ambientales y sociales hacia las generaciones actuales y futuras. La sostenibilidad a nivel de producto es un enfoque importante y orientado al futuro en el sector de la construcción. Para proporcionar información cuantificada sobre el impacto ambiental de un producto a lo largo de su ciclo de vida, dormakaba proporciona Declaraciones Ambientales de Producto (DAP), basadas en evaluaciones holísticas del ciclo de vida.

<https://www.dormakabagroup.com/en/sustainability/product-declarations>.

Guía de arquitectura del sistema y seguridad informática de
Axessor Apexx - Rev. B
Sujeto a cambios sin previo aviso

Dormakaba SAL GmbH

Siemensstrasse 33
42551 Velbert
safelocks.de@dormakaba.com
T +49 2051 9111 0

dormakaba USA Inc.

1525 Bull Lea Road, Suite 100
Lexington, KY 460511
sales.safelocks.us@dormakaba.com
1-800-950-4744



AXESSOR APEXX IP
INSTALLATION AND
OPERATION GUIDES

dk.world/AxessorApexxIP

Logiciels de la série Axessor Apexx

Guide d'architecture système et de sécurité informatique pour
Axessor Apexx IP/CIT et CenconX



Table des matières

Architecture du système Apexx.....	3
Présentation	3
Système de serrures Axessor Apexx	3
Système de serrures CenconX.....	3
Appareils mobiles	4
API/Composants logiciels	4
API Apexx.....	4
Logiciel client Apexx	4
Base de données Apexx.....	4
Broker/serveur MQTT.....	5
SMTP	5
SSO.....	5
Configuration des utilisateurs - Axessor Apexx.....	5
Configuration des utilisateurs - CenconX	6
Configuration des utilisateurs - Utilisateurs du logiciel	6
Utilisateurs du logiciel - Axessor Apexx	6
Utilisateurs du logiciel - CenconX.....	6
Licences.....	7
Méthodes de mise à jour du firmware.....	7
Mises à jour du firmware - Système de serrures Axessor Apexx	7
Mises à jour du firmware - Système de serrures CenconX.....	7
Transit de données	8
Sécurité et chiffrement des données	10
Infrastructure à clé publique (PKI).....	11

Configurations du matériel informatique.....	13
Configuration d'un seul ordinateur (connexion USB).....	13
Configuration d'un seul ordinateur (TCP/IP).....	14
Configurations de plusieurs ordinateurs	15
Points à prendre en considération concernant la base de données.....	17
Spécifications minimales de l'ordinateur recommandées pour Apexx.....	17
Spécifications de l'appareil mobile Apexx.....	17
Guide de sécurité informatique Apexx	18
Remarques sur le logiciel local	18
Appairage d'un logiciel local avec une eBox (Axessor Apexx).....	18
Récupération après sinistre	19
Visualisation et exportation des journaux d'événements Apexx	19
Principaux enseignements.....	20

Architecture du système Apexx

Présentation

Le **logiciel de la série Apexx** permet de gérer et de configurer à distance divers aspects des systèmes de serrures Axessor Apexx et CenconX. Ce document explique l'architecture du système, l'infrastructure informatique et les exigences relatives à l'utilisation du logiciel de la série Apexx pour prendre en charge et gérer les systèmes de serrures Axessor Apexx et CenconX.

Système de serrures Axessor Apexx

Les systèmes de verrouillage Axessor Apexx se composent de deux réseaux de communication sécurisés : Le **bus Can du système de serrures** et le **réseau API/logiciel**

Le **bus CAN du système de serrures** prend en charge les composants suivants :

- **Claviers de la série Apexx** (maximum = 2, minimum/requis = 1)
 - Utilisés comme interface utilisateur pour l'accès au système de serrures et sa configuration
- **Serrures de la série Apexx** (maximum = 16, minimum/requis = 1)
 - Serrure physique électromécanique qui contrôle l'accès de l'utilisateur au coffre-fort
- **eBox Apexx** (requis pour le mode réseau/connexion IP)
 - Fonctionne comme un convertisseur de protocole (IP vers bus CAN) entre le système de serrures Axessor Apexx et l'API/le logiciel
 - Fonctionne également comme un boîtier E/S (entrée/sortie)

Système de serrures CenconX

Les systèmes de verrouillage CenconX se composent de deux réseaux de communication sécurisés : Le **système de serrures** et le **réseau API/logiciel**

Le **système de serrures** prend en charge les composants suivants :

- **Claviers de la série CenconX** (1)
 - Utilisés comme interface utilisateur pour l'accès au système de serrures et sa configuration
- **Serrures de la série CenconX** (1)
 - Serrure physique électromécanique qui contrôle l'accès de l'utilisateur au coffre-fort

Appareils mobiles

L'application mobile Safe Locks de dormakaba peut être utilisée comme interface avec les systèmes de serrures Axessor Apexx et CenconX. Vous pouvez la télécharger gratuitement sur Google Play et l'Apple Store, mais elle ne sera fonctionnelle qu'à partir du moment où elle aura été enregistrée à l'aide du logiciel de la série Apexx. Pour en savoir plus sur l'utilisation de l'application mobile et sur l'enregistrement d'un appareil mobile, reportez-vous au Guide d'utilisation du système CenconX (document n° CX003.0524) et au menu d'aide du logiciel de la série Apexx.

- **Systèmes de serrures Axessor Apexx** > Les dispositifs Axessor Apexx dotés de la version 2.1.x.x ou supérieure du firmware peuvent intégrer des appareils mobiles via **l'application mobile Safe Locks** de dormakaba.
- **Systèmes de serrures CenconX** > **L'application mobile Safe Locks** de dormakaba sert de pont entre le système de serrures CenconX et l'API/le logiciel, et permet d'authentifier et d'ouvrir les serrures CenconX.

API/Composants logiciels

L'API/le logiciel se compose de quatre éléments principaux :

- API Apexx
- Logiciel client Apexx
- Base de données Apexx - Microsoft SQL Server 2019 Express
- Broker/serveur MQTT

Remarque : le serveur/client Apexx doit être configuré à l'aide d'une adresse IP accessible au public afin de faciliter la communication avec les appareils mobiles.

API Apexx

L'interface de programmation d'application, ou API, joue le rôle d'éditeur et d'abonné dans l'architecture MQTT.

Logiciel client Apexx

Le logiciel client Apexx (« logiciel de la série Apexx ») est une interface utilisateur graphique (GUI) qui permet à ses utilisateurs de se servir de l'API pour effectuer des actions dans le système Apexx/CenconX (modifier les paramètres du système, stocker/récupérer des données, etc.)

Le logiciel client Apexx prend en charge plusieurs utilisateurs, mais pas de façon simultanée chez un seul client. Une seule personne peut être connectée à une instance client à la fois.

Base de données Apexx

La base de données Apexx sert d'emplacement principal pour le stockage des données dans le système Apexx. La base de données Apexx utilise le système de gestion de base de données relationnelle propriétaire de Microsoft, Microsoft SQL Server 2019 Express, comme moyen de stockage et d'extraction des données du système.

Broker/serveur MQTT

Message Queuing Telemetry Transport, ou MQTT, est un protocole de messagerie qui utilise un modèle de publication et d'abonnement pour faciliter la communication entre les appareils. Le broker/serveur MQTT agit comme un centre de messagerie centralisé et utilise le protocole MQTT pour gérer la communication entre les appareils. Plus précisément, MQTT transmet des messages entre le logiciel client Windows et l'eBox.

SMTP

Le logiciel de la série Apexx utilise le protocole de communication SMTP (Simple Mail Transport Protocol) pour envoyer les éléments suivants : Alertes actives, rapports programmés et informations sur la configuration des appareils mobiles.

- Les alertes actives sont envoyées aux destinataires en fonction de l'occurrence d'un ou de plusieurs événement(s) d'audit sélectionné(s) par l'utilisateur du logiciel.
- Les rapports programmés peuvent être envoyés par courrier électronique aux destinataires selon un calendrier défini par l'utilisateur, également via le protocole SMTP.
- Lors de l'ajout d'un nouvel appareil mobile dans le logiciel de la série Apexx, vous pouvez utiliser le code QR généré pour la configuration de l'appareil mobile. Lorsque vous utilisez l'application mobile Safe Locks pour scanner le code QR, le système utilise le protocole SMTP pour envoyer les informations de configuration à l'appareil mobile.
- Consultez le menu d'aide du logiciel de la série Apexx pour en savoir plus sur la configuration des paramètres SMTP.

SSO

Le logiciel de la série Apexx utilise l'authentification unique, ce qui garantit qu'un utilisateur du logiciel peut se connecter à l'API à l'aide d'un seul ensemble d'identifiants.

Configuration des utilisateurs - Axessor Apexx

Les utilisateurs du système Axessor Apexx se répartissent en deux catégories distinctes : les **utilisateurs de serrures de coffre-fort** et les **utilisateurs du logiciel**.

Les **utilisateurs de serrures de coffre-fort** sont des utilisateurs qui se serviront du système de serrures Axessor Apexx (composé des claviers physiques, des serrures et de l'eBox), et disposeront d'identifiants et de rôles uniques avec des autorisations qui dictent leur accès au système de serrures.

Les utilisateurs de serrures de coffre-fort saisissent des identifiants numériques et des codes PIN pour accéder au système de serrures à l'aide du clavier de la série Apexx. Ce mode de fonctionnement est connu sous le nom de Mode Banque (ou Mode Statique).

Les trois types d'utilisateurs des serrures de coffre-fort par défaut (Administrateur, Gestionnaire et Utilisateur) constituent une hiérarchie d'utilisateurs ayant chacun des rôles et des privilèges prédéfinis dans le système de verrouillage. En plus de ces types d'utilisateurs, d'autres rôles d'utilisateurs des serrures de coffre-fort peuvent être créés à l'aide des outils d'administration du logiciel de la série Apexx, dont les autorisations sont définies par un utilisateur du logiciel. Ces rôles d'utilisateurs supplémentaires sont créés à partir des trois types d'utilisateurs initiaux, de façon à ce que les nouveaux types d'utilisateurs répondent aux besoins de personnalisation du client.

Les appareils Axessor Apexx dotés d'une version 2.1.x.x ou supérieure du firmware introduisent des types d'utilisateurs supplémentaires (un administrateur principal et un administrateur locataire), ainsi que deux modes utilisateurs supplémentaires (Mode OTC et Mode ICS) qui intègrent l'utilisation d'appareils mobiles pour accéder à la serrure. Consultez le Guide d'utilisation du système de clavier de la série Apexx (document n° 802.0622) pour en savoir plus sur les types d'utilisateurs de serrures de coffre-fort et les modes utilisateurs.

Configuration des utilisateurs - CenconX

Les utilisateurs du système Axessor Apexx se répartissent en deux catégories distinctes : les **utilisateurs de serrures de coffre-fort** et les **utilisateurs du logiciel**.

Les **utilisateurs de serrures de coffre-fort** sont des utilisateurs qui se servent du système de serrures CenconX (composé des claviers physiques, des serrures, etc.), et disposeront d'identifiants et de rôles uniques avec des autorisations qui définissent leur accès au système de serrures.

Les types d'utilisateurs de serrures de coffre-fort dans les systèmes CenconX comprennent les administrateurs, les gestionnaires, les utilisateurs de code PIN statique (Mode Banque) et les utilisateurs d'OTC (code à usage unique). Consultez le Guide d'utilisation du système CenconX (document n° CX003.0524) pour en savoir plus sur les types d'utilisateurs et leurs autorisations.

Configuration des utilisateurs - Utilisateurs du logiciel

Les **utilisateurs du logiciel** désignent les utilisateurs qui exécutent le logiciel de la série Apexx et utilisent les outils logiciels pour effectuer des tâches de gestion et d'administration. Contrairement aux utilisateurs de serrures de coffre-fort, les utilisateurs du logiciel n'accèdent pas directement au système de serrures physique (ouverture/fermeture des portes de coffre-fort), mais effectuent des tâches d'administration et de gestion par l'intermédiaire du logiciel (ajout d'utilisateurs de serrures, réinitialisation des mots de passe des utilisateurs de serrures).

Les utilisateurs du logiciel saisissent des identifiants pour accéder au logiciel de la série Apexx à l'aide de l'authentification unique (SSO). Les autres types d'authentification auxquels sont soumis les utilisateurs du logiciel de la série Apexx comprennent l'authentification Windows (à l'exception d'Entra ID), l'authentification de domaine Windows et Google OAuth 2.0.

Les utilisateurs du logiciel qui disposent d'une autorisation d'écriture peuvent ajouter de nouveaux utilisateurs du logiciel et configurer les autorisations de lecture et d'écriture.

Utilisateurs du logiciel - Axessor Apexx

Les types d'utilisateurs du logiciel dans les systèmes Axessor Apexx comprennent les administrateurs et les gestionnaires. Pour les applications de transport de fonds, les régulateurs et les utilisateurs en audit uniquement ont également un rôle à jouer (**remarque** : la version 2.1.x.x ou supérieure du firmware de l'appareil est requise).

Consultez le menu d'aide du logiciel de la série Apexx pour en savoir plus sur les types d'utilisateurs du logiciel et les autorisations.

Utilisateurs du logiciel - CenconX

Les types d'utilisateurs du logiciel dans les systèmes CenconX comprennent les administrateurs, les gestionnaires, les régulateurs et les utilisateurs en audit uniquement. Consultez le Guide d'utilisation du système CenconX (document n° CX003.0524) pour en savoir plus sur les types d'utilisateurs et leurs autorisations.

Lors de la configuration de votre système de serrures CenconX, vous avez la possibilité de configurer un seul client ou une seule base de données pour un seul propriétaire (régulateur principal), ou vous pouvez introduire un second client ou une seconde base de données pour permettre à un régulateur secondaire de disposer d'un contrôle partagé sur la gestion du système et son accès. Consultez le Guide d'utilisation du système CenconX pour en savoir plus (document n° CX003.0524).

Licences

Le logiciel de la série Apexx dispose de plusieurs types de licences, chacune d'entre elles permettant d'accéder à différentes fonctionnalités et caractéristiques du logiciel. Pour plus d'informations, consultez les Catalogues de prix Axessor Apexx IP et CenconX.

Méthodes de mise à jour du firmware

La procédure de mise à jour du firmware de votre appareil Axessor Apexx varie en fonction de la licence que vous avez achetée.

Pour en savoir plus sur le processus de mise à jour du firmware, consultez le Guide d'utilisation du système Axessor Apexx (document n° 802.0622), le Guide d'utilisation CenconX (document n° CX003.0524) et le menu d'aide du logiciel de la série Apexx.

Mises à jour du firmware - Système de serrures Axessor Apexx

Les **mises à jour du firmware local** peuvent être effectuées en établissant une connexion USB temporaire entre l'ordinateur hébergeant le logiciel de la série Apexx et le clavier de votre système de serrures.

Les **mises à jour à distance du firmware** peuvent se faire via une connexion réseau par l'intermédiaire de l'eBox. Il s'agit d'un processus en trois étapes :

1. Un utilisateur du logiciel lance le processus de mise à jour à distance du firmware, en envoyant le firmware de l'API ou du logiciel vers le système de verrouillage par l'intermédiaire de l'eBox.
2. Le firmware est téléchargé et stocké dans le système de verrouillage. Un message apparaît sur l'écran du clavier pour informer les utilisateurs de serrures de coffre-fort qu'une mise à jour du firmware est en attente.
3. Un utilisateur de serrures de coffre-fort saisit des identifiants valides (ID utilisateur et code PIN) au clavier, puis lance la mise à jour du firmware.

Mises à jour du firmware - Système de serrures CenconX

Les **mises à jour du firmware local** peuvent être effectuées en établissant une connexion USB temporaire entre l'ordinateur hébergeant le logiciel de la série Apexx et le clavier de votre système de serrures.

Les utilisateurs mobiles de CenconX ont également la possibilité d'effectuer des **mises à jour mobiles du firmware**, grâce à l'application mobile Safe Locks de dormakaba, qui permet de recevoir les mises à jour du firmware. Le processus consiste à utiliser le logiciel de la série Apexx afin de transférer les fichiers de mise à jour du firmware à l'appareil mobile de l'utilisateur. Ce dernier peut alors se connecter à l'application Safe Locks, télécharger les fichiers nécessaires, puis lancer le processus de mise à jour du firmware à l'aide d'une connexion BLE entre l'appareil mobile et le clavier CenconX.

Transit de données

La Figure 1 et le tableau qui l'accompagne montrent le flux de données entre les différents composants matériels et logiciels du système de serrures Axxor Apexx.

Port de communication	Description
443	Ce port est utilisé pour le trafic TCP/IP sortant.
587	Ce port est utilisé pour communiquer avec l'hôte du protocole SMTP. Il est obligatoire et sa valeur par défaut est 587.
5001	Il s'agit du port par défaut utilisé pour la mise en service d'un système de serrures Apexx.
8883	Il s'agit du port par défaut utilisé par le broker MQTT.

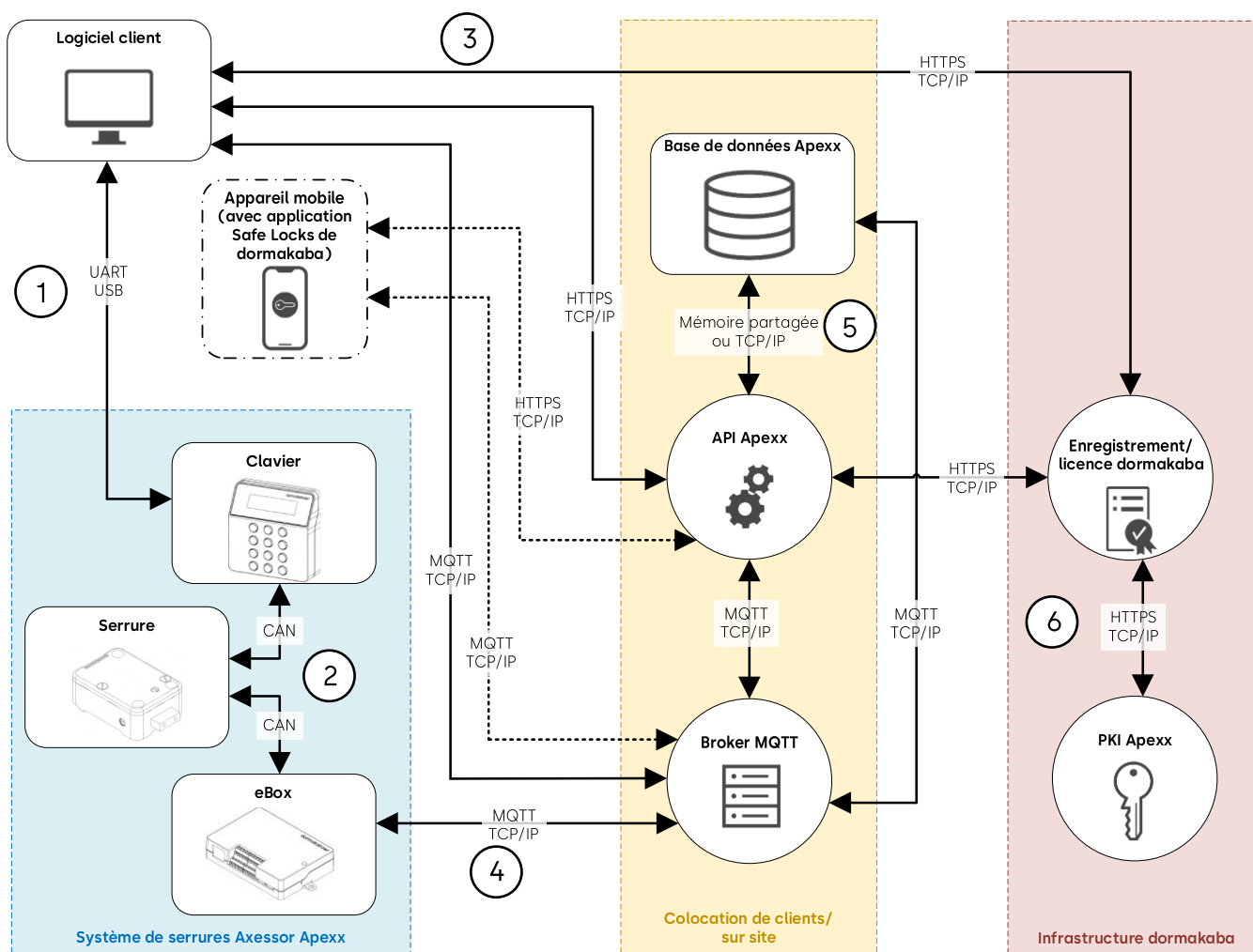


Figure 1 - Architecture du système Apexx avec le système de serrures Axxor Apexx - Composants du système et transit de données

	Protocoles de communication	Flux de données	Description/Objectif
1	UART sur USB	Chemin bidirectionnel : Logiciel client vers clavier	Configuration directe et récupération des audits
2	CAN	Chemin bidirectionnel : - Clavier vers serrure - Serrure vers eBox	Communication d'appareil à appareil
3	HTTPS sur TCP/IP	Chemin bidirectionnel : Logiciel client vers enregistrement/licence dormakaba	Licence et enregistrement en ligne
4	MQTT sur TCP/IP	Chemin bidirectionnel : - Logiciel client vers broker MQTT Chemin bidirectionnel : - eBox vers broker MQTT Chemin bidirectionnel : - Appareil avec application mobile Safe Locks de dormakaba vers le broker MQTT	Configuration en réseau et récupération des audits
5	Mémoire partagée ou TCP/IP	Chemin bidirectionnel : API Apexx vers base de données Apexx	Stockage de données persistantes avec SQL Server
6	HTTPS sur TCP/IP	Chemin bidirectionnel : - Logiciel client vers API Apexx - API Apexx vers enregistrement/licence dormakaba - Enregistrement/licence dormakaba vers PKI Apexx - Appareil avec application mobile Safe Locks de dormakaba vers API Apexx	Délivrance de certificats x.509

La Figure 2 montre un schéma similaire à celui présenté dans la Figure 1, mais avec le système de serrures CenconX au lieu du système Axessor Apexx. Dans ce cas, l'appareil mobile sert de canal de communication entre le système de serrures CenconX et l'infrastructure logicielle.

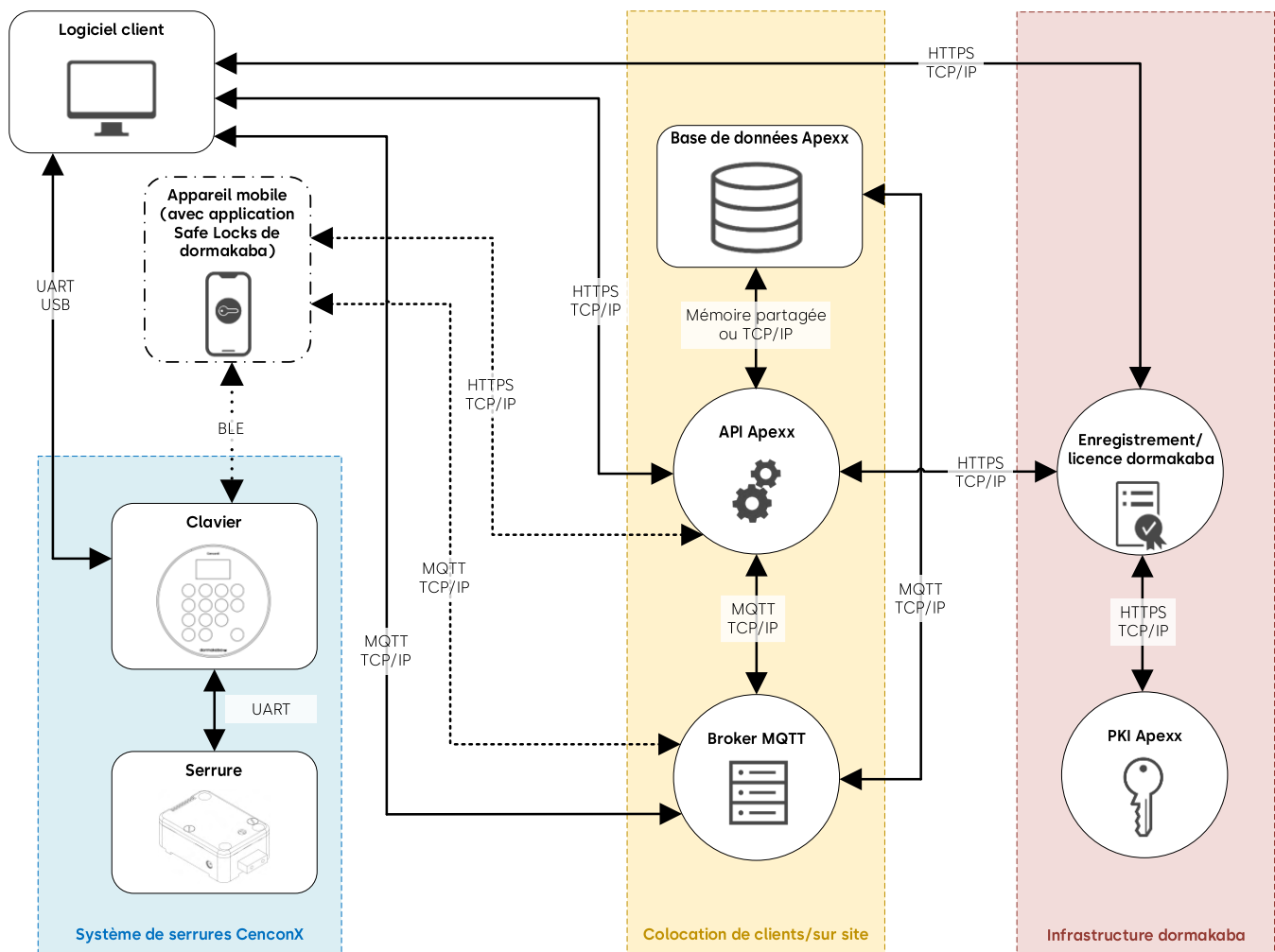


Figure 2 - Architecture du système Apexx avec le système de serrures CenconX - Composants du système et transit de données

Sécurité et chiffrement des données

Le logiciel de la série Apexx, les systèmes de serrures CenconX, les systèmes de serrures Axessor Apexx et les appareils mobiles mis en service utilisent plusieurs méthodes de chiffrement, notamment les certificats AES256, PBKDF2 et TLS, afin de garantir une communication et un stockage des données sûrs et sécurisés.

Infrastructure à clé publique (PKI)

Le logiciel de la série Apexx, les systèmes de serrures CenconX et Axessor Apexx et les appareils mobiles mis en service utilisent une infrastructure à clé publique pour créer, stocker et distribuer des certificats numériques aux appareils Apexx par l'intermédiaire des autorités de certification.

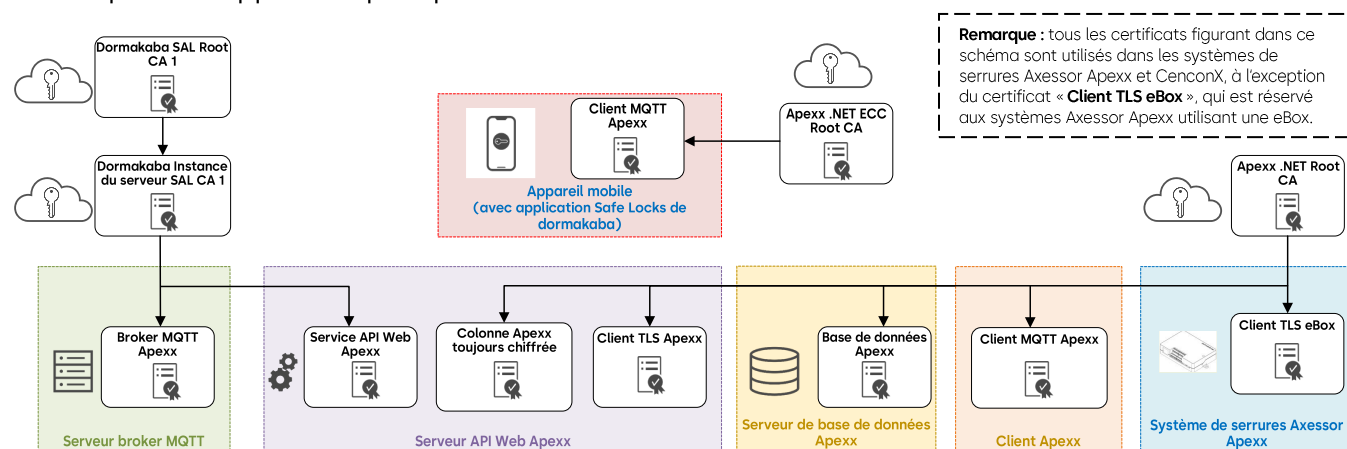


Figure 3 - Infrastructure à clé publique

Type de certificat	Description
Dormakaba SAL Root CA	- Ce certificat est préchargé sur les appareils en usine et remplacé en mettant à jour le firmware - Lors de l'installation du logiciel de la série Apexx, ce certificat est également installé lors de l'exécution du fichier Prerequisites Installer sur les machines client et serveur (stocké dans le dossier Trusted Root Certification Authorities)
Dormakaba Instance du serveur SAL CA	- Les serveurs qui exécutent des services logiciels locaux pour Apexx nécessitent des certificats signés par la PKI dormakaba SAL pour recevoir l'approbation des appareils - Ce certificat doit être déployé sur tous les serveurs qui exécutent des services logiciels locaux - Lors de l'installation du logiciel de la série Apexx, ce certificat est également installé lors de l'exécution du fichier Prerequisites Installer sur les machines client et serveur (stocké dans le dossier Intermediate Certification Authorities)
Broker MQTT Apexx	- Créé lors de l'installation du logiciel - Utilisé pour les connexions TLS et l'authentification
Service API Web Apexx	- Créé lors de l'installation du logiciel - Contient le nom du serveur (ordinateur sur lequel ce service est installé), l'autorité de certification approuvée et la clé de chiffrement publique du serveur
Client TLS Apexx	- Utilisé pour l'authentification du client Apexx - Le certificat est un utilisateur vérifié si l'émetteur correspond au .NET Root CA Apexx installé sur le serveur du broker
Base de données Apexx	- SQL Server sous Windows est le seul moteur de base de données pris en charge - Les paramètres suivants sont activés sur l'instance/la base de données : - Authentification Windows - Le contrôle d'accès basé sur les rôles (RBAC) est utilisé dans le cadre de l'authentification Windows pour contrôler les autorisations
Client TLS eBox	- Utilisé pour l'authentification de l'eBox - Le certificat est un utilisateur vérifié si l'émetteur correspond au .NET Root CA Apexx installé sur le serveur du broker

Type de certificat	Description
Apexx .NET Root CA	• Créé lors de l'installation du logiciel et stocké dans le magasin de certificats de la machine locale, dans le dossier Trusted Root Certification Authorities • Lors du processus d'installation de l'API, il est stocké dans le dossier Personal Certificates de la machine locale (LM\Personal\Certificates) • Tout ordinateur exécutant le logiciel (client, serveur, base de données, etc.) nécessite une copie de ce certificat à des fins de sécurité et d'identification • La PKI du logiciel local signe les demandes de certificats pour tous les clients du broker MQTT • Ces certificats sont utilisés pour établir des connexions TLS (Transport Layer Security) approuvées mutuellement et l'authentification avec le broker MQTT • Il est également possible de signer les certificats utilisés par SQL Server pour les connexions TLS • Utilise RSA pour les signatures
Apexx .NET ECC Root CA	• Créé lors de l'installation du logiciel et stocké dans le magasin de certificats de la machine locale, dans le dossier Trusted Root Certification Authorities • Lors du processus d'installation de l'API, il est stocké dans le dossier Personal Certificates de la machine locale (LM\Personal\Certificates) • Tout ordinateur exécutant le logiciel (client, serveur, base de données, etc.) nécessite une copie de ce certificat à des fins de sécurité et d'identification • La PKI du logiciel local signe les demandes de certificats pour tous les clients du broker MQTT • Ces certificats sont utilisés pour établir des connexions TLS (Transport Layer Security) approuvées mutuellement et l'authentification avec le broker MQTT • Il est également possible de signer les certificats utilisés par SQL Server pour les connexions TLS • Utilise ECDSA pour les signatures
Client MQTT Apexx	• Créé lors de la connexion du client au logiciel • Utilisé pour les connexions TLS et l'authentification
Colonne Apexx toujours chiffrée	• Chiffrement des données au niveau de l'API qui sont transférées dans la colonne chiffrée de la base de données • Lors du processus d'installation de l'API, il est stocké dans le dossier Personal Certificates de la machine locale (LM\Personal\Certificates)

Remarque : les certificats peuvent être renouvelés 60 jours avant leur expiration en renouvelant votre licence à l'aide de l'outil d'enregistrement en ligne du logiciel de la série Apexx.

Configurations du matériel informatique

La partie matériel informatique/API/logiciel du système Apexx peut être configurée de différentes manières en fonction de la complexité de votre système (nombre de systèmes de verrouillage Apexx, leur emplacement, etc.). Cette section ne présente que quelques-unes des nombreuses configurations possibles. Pour plus en savoir plus sur les licences requises pour les différentes configurations informatiques et matérielles, reportez-vous aux Catalogues de prix Axessor Apexx ou CenconX.

Remarque : si vous le souhaitez, l'un des composants logiciels (client, base de données, API ou MQTT) peut être hébergé sur une machine virtuelle.

Configuration d'un seul ordinateur (connexion USB)

La Figure 4 illustre une configuration de base impliquant un seul ordinateur et un système de verrouillage Axessor Apexx et/ou CenconX. Dans cette configuration, tous les éléments API/logiciels sont hébergés sur un seul ordinateur, une connexion USB étant utilisée pour se connecter temporairement au système de verrouillage Axessor Apexx ou CenconX à des fins de programmation et de configuration du système.

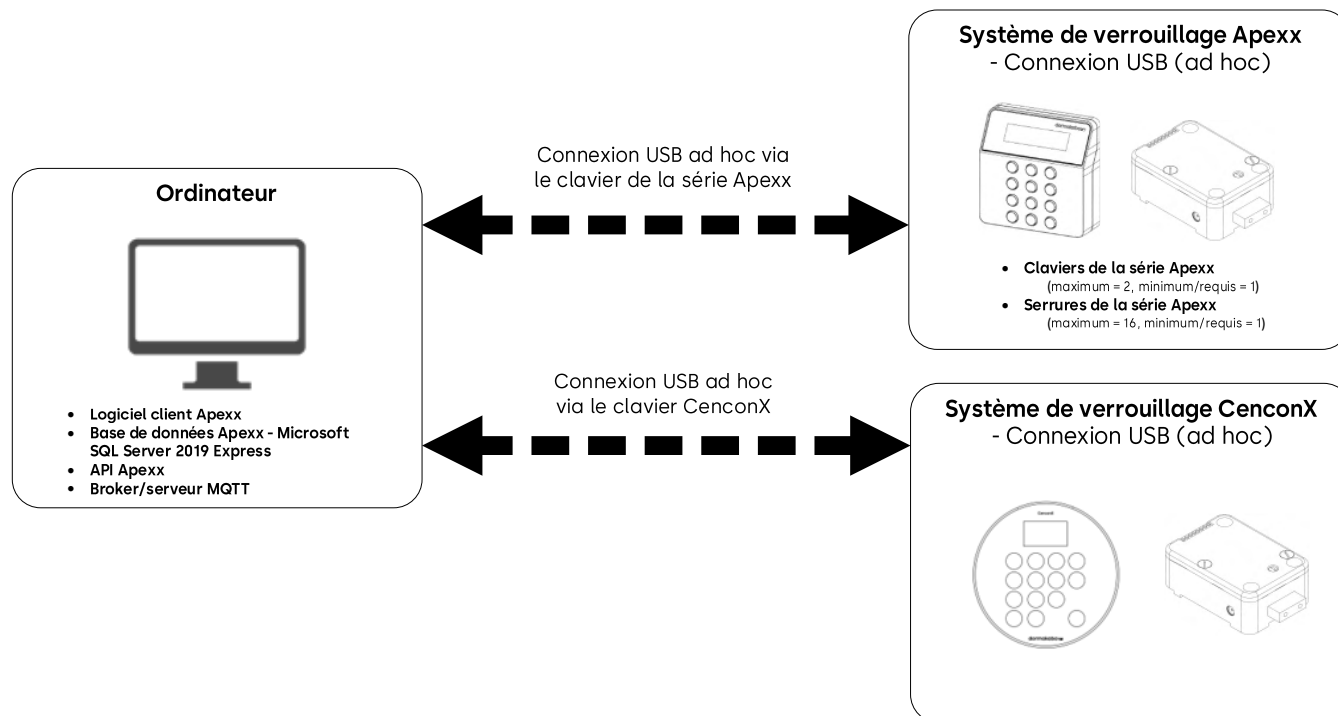


Figure 4 - Configuration d'un seul ordinateur - Connexion USB ad hoc

Systèmes de serrures Axessor Apexx - Connexion USB

En ce qui concerne le système Axessor Apexx, cette configuration fonctionne bien pour les petits sites où l'ordinateur et tous les composants du système de verrouillage (claviers et serrures) se trouvent au même endroit, mais n'offre pas la même polyvalence et la même praticité que les configurations en réseau utilisant l'eBox Apexx.

Systèmes de serrures CenconX - Connexion USB

Pour CenconX, les connexions USB uniquement ne sont pas recommandées pour les systèmes CenconX utilisant la fonctionnalité OTC.

Configuration d'un seul ordinateur (TCP/IP)

La Figure 5 montre une autre configuration simple impliquant seulement un ordinateur et un système de verrouillage Axessor Apexx et/ou CenconX.

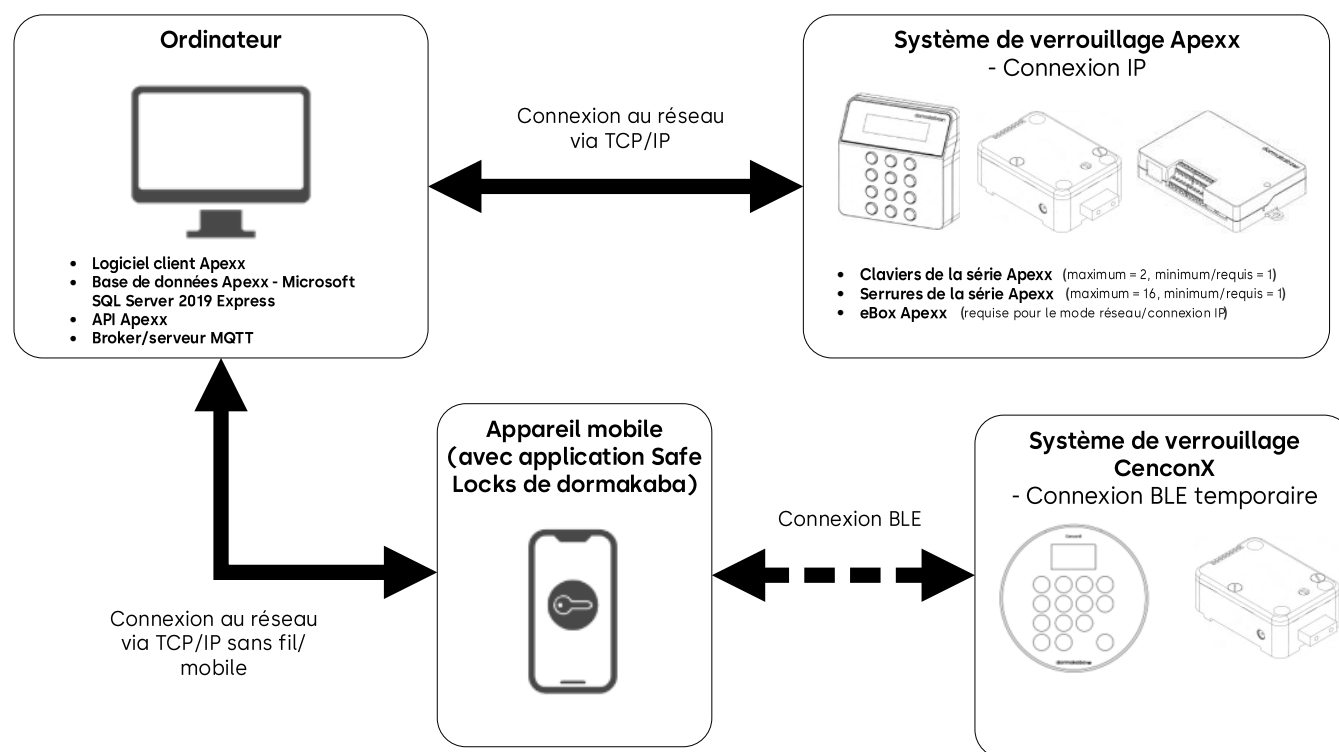


Figure 5 - Configuration d'un seul ordinateur - Réseau via l'eBox (TCP/IP) et mobile

Systèmes de serrures Axessor Apexx - Configuration d'un seul ordinateur (TCP/IP)

L'eBox Apexx est utilisée pour fournir une connexion réseau/IP pour une communication continue ou en direct entre l'ordinateur et le système de verrouillage Axessor Apexx.

En ce qui concerne les systèmes de verrouillage Axessor Apexx, cette configuration est également utile pour les configurations plus petites où tout l'équipement se trouve au même endroit, mais l'inclusion de l'eBox permet à l'administrateur du système de profiter de toutes les fonctionnalités offertes par une connexion IP active (audits en direct, surveillance active du système, mises à jour à distance du firmware et autres fonctionnalités matérielles/logicielles).

Systèmes de serrures CenconX - Configuration d'un seul ordinateur (TCP/IP)

En ce qui concerne le système de verrouillage CenconX, l'appareil mobile se connecte au serveur/client de l'ordinateur via une connexion réseau/IP et un « pont » BLE temporaire connecte l'appareil mobile au système de verrouillage CenconX.

Configurations de plusieurs ordinateurs

Pour les sites plus importants impliquant des bâtiments plus grands et/ou plusieurs systèmes de verrouillage, la configuration à plusieurs ordinateurs illustrée dans la Figure 6 offre une plus grande flexibilité.

Remarque : une seule API, un seul broker MQTT et une seule base de données SQL Server sont autorisés dans le système.

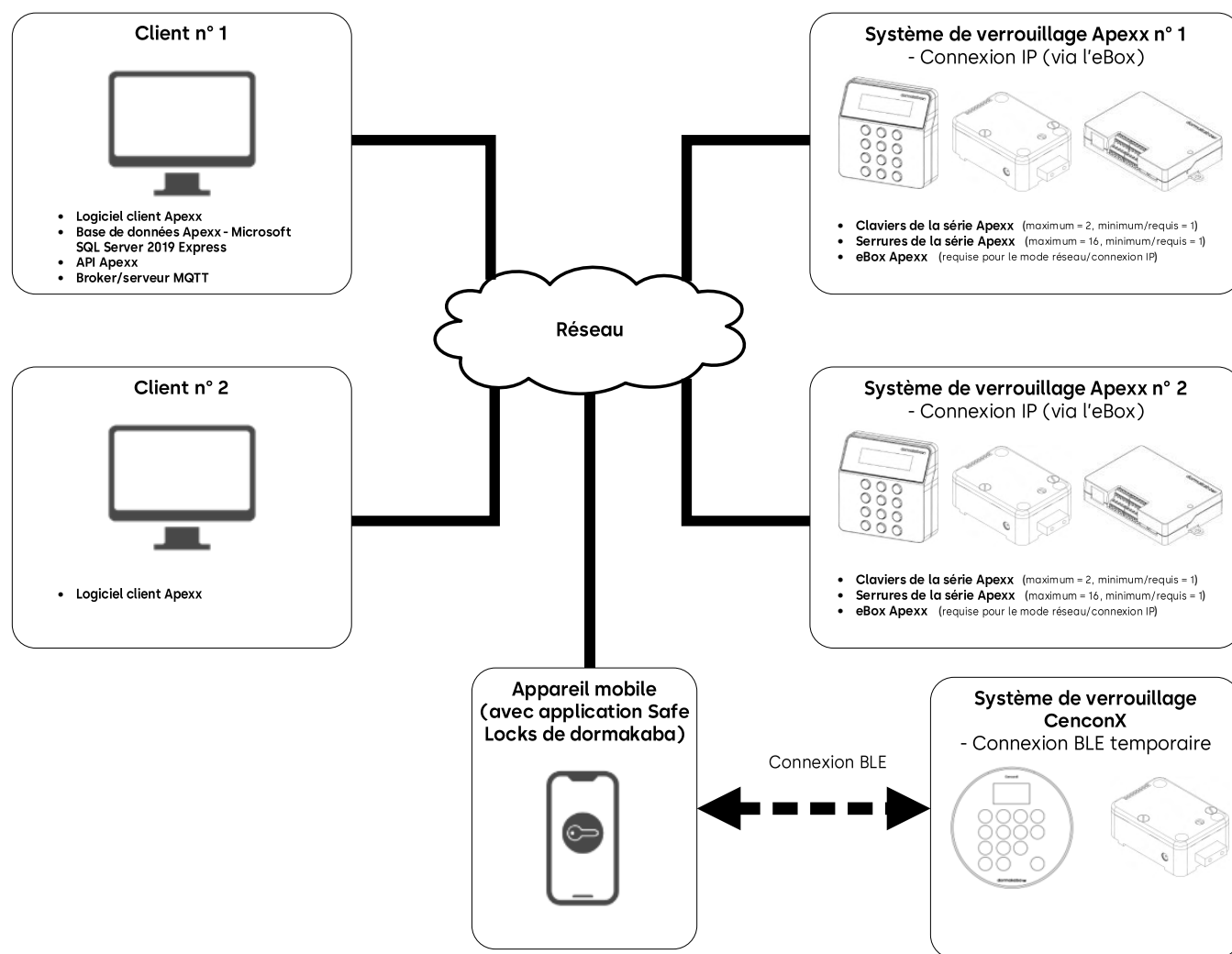


Figure 6 - Configuration de plusieurs ordinateurs avec plusieurs systèmes de verrouillage

Dans une telle configuration, la totalité ou une partie des composants logiciels peuvent être installés sur un ou plusieurs ordinateurs (ou machines virtuelles), ce qui permet davantage de praticité et de flexibilité lorsqu'il s'agit d'exécuter et de configurer vos systèmes de serrures. Il convient de noter que chaque système de verrouillage Axessor Apexx se connecte au réseau via une eBox Apexx.

Ce concept est davantage développé dans le système montré à la Figure 7, qui comprend plusieurs ordinateurs et systèmes de serrures répartis dans plusieurs bâtiments.

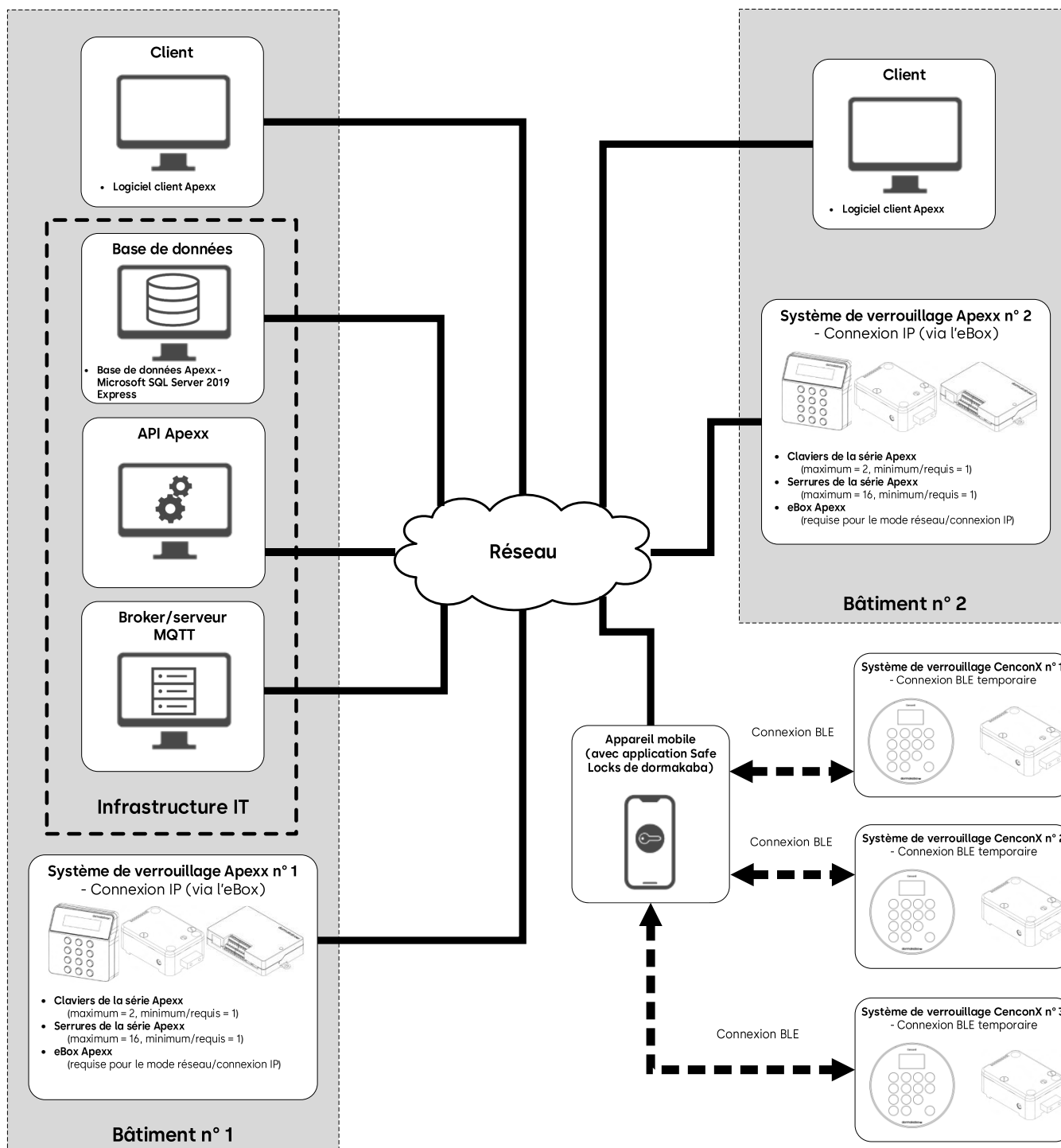


Figure 7 - Configuration de plusieurs ordinateurs/systèmes de verrouillage avec configuration multi-serveurs

Cette configuration se distingue des autres grâce au fait qu'elle comprend plusieurs ordinateurs qui hébergent différents composants logiciels. Notez que deux des ordinateurs du bâtiment n° 1 hébergent respectivement l'API Apexx et la base de données Apexx. Ces deux ordinateurs peuvent être configurés pour servir d'API et de base de données pour les systèmes de verrouillage du bâtiment n° 1, du bâtiment n° 2 et/ou de tout autre système de serrures sur l'ensemble du réseau.

Le dernier exemple montre que de nombreuses configurations différentes sont possibles en fonction des besoins de votre organisation et de la configuration de l'infrastructure informatique.

Points à prendre en considération concernant la base de données

Le logiciel de la série Apexx inclut Microsoft SQL Server 2019 Express comme moteur de base de données interne dédié.

	Microsoft SQL Server 2019 Express (64 bits)
Limite de la base de données	10 GO
Nombre de processeurs	1 processeur physique
RAM	1 GO
Systèmes d'exploitation pris en charge	Windows 10, Windows Server 2016, Windows Server 2019

Spécifications minimales de l'ordinateur recommandées pour Apexx

*Envisager le doublement pour les installations plus importantes

Station de travail client Apexx

- Processeur 2,0 GHz avec 4 cœurs*
- RAM de 16 Go
- Disque dur de 500 Go
- Windows 10 Professionnel 64 bits

Serveur broker Apexx

- Processeur 2,0 GHz avec 4 cœurs*
- RAM de 16 Go
- Disque dur de 500 Go
- Windows 2019 Server Standard 64 bits

Serveur de base de données Apexx et API Apexx

- Processeur 2,0 GHz avec 6 cœurs*
- RAM de 32 Go*
- Disque dur de 1 To
- Windows 2019 Server Standard 64 bits
- Microsoft SQL Server Standard ou Enterprise

Remarque : si vous le souhaitez, l'un des composants logiciels (client, base de données, API ou broker MQTT) peut être hébergé sur une machine virtuelle.

Spécifications de l'appareil mobile Apexx

(à la date de publication du document)

- Système d'exploitation mobile : Android 8+ ou iOS 15+
- Doit être compatible BLE

Remarque : consultez Google Play et l'Apple Store pour obtenir les dernières versions de l'application mobile Safe Locks de dormakaba et en savoir plus sur la compatibilité entre les appareils et les OS.

Guide de sécurité informatique Apexx

Remarques sur le logiciel local

- Tous les éléments du logiciel (MQTT, client et API) sont conçus comme des applications Windows. Pour les utiliser dans un environnement cloud, vous devez pouvoir gérer les canaux de communication entre eux.
- Les canaux de communication sont établis lors de l'installation. Ils s'appuient sur le DNS (ou les adresses IP statiques). Une fois l'installation terminée, des certificats seront établis à des fins de sécurité. Ils doivent faire l'objet d'une gestion adaptée afin d'éviter toute attaque.
- La communication vers et depuis le système de verrouillage se fait par MQTT sur SSL, de sorte que les ports standard doivent être accessibles.
- Le sous-système de certificats de Windows et une base de données SQL19 sont nécessaires pour faire fonctionner le logiciel.
- Ce dernier n'est pas compatible avec les systèmes Mac ou Linux.
- Les environnements cloud testés sont Azure et AWS.
- Un même utilisateur ne peut être connecté à plusieurs clients en même temps.

Appairage d'un logiciel local avec une eBox (Axessor Apexx)

Le logiciel local et l'eBox Apexx doivent être appairés avant qu'une connexion puisse être établie. Lorsqu'une nouvelle eBox doit être installée :

1. L'eBox est physiquement installée sur le bus CAN.
2. Un utilisateur autorisé doit se connecter au clavier et mettre en service l'eBox sur le bus CAN (aucun appareil non autorisé ne peut écouter le bus CAN).
3. Après la mise en service de l'eBox, celle-ci pourra obtenir les clés de chiffrement du bus CAN (AES-256 avec des clés spécifiques au système).
4. Une fois que l'eBox est sur le bus CAN, une connexion doit être établie avec le logiciel local. L'adresse IP peut être consultée et modifiée dans les paramètres du réseau, dans le menu avancé du clavier. S'il existe un réglage, il sera utilisé. Sinon, l'eBox utilisera le protocole DHCP pour obtenir l'adresse IP.
5. Une fois que les paramètres Ethernet sont valides, l'eBox tente de se connecter au serveur MQTT dans le logiciel local (soit par communication IP directe en fonction des paramètres, soit par diffusion sur le réseau local dans le cadre du protocole DHCP). Cette opération s'effectue via TLS.
6. Si le logiciel local détecte une nouvelle eBox, celle-ci doit être autorisée dans le logiciel avant de la connecter avec succès à l'aide du code de réclamation. Une fois que l'eBox est autorisée sur le logiciel, celui-ci génère un code PIN de vérification à valider sur le clavier (vérification du logiciel sur l'eBox, et de l'eBox sur le logiciel).

7. Une fois le système vérifié, un canal sécurisé est établi. Pour ce faire, des certificats préinstallés signés en usine sont utilisés (infrastructure PKI). Toute communication ultérieure est chiffrée à l'aide de TLS.
8. LeBox TLS 1.2. communique aussi initialement sur le port TCP 5001 (API) pour vérifier que le logiciel est activé, puis sur le port 8883 (par défaut) pour la communication.
9. Le logiciel doit être activé et disposer des certificats appropriés pour que l'eBox s'active correctement. Un logiciel inactivé entraînera un déni de service.

Pour en savoir plus sur l'installation, la connexion et la configuration de l'eBox Apexx, reportez-vous au Guide d'installation d'Axessor Apexx (document n° 801.0622), au Guide d'utilisation du système de clavier de la série Apexx (document n° 802.0622) et au menu d'aide du logiciel de la série Apexx.

Récupération après sinistre

Le logiciel local se connecte à la base de données SQL19 à des fins de stockage des données (SQL19 Express de Microsoft - Référence : <https://www.microsoft.com/en-ca/sql-server/sql-server-2019-pricing>). La configuration de la base de données doit être introduite dans le logiciel local sous la forme d'un fichier de configuration. Le chiffrement/la protection et la récupération des données suivront alors le chemin de la base de données SQL19. La base de données devrait être gérée par le service informatique local.

Le chemin de récupération devra alors réinstaller l'API, MQTT et le client soit avec une nouvelle copie de dormakaba, soit en utilisant une sauvegarde locale. Toutes les données sont conservées dans la base de données SQL. L'API, MQTT et le client ne stockent aucune donnée de verrouillage ou d'utilisateur, uniquement les paramètres de connexion et de configuration.

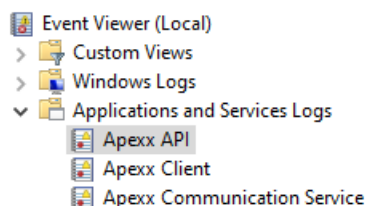
La base de données est créée automatiquement pour la première fois par le service API. La base de données utilise les connexions par défaut spécifiques au service NT (API ou BROKER) et s'authentifie par le biais des canaux Kerberos. Les paramètres par défaut de la base de données sont l'authentification Windows et les colonnes chiffrées. Nous recommandons le chiffrement au niveau du moteur, mais ne l'exigeons pas.

Visualisation et exportation des journaux d'événements Apexx



L'Observateur d'événements de Windows peut être utilisé pour visualiser et résoudre les problèmes liés aux applications et services Apexx.

1. Ouvrez l'observateur d'événements > saisissez « **Observateur d'événements** » dans la barre de recherche de Windows, puis ouvrez le programme.
2. Cliquez sur la flèche située à côté de > 📁 « **Applications et journaux des services** » pour dérouler la liste.
3. Cliquez sur l'application ou le service Apexx pour afficher tous les événements liés à cette application ou à ce service (API Apexx, client Apexx, service de communication Apexx).



4. À partir de là, vous pouvez trier les événements en fonction de l'heure, de l'identifiant de l'événement, etc. afin de faciliter la visualisation de votre configuration Apexx et de résoudre les problèmes qui y sont liés.
5. Exporter les journaux d'événements Apexx > Sous « **Actions** », vous pouvez choisir  « **Enregistrer tous les événements sous...** » pour exporter les journaux d'événements de l'application ou du service sélectionné(e) et les enregistrer dans l'un des formats suivants (.evtx, .xml, .txt, .csv).

Principaux enseignements

1. Seuls les serveurs dotés d'un logiciel local doivent avoir une adresse IP, ce qui n'est pas le cas de l'eBox.
2. La communication entre l'eBox et le logiciel local (trafic sur l'intranet/Internet) est chiffrée à l'aide de TLS.
3. Veuillez inclure SQL Server dans votre plan de récupération après sinistre. Cette base de données est essentielle au fonctionnement du système.



Access Automation Solutions

Entrance Automation
Entrance Security



Access Control Solutions

Electronic Access & Data
Escape and Rescue Systems
Lodging Systems



Access Hardware Solutions

Door Closers
Architectural Hardware
Mechanical Key Systems



Services

Technical Support
Installation and commissioning
Maintenance and Repair



Key & Wall Solutions

Key Systems
Movable / Sliding Walls



Safe Locks

Electronic Safe Locks
Mechanical Safe Locks
Boltworks and Accessories



Glass systems

Manual door systems
Glass fittings
Horizontal Sliding Walls

Notre engagement en matière de développement durable

Nous nous engageons à favoriser un développement durable tout au long de notre chaîne de valeur, conformément à nos responsabilités économiques, environnementales et sociales envers les générations actuelles et futures. La durabilité des produits est une approche importante et tournée vers l'avenir dans le secteur de la construction. Afin de fournir des informations quantifiées sur l'impact environnemental d'un produit tout au long de son cycle de vie, dormakaba fournit des Déclarations Environnementales de Produit (DEP), basées sur des analyses holistiques du cycle de vie.

<https://www.dormakabagroup.com/en/sustainability/product-declarations>.

Guide d'architecture système et de sécurité informatique
Axessor Apexx - Rév. B
Sous réserve de modifications sans préavis

Dormakaba SAL GmbH

Siemensstrasse 33
42551 Velbert
safelocks.de@dormakaba.com
T +49 2051 9111 0

dormakaba USA Inc.

1525 Bull Lea Road, Suite 100
Lexington, KY 460511
sales.safelocks.us@dormakaba.com
1-800-950-4744



AXESSOR APEXX IP
INSTALLATION AND
OPERATION GUIDES

dk.world/AxessorApexxIP

Software della serie Axessor Apexx

Guida all'architettura di sistema e alla sicurezza IT per Axessor Apexx IP/CIT e CenconX



Indice

- Architettura del sistema Apexx 3**
 - Panoramica..... 3
 - Sistema di chiusura Axessor Apexx..... 3
 - Sistema di chiusura CenconX..... 3
 - Dispositivi mobili 4
 - Componenti API/software..... 4
 - API Apexx..... 4
 - Apexx Client Software..... 4
 - Database Apexx..... 4
 - Broker/server MQTT..... 5
 - SMTP 5
 - SSO..... 5
 - Configurazione utente - Axessor Apexx 5
 - Configurazione utente - CenconX..... 6
 - Configurazione utente - Utenti software 6
 - Utenti del software - Axessor Apexx 6
 - Utenti del software - CenconX..... 6
 - Licenze..... 7
 - Metodi di aggiornamento del firmware 7
 - Aggiornamenti del firmware - Sistema di chiusura Axessor Apexx 7
 - Aggiornamenti del firmware - Sistema di chiusura CenconX..... 7
 - Transito di dati 8
 - Sicurezza e crittografia dei dati 10
 - Infrastruttura a chiave pubblica (PKI)..... 11

Configurazioni hardware del computer	13
Impostazione di un singolo computer (connessione USB)	13
Configurazione di un singolo computer (TCP/IP)	14
Configurazioni di più computer	15
Considerazioni sul database	17
Specifiche minime consigliate per il computer Apexx	17
Specifiche del dispositivo mobile Apexx	17
Guida alla sicurezza informatica di Apexx	18
Note sul software locale	18
Accoppiamento del software locale con eBox (Axessor Apexx)	18
Recupero in caso di catastrofe	19
Visualizzazione ed esportazione dei registri eventi Apexx	19
Punti salienti	20

Architettura del sistema Apexx

Panoramica

Il **software della serie Apexx** può essere utilizzato per gestire e configurare da remoto vari aspetti dei sistemi di chiusura Axessor Apexx e CenconX. Questo documento descrive gli aspetti dell'architettura del sistema, dell'infrastruttura informatica e dei requisiti per l'utilizzo del software della serie Apexx per il supporto e la gestione dei sistemi di chiusura Axessor Apexx e CenconX.

Sistema di chiusura Axessor Apexx

I sistemi di chiusura Axessor Apexx sono costituiti da 2 reti di comunicazione sicure: il **CAN bus del sistema di chiusura** e la **rete API/software**.

Il **CAN bus del sistema di chiusura** supporta i seguenti componenti:

- **Tastierini serie Apexx** (massimo = 2, minimo/richiesto = 1)
 - Utilizzato come interfaccia utente per l'accesso e la configurazione del sistema di chiusura
- **Serrature serie Apexx** (massimo = 16, minimo/richiesto = 1)
 - Serratura fisica elettromeccanica che controlla l'accesso degli utenti alla cassaforte
- **eBox Apexx** (necessario per la modalità connessa in rete/IP)
 - Funziona come convertitore di protocollo (da IP a CAN bus) tra il sistema di chiusura Axessor Apexx e l'API/Software
 - Funziona anche come box I/O (ingresso/uscita)

Sistema di chiusura CenconX

I sistemi di chiusura CenconX sono costituiti da 2 reti di comunicazione sicure: il **sistema di chiusura** e la **rete API/Software**

Il **sistema di chiusura** supporta i seguenti componenti:

- **Tastierini serie CenconX** (1)
 - Utilizzato come interfaccia utente per l'accesso e la configurazione del sistema di chiusura.
- **Serrature serie CenconX** (1)
 - Serratura fisica elettromeccanica che controlla l'accesso degli utenti alla cassaforte.

Dispositivi mobili

La Mobile App Safe Locks di dormakaba può essere utilizzata per interfacciarsi con i sistemi di chiusura Axessor Apexx e CenconX. È disponibile per il download gratuito su Google Play e Apple Store, ma non funziona finché non viene registrata con il software della serie Apexx. Per informazioni sull'uso dell'applicazione mobile e su come registrare un dispositivo mobile, consultare la Guida utente del sistema CenconX (documento #CX003.0524) e il menu di aiuto del software della serie Apexx.

- **Sistemi di chiusura Axessor Apexx** > I dispositivi Axessor Apexx con versione firmware 2.1.x.x o superiore possono incorporare dispositivi mobili tramite **l'app mobile dormakaba Safe Locks**.
- **Sistemi di chiusura CenconX** > **L'app mobile Safe Locks** di dormakaba funge da ponte tra il sistema di chiusura CenconX e l'API/Software e serve ad autenticare e aprire le serrature CenconX.

Componenti API/software

L'**API/software** è costituito da 4 componenti principali:

- API Apexx
- Apexx Client Software
- Database Apexx - Microsoft SQL Server 2019 Express
- Broker/server MQTT

Nota: Il server/client Apexx deve essere configurato utilizzando un IP accessibile al pubblico per facilitare la comunicazione con i dispositivi mobili.

API Apexx

L'interfaccia di programmazione delle applicazioni, o API, funge sia da publisher che da subscriber nell'architettura MQTT.

Apexx Client Software

L'Apexx Client Software ("della serie Apexx Software") è un'interfaccia grafica utente (GUI) che consente agli utenti del software di utilizzare l'API per eseguire azioni nel sistema Apexx/CenconX (modificare le impostazioni del sistema, memorizzare/recuperare dati, ecc.)

Il client Apexx supporta più utenti, ma non supporta molteplici utenti in simultanea su un singolo client. Una sola persona può accedere a una singola istanza del client in un dato momento.

Database Apexx

Il database Apexx è il luogo principale di archiviazione dei dati nel sistema Apexx. Il database Apexx utilizza il sistema di gestione di database relazionali proprietario di Microsoft, Microsoft SQL Server 2019 Express, come mezzo per archiviare e recuperare i dati del sistema.

Broker/server MQTT

Message Queuing Telemetry Transport, o MQTT, è un protocollo di messaggistica che utilizza un modello publish-subscribe per facilitare la comunicazione tra dispositivi. Il broker/server MQTT funge da hub di messaggistica centralizzato e utilizza il protocollo MQTT per gestire la comunicazione tra i dispositivi. In particolare, MQTT passa i messaggi tra il software client Windows e l'eBox.

SMTP

Il software della serie Apexx utilizza il Simple Mail Transport Protocol (SMTP) per inviare quanto segue: Avvisi attivi, rapporti programmati e informazioni sulla configurazione dei dispositivi mobili.

- Gli avvisi attivi vengono inviati ai destinatari in base al verificarsi di uno o più eventi di audit selezionati dall'utente.
- I rapporti programmati possono essere inviati via e-mail ai destinatari in base a una pianificazione definita dall'utente, anche tramite SMTP.
- Quando si aggiunge un nuovo dispositivo mobile nel software della serie Apexx, è possibile utilizzare il codice QR generato per la configurazione del dispositivo mobile. Quando si utilizza l'applicazione mobile Safe Locks per scansionare il codice QR, il sistema utilizza SMTP per inviare le informazioni di configurazione al dispositivo mobile.
- Per informazioni su come configurare le impostazioni SMTP, consultare il menu di aiuto del software della serie Apexx.

SSO

Il software della serie Apexx utilizza il Single Sign-On, garantendo che un utente del software possa utilizzare le proprie credenziali per accedere all'API utilizzando un unico set di credenziali.

Configurazione utente - Axessor Apexx

Gli utenti del sistema Axessor Apexx si dividono in due categorie distinte: **Utenti della serratura della cassaforte** e **utenti del software**

Gli **utenti della serratura della cassaforte** sono utenti che utilizzeranno il sistema di chiusura Axessor Apexx (costituito da tastierini fisici, serrature ed eBox) e avranno credenziali e ruoli unici con autorizzazioni che determineranno il loro accesso al sistema di chiusura.

Gli utenti della serratura della cassaforte utilizzano ID utente e PIN numerici per accedere al sistema di chiusura tramite il tastierino della serie Apexx. Questa modalità di funzionamento è nota come modalità banca (o modalità statica).

I tre tipi di utente della serratura della cassaforte predefiniti (Amministratore, Manager e Utente) costituiscono una gerarchia di utenti, ciascuno con ruoli e privilegi predefiniti all'interno del sistema di chiusura. Oltre a questi tipi di utenti, è possibile creare ulteriori ruoli utente della serratura della cassaforte utilizzando gli strumenti amministrativi del software Apexx Series, con autorizzazioni definite da un utente software. Questi ruoli utente aggiuntivi vengono creati utilizzando una struttura dei 3 tipi di utente iniziali, consentendo così di creare nuovi tipi di utente per soddisfare le esigenze di personalizzazione del cliente.

I dispositivi Axessor Apexx con versione firmware 2.1.x.x o successiva introducono ulteriori tipi di utenti (un Amministratore primario e un Amministratore tenant), nonché due modalità utente aggiuntive (modalità OTC e modalità ICS) che prevedono l'uso di dispositivi mobili per l'accesso alla serratura. Per ulteriori dettagli sui tipi di utente e sulle modalità utente di Safe Lock, consultare la Guida utente del sistema di tastierini della serie Apexx (documento n. 802.0622).

Configurazione utente - CenconX

Gli utenti del sistema Axessor Apexx si dividono in due categorie distinte: **Utenti della serratura della cassaforte** e **utenti del software**

Gli **utenti della serratura della cassaforte** sono utenti che utilizzeranno il sistema di chiusura CenconX (costituito da tastierini fisici, serrature, ecc.) e avranno credenziali e ruoli unici con autorizzazioni che definiscono il loro accesso al sistema di chiusura.

I tipi di utenti della serratura della cassaforte nei sistemi CenconX includono amministratori, manager, utenti con PIN statico (modalità banca) e utenti OTC (One Time Code). Per ulteriori informazioni sui tipi di utente e sulle relative autorizzazioni, consultare la Guida utente del sistema CenconX (documento n. CX003.0524).

Configurazione utente - Utenti software

Per **utenti del software** si intendono gli utenti che utilizzano il software della serie Apexx e i suoi strumenti per eseguire attività di gestione e amministrazione. A differenza degli utenti della serratura della cassaforte, gli utenti del software non accedono direttamente al sistema di chiusura fisico (aprire/chudere le porte della cassaforte), ma eseguono compiti amministrativi/gestionali tramite il software (aggiungere utenti del sistema di chiusura, reimpostare le password degli utenti del sistema di chiusura).

Gli utenti del software utilizzano le credenziali per accedere al software della serie Apexx tramite single sign-on (SSO). Altri tipi di autenticazione per gli utenti del software della serie Apexx includono l'autenticazione di Windows (ad eccezione di Entra ID), l'autenticazione di dominio di Windows e Google OAuth 2.0.

Gli utenti software che dispongono di un'autorizzazione di "scrittura" in qualità di utente software possono aggiungere nuovi utenti software e configurare le autorizzazioni di lettura/scrittura.

Utenti del software - Axessor Apexx

I tipi di utenti del software nei sistemi Axessor Apexx includono amministratori e manager. Per le applicazioni trasporto di denaro in contanti, anche i dispatcher e gli utenti di sola verifica hanno un ruolo (**Nota:** è richiesto il firmware del dispositivo 2.1.x.x o superiore).

Per ulteriori dettagli sui tipi di utente del software e sulle autorizzazioni, consultare il menu della guida del software della serie Apexx.

Utenti del software - CenconX

I tipi di utenti del software nei sistemi CenconX comprendono gli amministratori, i manager, i dispatcher e gli utenti di sola verifica. Per ulteriori informazioni sui tipi di utente e sulle relative autorizzazioni, consultare la Guida utente del sistema CenconX (documento n. CX003.0524).

Quando si configura il sistema di chiusura CenconX, si ha la possibilità di configurare un unico client/database per un unico proprietario (dispatcher primario), oppure si può introdurre un secondo client/database per consentire a un dispatcher secondario di avere un controllo condiviso sulla gestione e sull'accesso al sistema. Per ulteriori informazioni, consultare la Guida dell'utente del sistema CenconX (documento n. CX003.0524).

Licenze

Il software della serie Apexx dispone di diversi tipi di licenza, ognuno dei quali offre diverse funzioni e caratteristiche del software. Per ulteriori informazioni, consultare i listini Axessor Apexx IP e CenconX.

Metodi di aggiornamento del firmware

Il processo di aggiornamento del firmware del dispositivo Axessor Apexx varia a seconda della licenza acquistata.

Per ulteriori informazioni sul processo di aggiornamento del firmware, consultare la Guida dell'utente del sistema Axessor Apexx (documento n. 802.0622), la Guida dell'utente CenconX (documento n. CX003.0524) e il menu di aiuto del software della serie Apexx.

Aggiornamenti del firmware - Sistema di chiusura Axessor Apexx

Gli **aggiornamenti locali del firmware** possono essere eseguiti stabilendo una connessione USB temporanea tra il computer che ospita il software della serie Apexx e il tastierino del sistema di chiusura.

Gli **aggiornamenti remoti del firmware** possono essere eseguiti tramite una connessione di rete attraverso l'eBox. Si tratta di un processo in tre fasi:

1. Un utente software avvia il processo di aggiornamento remoto del firmware, inviando il firmware dall'API/software al sistema di chiusura tramite l'eBox.
2. Il firmware viene scaricato e memorizzato nel sistema di chiusura. Sul display del tastierino appare un messaggio che informa gli utenti della serratura della cassaforte che è in corso un aggiornamento del firmware.
3. L'utente della serratura della cassaforte inserisce credenziali valide (ID utente e PIN) sul tastierino, quindi avvia l'aggiornamento del firmware.

Aggiornamenti del firmware - Sistema di chiusura CenconX

Gli **aggiornamenti locali del firmware** possono essere eseguiti stabilendo una connessione USB temporanea tra il computer che ospita il software della serie Apexx e il tastierino del sistema di chiusura.

Gli utenti di CenconX mobile hanno anche l'opzione **Aggiornamenti firmware mobile**, con la quale l'applicazione mobile Safe Locks di dormakaba può essere utilizzata per ricevere gli aggiornamenti del firmware. Il processo prevede l'utilizzo del software della serie Apexx per inviare i file di aggiornamento del firmware al dispositivo mobile dell'utente. L'utente del dispositivo mobile può quindi accedere all'applicazione Safe Locks, scaricare i file necessari e avviare il processo di aggiornamento del firmware utilizzando una connessione BLE tra il dispositivo mobile e il tastierino CenconX.

Transito di dati

Figura 1 e il grafico che lo accompagna mostrano il flusso di dati tra i vari componenti hardware e software del sistema di chiusura Axessor Apexx.

Porta di comunicazione	Descrizione
443	Questa porta è utilizzata per il traffico TCP/IP in uscita.
587	Questa porta viene utilizzata per comunicare con l'host SMTP. È necessaria ed è impostata su 587.
5001	È la porta predefinita utilizzata per la messa in servizio di un sistema di chiusura Apexx.
8883	È la porta predefinita utilizzata dal broker MQTT.

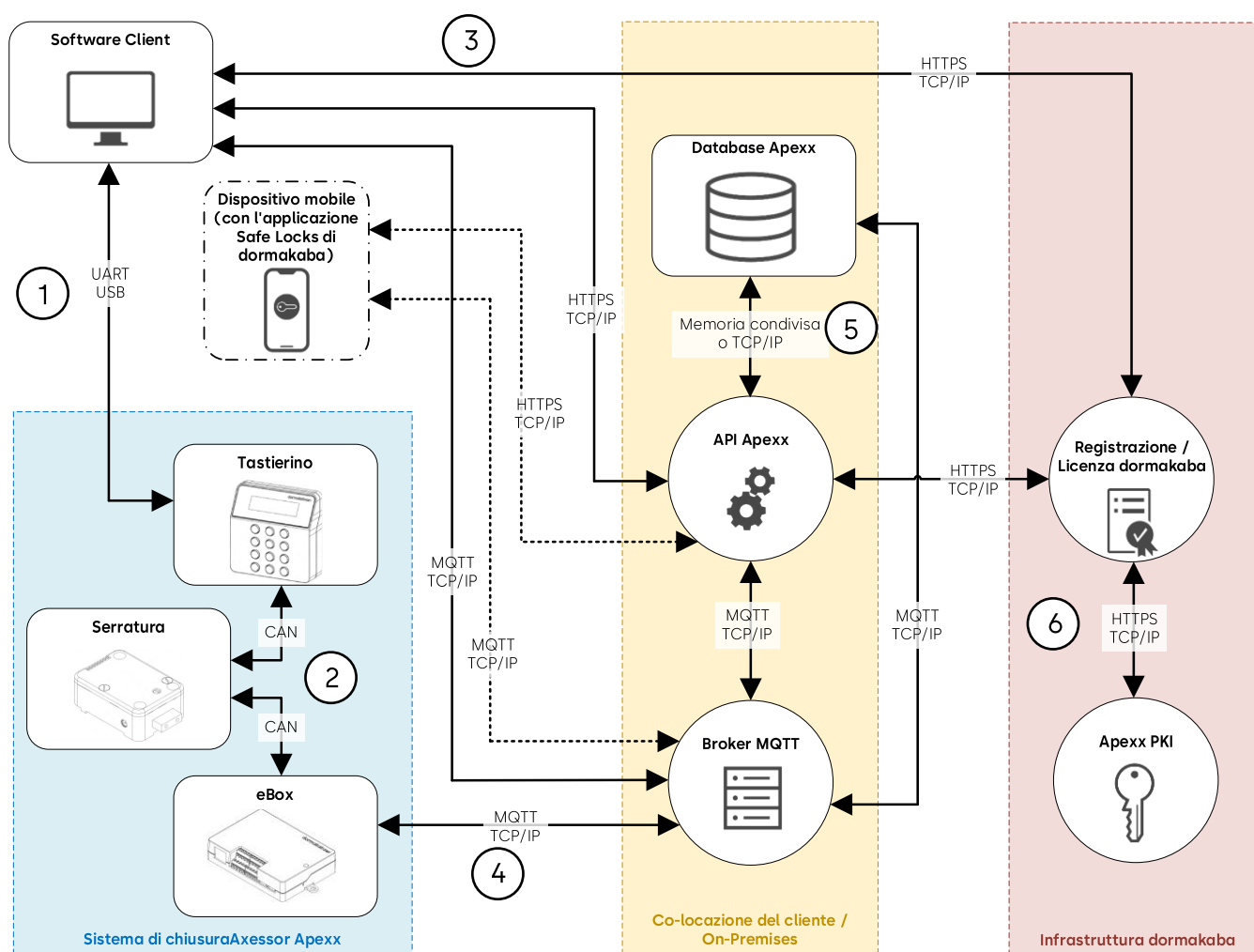


Figura 1 - Architettura del sistema Apexx con il sistema di chiusura Apexx - Componenti del sistema e transito di dati

	Protocolli di comunicazione	Flusso di dati	Descrizione/scopo
1	UART su USB	Percorso bidirezionale: Client Software a tastierino	Configurazione diretta e recupero degli audit
2	CAN	Percorso bidirezionale: - Tastierino a serratura - Serratura ad eBox	Comunicazione da dispositivo a dispositivo
3	HTTPS su TCP/IP	Percorso bidirezionale: Software client per la registrazione/licenza di dormakaba	Licenza e registrazione online
4	MQTT su TCP/IP	Percorso bidirezionale: - Software client per broker MQTT Percorso bidirezionale: - Broker da eBox a MQTT Percorso bidirezionale: - Dispositivo con applicazione mobile Safe Locks di dormakaba al broker MQTT	Configurazione in rete e recupero degli audit
5	Memoria condivisa o TCP/IP	Percorso bidirezionale: Da Apexx API al database Apexx	Archiviazione duratura dei dati con SQL Server
6	HTTPS su TCP/IP	Percorso bidirezionale: - Client Software ad Apexx API - Apexx API con Registrazione/Licenza dormakaba - Registrazione/Licenza dormakaba ad Apexx PKI - Dispositivo con applicazione mobile Safe Locks di dormakaba ad Apexx API	Emissione di certificati x.509

Figura 2 mostra uno schema simile a quello illustrato in Figura 1, ma con un sistema di chiusura CenconX al posto del sistema di chiusura Axessor Apexx. In questo caso, il dispositivo mobile funge da tramite per la comunicazione tra il sistema di chiusura CenconX e l'infrastruttura software.

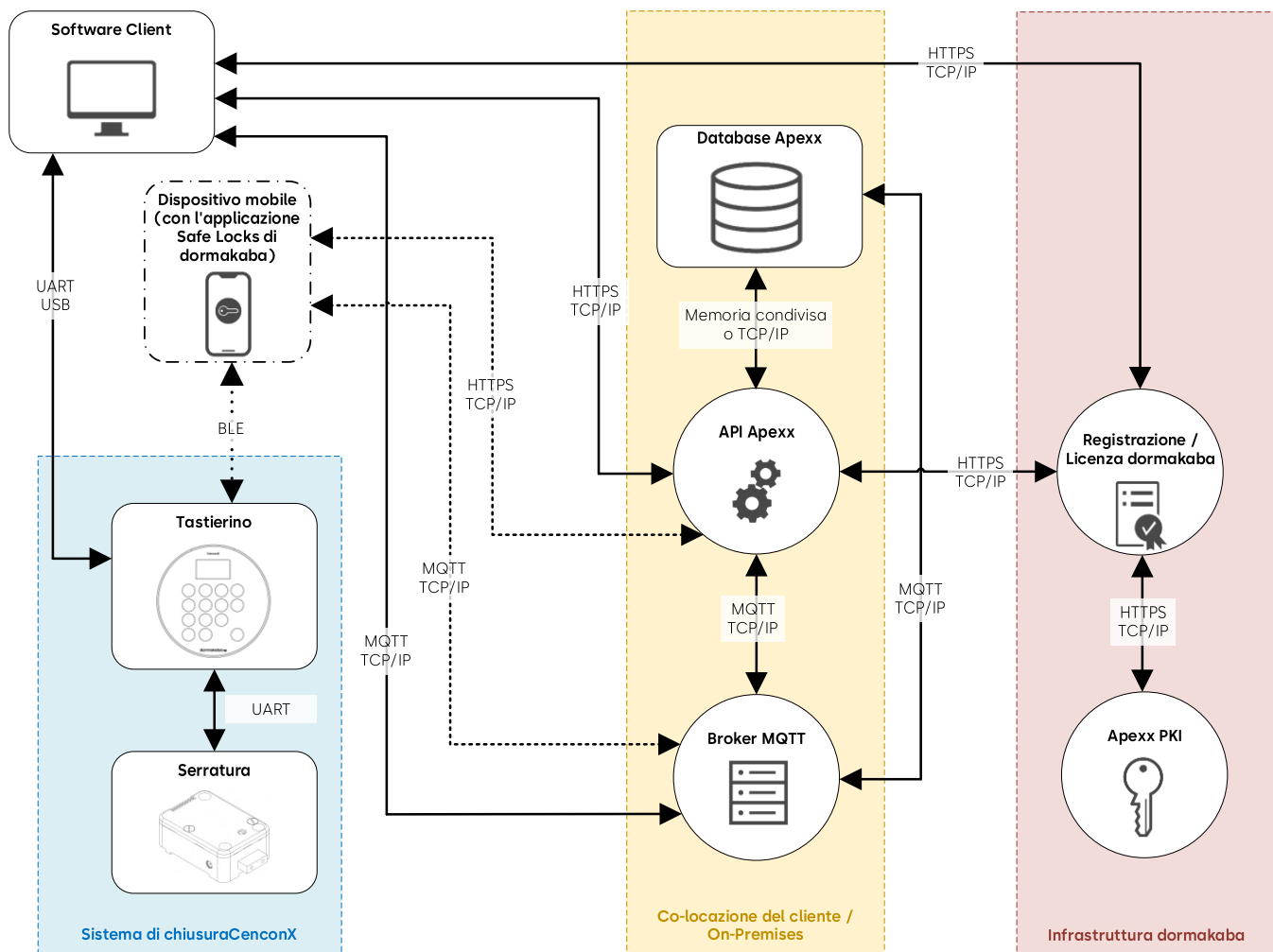


Figura 2 - Architettura del sistema Apexx con sistema di chiusura CenconX - Componenti del sistema e transito di dati

Sicurezza e crittografia dei dati

Il software della serie Apexx, i sistemi di chiusura CenconX, i sistemi di chiusura Axessor Apexx e i dispositivi mobili messi in servizio utilizzano diversi metodi di crittografia, tra cui AES256, PBKDF2 e certificati TLS, per garantire la sicurezza della comunicazione e della memorizzazione dei dati.

Infrastruttura a chiave pubblica (PKI)

Il software della serie Apexx, i sistemi di chiusura CenconX, i sistemi di chiusura Axessor Apexx e i dispositivi mobili messi in servizio utilizzano un'infrastruttura a chiave pubblica per creare, memorizzare e distribuire certificati digitali ai dispositivi Apexx tramite le autorità di certificazione.

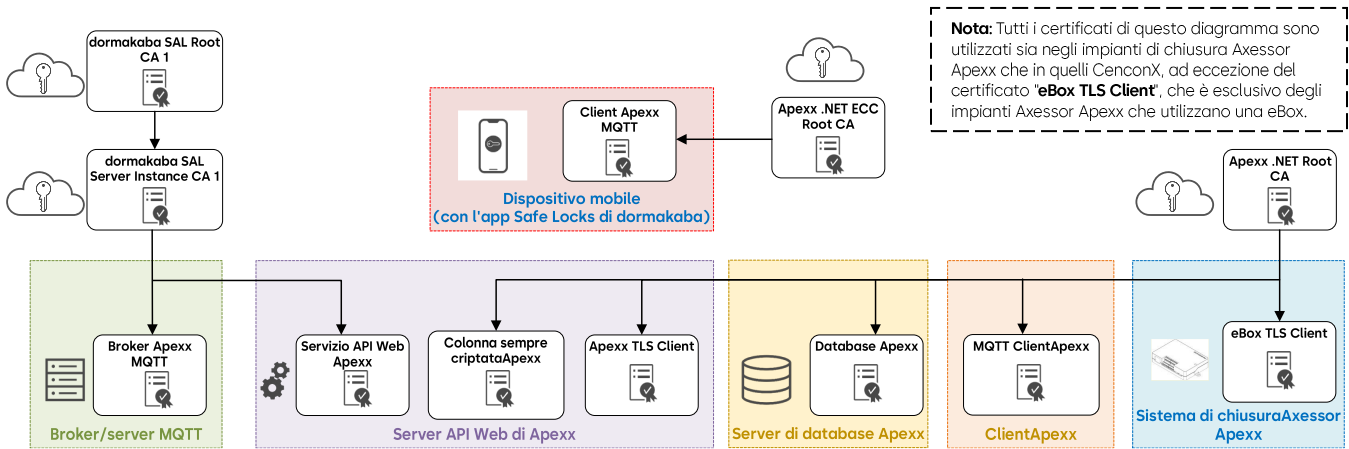


Figura 3 - Infrastruttura a chiave pubblica

Tipo di certificato	Descrizione
dormakaba SAL Root CA	- Questo certificato viene precaricato in fabbrica sui dispositivi e sostituito tramite aggiornamento del firmware. - Durante l'installazione del software della serie Apexx, questo certificato viene installato anche quando si esegue il file Prerequisites Installer sui computer client e server (memorizzato nella cartella Trusted Root Certification Authorities).
dormakaba SAL Server Instance CA	- I server che eseguono servizi software locali per Apexx necessitano di certificati firmati da dormakaba SAL PKI affinché i dispositivi possano considerarli affidabili. - Questo certificato deve essere distribuito a tutti i server che eseguono servizi software locali. - Durante l'installazione del software della serie Apexx, questo certificato viene installato anche quando si esegue il file Prerequisites Installer sui computer client e server (memorizzato nella cartella Intermediate Certification Authorities).
Broker Apexx MQTT	- Creato durante l'installazione del software. - Utilizzato per le connessioni TLS e l'autenticazione.
Servizio API Web di Apexx	- Creato durante l'installazione del software. - Contiene il nome del server (computer in cui è installato il servizio), l'autorità di certificazione di fiducia e la chiave pubblica di crittografia del server.
Apexx TLS Client	- Utilizzato per l'autenticazione del client Apexx. - Il certificato è un utente verificato se l'emittente corrisponde alla Apexx .NET Root CA installata sul server del broker.
Database Apexx	- SQL Server su Windows è l'unico motore di database supportato. - Le seguenti impostazioni sono abilitate sull'istanza/database: - Autenticazione di Windows - Il controllo degli accessi basato sui ruoli (RBAC) viene utilizzato all'interno, insieme all'autenticazione di Windows, per controllare le autorizzazioni.
eBox TLS Client	- Utilizzato per l'autenticazione dell'eBox. - Il certificato è un utente verificato se l'emittente corrisponde alla Apexx .NET Root CA installata sul server del broker.

Tipo di certificato	Descrizione
Apexx .NET Root CA	• Creato durante l'installazione del software e memorizzato nell'archivio dei certificati del computer locale nella cartella Trusted Root Certification Authorities. • Durante il processo di installazione dell'API, viene memorizzato nella cartella Personal Certificates del computer locale (LM\Personal\Certificates). • Ogni computer che esegue il software (client, server, database, ecc.) richiede una copia di questo certificato per motivi di sicurezza/identificazione. • La PKI software locale firma le richieste di certificato per tutti i client del broker MQTT. • Questi certificati sono utilizzati sia per stabilire connessioni Transport Layer Security (TLS) a fiducia reciproca, sia per l'autenticazione con il broker MQTT. • Può anche firmare i certificati utilizzati da SQL Server per TLS. • Utilizza RSA per le firme.
Apexx .NET ECC Root CA	• Creato durante l'installazione del software e memorizzato nell'archivio dei certificati del computer locale nella cartella Trusted Root Certification Authorities. • Durante il processo di installazione dell'API, viene memorizzato nella cartella Personal Certificates del computer locale (LM\Personal\Certificates). • Ogni computer che esegue il software (client, server, database, ecc.) richiede una copia di questo certificato per motivi di sicurezza/identificazione. • La PKI software locale firma le richieste di certificato per tutti i client del broker MQTT. • Questi certificati sono utilizzati sia per stabilire connessioni Transport Layer Security (TLS) a fiducia reciproca, sia per l'autenticazione con il broker MQTT. • Può anche firmare i certificati utilizzati da SQL Server per TLS. • Utilizza ECDSA per le firme.
Client Apexx MQTT	• Creato durante il login del client software. • Utilizzato per le connessioni TLS e l'autenticazione.
Colonna sempre criptata Apexx	• Crittografia dei dati dell'API che vanno alla colonna crittografata del database. • Durante il processo di installazione dell'API, viene memorizzato nella cartella Personal Certificates del computer locale (LM\Personal\Certificates).

Nota: I certificati possono essere rinnovati 60 giorni prima della scadenza rinnovando la licenza tramite lo strumento di registrazione online di della serie Apexx Software.

Configurazioni hardware del computer

La parte hardware/API/software del sistema Apexx può essere configurata in vari modi, a seconda della complessità del sistema (numero di sistemi di chiusura Apexx, ubicazione, ecc.). Questa sezione illustra solo alcune delle diverse configurazioni possibili. Per ulteriori informazioni sui requisiti di licenza per le varie configurazioni di computer/hardware, consultare il listino prezzi di Axessor Apexx o CenconX.

Nota: Se lo si desidera, uno qualsiasi dei componenti software (client, database, API o MQTT) può essere ospitato su una macchina virtuale.

Impostazione di un singolo computer (connessione USB)

Figura 4 illustra una configurazione di base che prevede un solo computer e un sistema di chiusura Axessor Apexx e/o un sistema di chiusura CenconX. In questa configurazione, tutti gli elementi API/software sono ospitati su un unico computer, con una connessione USB utilizzata per collegarsi temporaneamente al sistema di chiusura Axessor Apexx o CenconX a fini di programmazione/configurazione del sistema.

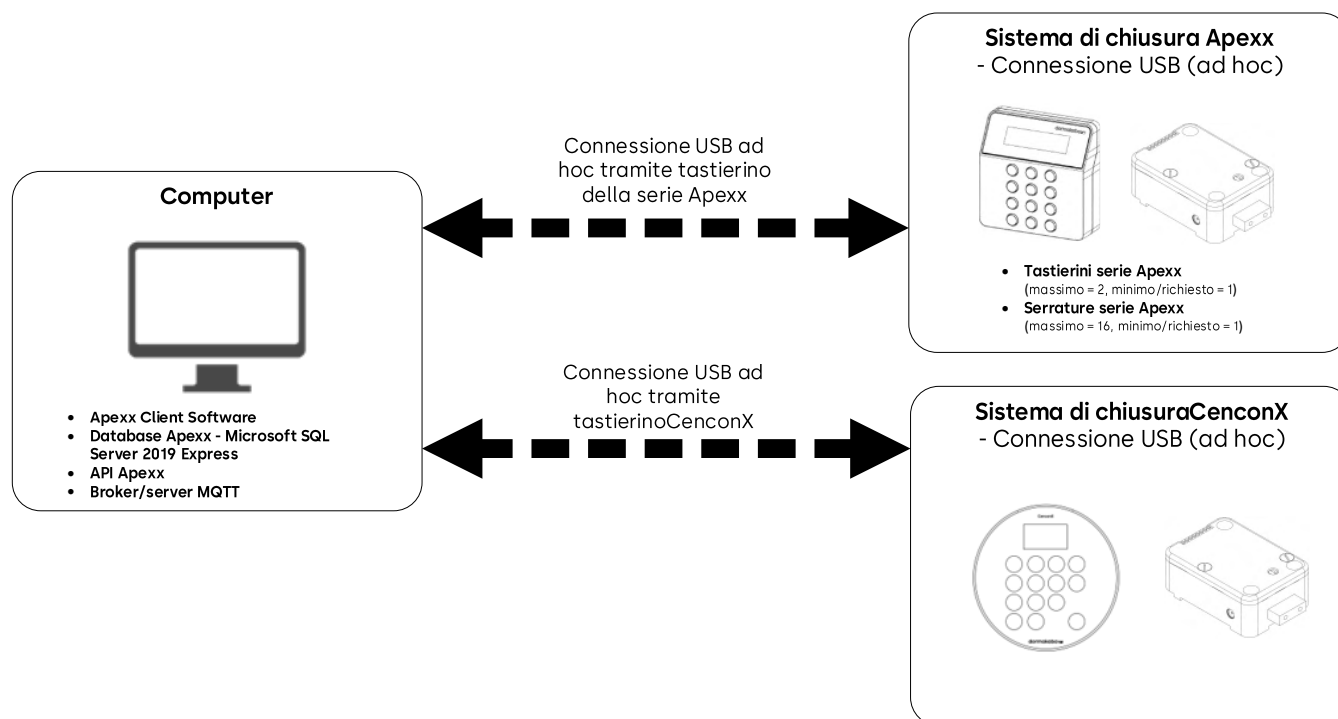


Figura 4 - Configurazione di un singolo computer - connessione USB ad hoc

Sistemi di chiusura Axessor Apexx - Connessione USB

Per Axessor Apexx, questo tipo di configurazione funziona bene per le piccole sedi in cui il computer e tutti i componenti del sistema di chiusura (tastiere e serrature) si trovano nello stesso luogo fisico, ma manca della versatilità e della comodità offerte dalle configurazioni in rete che utilizzano eBox Apexx.

Sistemi di chiusura CenconX - Connessione USB

Per CenconX, le connessioni solo USB non sono consigliate per i sistemi CenconX che utilizzano la funzionalità OTC.

Configurazione di un singolo computer (TCP/IP)

Figura 5 mostra un'altra semplice configurazione che prevede un solo computer e un sistema di chiusura Axessor Apexx e/o un sistema di chiusura CenconX.

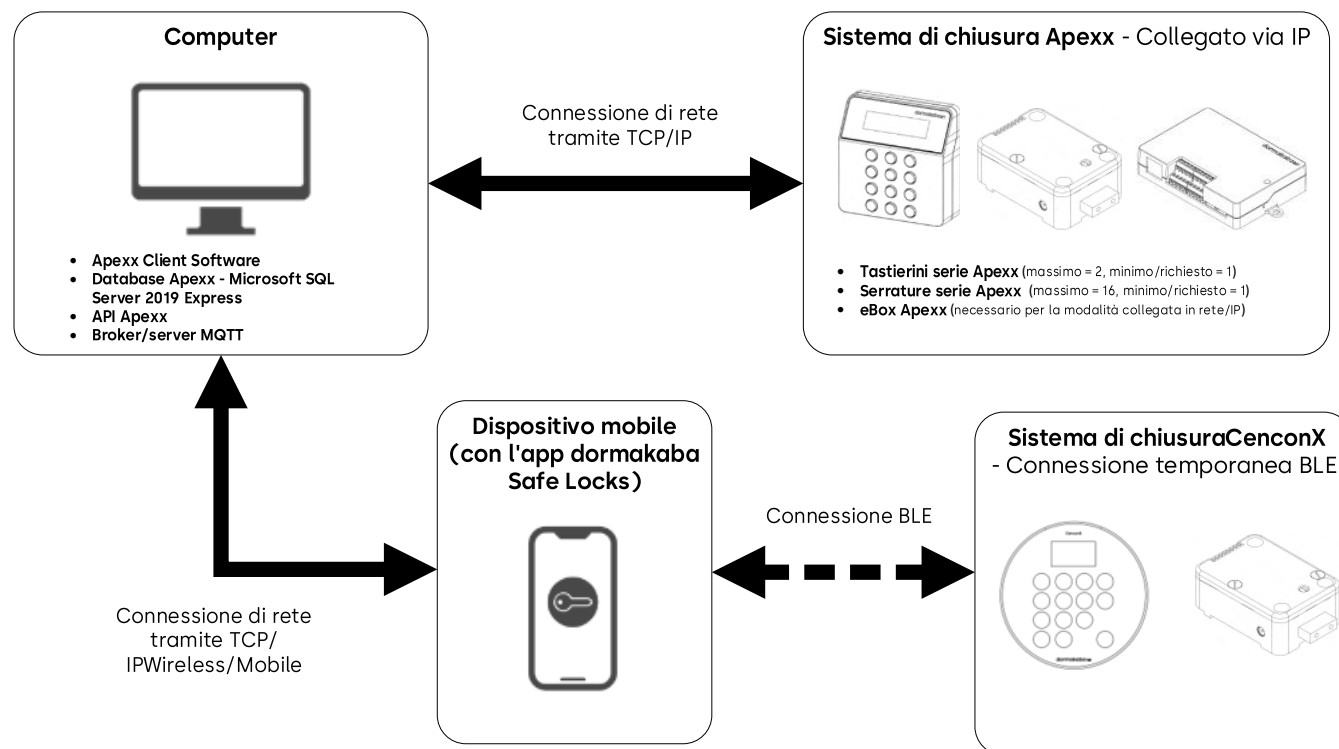


Figura 5 - Configurazione di un singolo computer - Rete tramite eBox (TCP/IP) e mobile

Sistemi di chiusura Axessor Apexx - Configurazione di un singolo computer (TCP/IP)

L'eBox Apexx serve a fornire una connessione di rete/IP per la comunicazione continua/live tra il computer e il sistema di chiusura Axessor Apexx.

Per i sistemi di chiusura Axessor Apexx, questa configurazione è utile anche per le installazioni più piccole in cui tutte le apparecchiature si trovano nella stessa sede fisica, ma l'inclusione dell'eBox consente all'amministratore del sistema di sfruttare tutte le funzionalità offerte da una connessione IP attiva (audit in tempo reale, monitoraggio attivo del sistema, aggiornamenti remoti del firmware e altre funzionalità hardware/software aggiuntive).

Sistemi di chiusura CenconX - Configurazione di un singolo computer (TCP/IP)

Per il sistema di chiusura CenconX, il dispositivo mobile si collega al server/client del computer tramite una connessione di rete/IP e una connessione temporanea BLE "ponte" collega il dispositivo mobile al sistema di chiusura CenconX.

Configurazioni di più computer

Per sedi più grandi che coinvolgono edifici di dimensioni maggiori e/o sistemi di chiusura multipli, la configurazione di più computer mostrata in Figura 6 offre una maggiore flessibilità.

Nota: Nel sistema sono ammessi solo un'API, un broker MQTT e un database SQL Server.

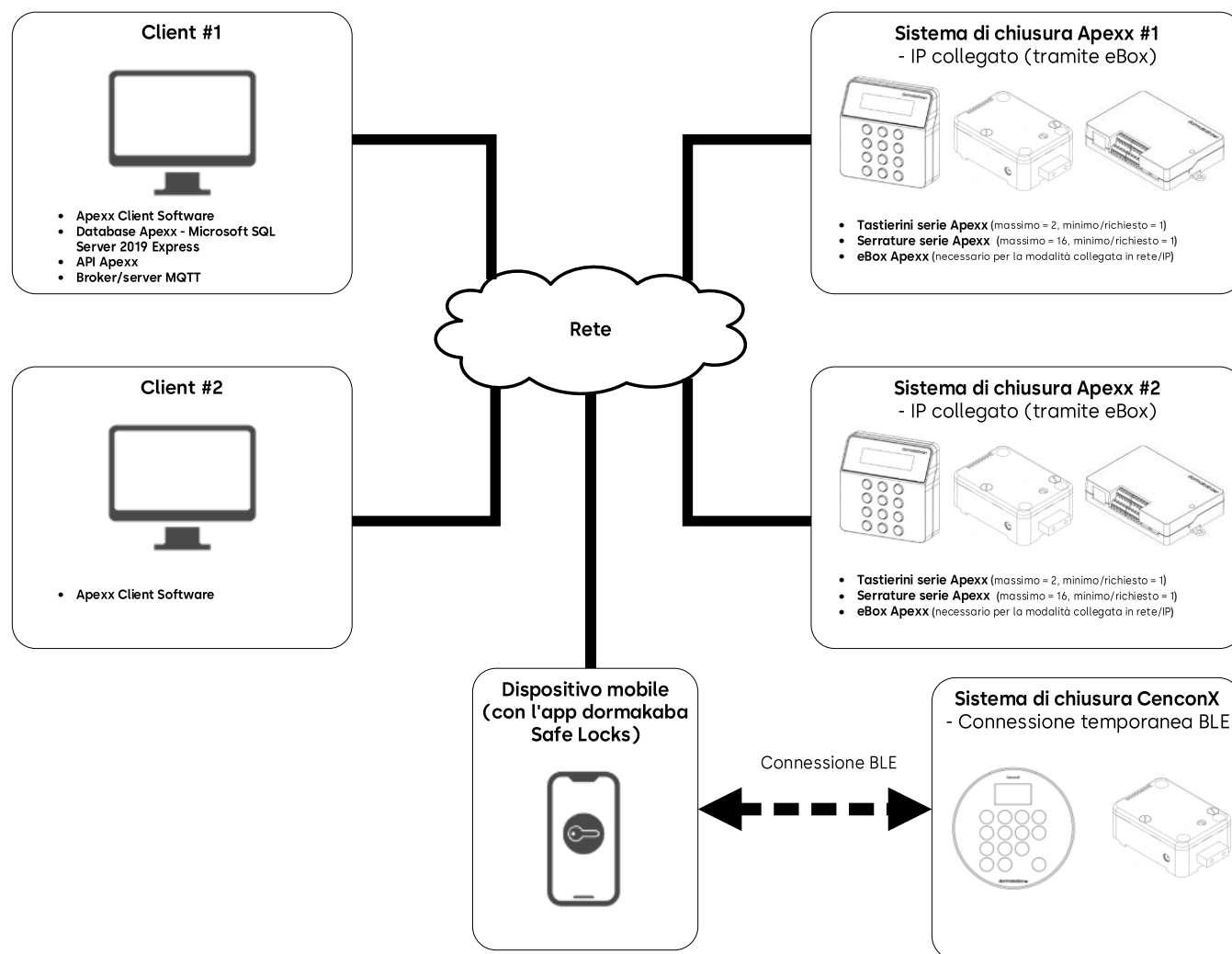


Figura 6 - Configurazione di più computer con più sistemi di chiusura

In questa configurazione, tutti i componenti del software possono essere installati su uno o più computer (o macchine virtuali), per una maggiore comodità e flessibilità nell'esecuzione e nella configurazione dei sistemi di chiusura. Si noti che ogni sistema di chiusura Axessor Apexx si collega alla rete tramite un eBox Apexx.

Questo concetto viene ulteriormente ampliato nel sistema illustrato in Figura 7, che comprende più computer e sistemi di chiusura distribuiti in più edifici.

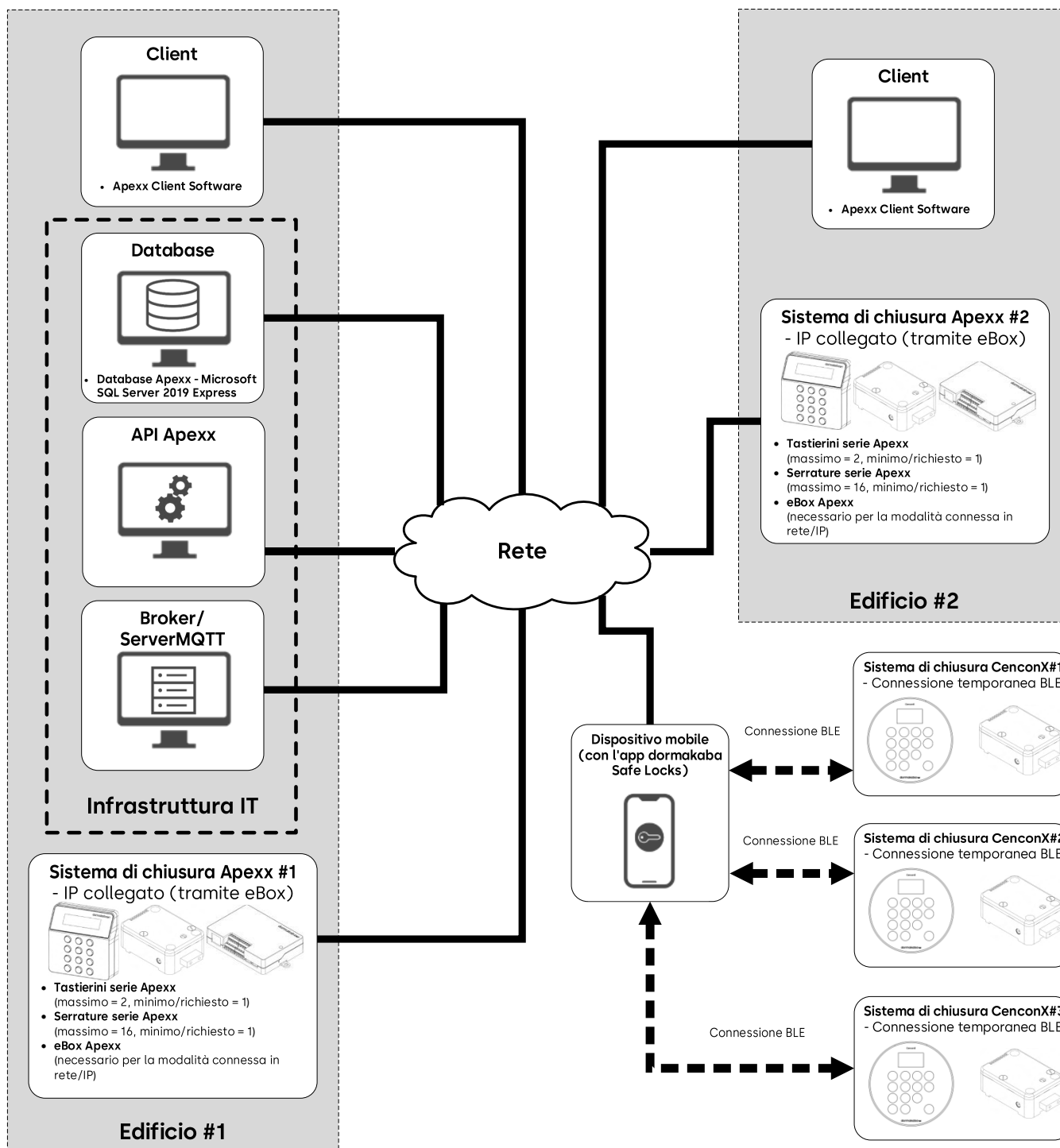


Figura 7 - Configurazione di più computer/sistema di chiusura con impostazione multi-server

Una differenza notevole tra questa configurazione e tutte le altre è che comprende più computer che ospitano diversi componenti software. Si noti come due dei computer dell'edificio #1 ospitino rispettivamente l'Apexx API e il database Apexx. Questi due computer possono essere configurati per essere utilizzati come API e database per i sistemi di chiusura dell'edificio #1, dell'edificio #2 e/o di qualsiasi altro sistema di chiusura dell'intera rete.

Questo esempio finale illustra che sono possibili diverse configurazioni a seconda delle esigenze organizzative e della configurazione dell'infrastruttura IT.

Considerazioni sul database

Il software della serie Apexx include Microsoft SQL Server 2019 Express come motore di database interno dedicato.

	Microsoft SQL Server 2019 Express (64 bit)
Limite del database	10 GB
Numero di CPU	1 processore fisico
RAM	1 GB
Sistemi operativi supportati	Windows 10, Windows Server 2016, Windows Server 2019

Specifiche minime consigliate per il computer Apexx

*Considerare il raddoppio per le installazioni più grandi

Stazione di lavoro Client Apexx

- Processore da 2,0 GHz con 4 core*
- 16 GB di RAM
- Disco rigido da 500 GB
- Windows 10 Professional 64bit

Server Broker Apexx

- Processore da 2,0 GHz con 4 core*
- 16 GB di RAM
- Disco rigido da 500 GB
- Windows 2019 Server Standard 64bit

Server di database Apexx e API Apexx

- Processore da 2,0 GHz con 6 core*
- 32 GB di RAM*
- Disco rigido da 1 TB
- Windows 2019 Server Standard 64bit
- Microsoft SQL Server Standard o Enterprise

Nota: Se lo si desidera, uno qualsiasi dei componenti software (client, database, API o MQTT Broker) può essere ospitato su una macchina virtuale.

Specifiche del dispositivo mobile Apexx

(Alla data di pubblicazione del documento)

- Sistema operativo mobile: Android 8+ o iOS 15+
- Deve essere compatibile con BLE

Nota: Consultare Google Play e Apple Store per le ultime versioni dell'applicazione mobile Safe Locks di dormakaba e per le informazioni sulla compatibilità dei dispositivi/OS.

Guida alla sicurezza informatica di Apexx

Note sul software locale

- Tutte le parti del software (MQTT, client e API) sono progettate come applicazioni Windows. Per poterle utilizzare in un ambiente cloud, bisogna essere in grado di gestire i canali di comunicazione tra di esse.
- I canali di comunicazione vengono stabiliti durante l'installazione: si basano su DNS (o indirizzi IP statici). Una volta completata l'installazione, verranno creati dei certificati a scopo di sicurezza. Questi certificati devono essere gestiti in modo appropriato per evitare qualsiasi attacco.
- La comunicazione da e verso il sistema di chiusura avviene tramite MQTT su SSL, pertanto le porte standard devono essere raggiungibili.
- Per funzionare, il software richiede il sottosistema dei certificati di Windows e un database SQL19.
- Il software non è supportato su sistemi Mac o Linux.
- Gli ambienti cloud testati sono Azure e AWS.
- Lo stesso utente non può accedere a più client contemporaneamente.

Accoppiamento del software locale con eBox (Axessor Apexx)

Il software locale e eBox Apexx devono essere accoppiati prima di poter stabilire una connessione. In caso di installazione di un nuovo eBox:

1. L'eBox è fisicamente installato sul CAN bus.
2. Un utente autorizzato deve accedere al tastierino e mettere in servizio l'eBox sul bus CAN (nessun dispositivo non autorizzato può ascoltare il bus CAN).
3. Dopo la messa in servizio, l'eBox sarà in grado di ottenere le chiavi di crittografia del CAN bus (AES-256 con chiavi specifiche del sistema).
4. Una volta che l'eBox è sul CAN bus, è necessario effettuare il collegamento con il software locale. L'indirizzo IP può essere visualizzato e modificato nelle impostazioni di rete del menu avanzato del tastierino. Se esiste un'impostazione, verrà utilizzata. Altrimenti, l'eBox assumerà il protocollo DHCP per ottenere l'indirizzo IP.
5. Se le impostazioni Ethernet sono valide, l'eBox tenterà di connettersi al server MQTT nel software locale (tramite comunicazione IP diretta in base alle impostazioni, oppure tramite broadcast sulla rete locale in caso di DHCP). Questo avviene tramite TLS.
6. Se il software locale rileva un nuovo eBox, è necessario autorizzarlo nel software prima di effettuare il login con il codice di riscatto. Una volta autorizzato l'eBox sul software, quest'ultimo produrrà un PIN di verifica che dovrà essere convalidato sul tastierino (Verifica del software all'eBox e dell'eBox al software).

7. Dopo la verifica del sistema, viene stabilito un canale sicuro. A tal fine si utilizzano certificati firmati in fabbrica preinstallati (infrastruttura PKI). Tutte le comunicazioni successive sono crittografate con TLS.
8. TLS 1.2. Inoltre, eBox comunica inizialmente sulla porta TCP 5001 (API) per verificare che il software sia attivato, quindi sulla porta 8883 (predefinita) per la comunicazione.
9. Affinché l'eBox si attivi correttamente, è necessario che il software sia attivato e che disponga di certificati adeguati. Il software non attivato provoca un'interruzione del servizio.

Per ulteriori informazioni sull'installazione, il collegamento e la configurazione di eBox Apexx, consultare la Guida all'installazione di Axessor Apexx (documento n. 801.0622), la Guida all'uso del sistema di tastiere della serie Apexx (documento n. 802.0622) e il menu di aiuto del software della serie Apexx.

Recupero in caso di catastrofe

Il software locale si collega al database SQL19 per la memorizzazione dei dati (SQL19 Express di Microsoft - riferimento: <https://www.microsoft.com/en-ca/sql-server/sql-server-2019-pricing>). La configurazione del database deve essere inserita nel software locale sotto forma di file di configurazione. La crittografia/protezione e il recupero dei dati seguiranno quindi il percorso del database SQL19. Si prevede che il database sia gestito dal dipartimento IT locale.

Il percorso di recupero sarà quindi quello di reinstallare l'API, MQTT e il client con una nuova copia da dormakaba o utilizzando un backup locale. Tutti i dati sono nel database SQL. API, MQTT e il client non memorizzano alcun dato della serratura o dell'utente, ma solo le impostazioni di connessione e configurazione.

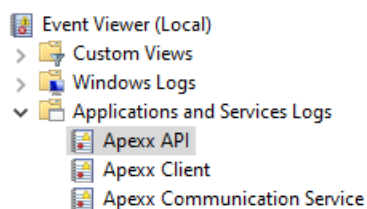
Il database viene creato automaticamente dal servizio API per la prima volta. Il database utilizza i login predefiniti specifici del servizio (API o BROKER) NT Service e si autentica tramite i canali Kerberos. Le impostazioni predefinite del DB sono Autenticazione Windows, colonne crittografate. Si consiglia, ma non si richiede, la crittografia a livello di motore.

Visualizzazione ed esportazione dei registri eventi Apexx



Il "Visualizzatore eventi" di Windows può essere utilizzato per visualizzare e risolvere i problemi relativi alle applicazioni e ai servizi Apexx.

1. Aprire Visualizzatore eventi > digitare "**Visualizzatore eventi**" nella barra di ricerca di Windows, quindi aprire il programma.
2. Fare clic sulla freccia accanto a > 📁 "**Registri applicazioni e servizi**" per espandere l'elenco.
3. Fare clic sull'applicazione/servizio Apexx per visualizzare tutti gli eventi relativi a tale applicazione o servizio (Apexx API, Apexx Client, Apexx Communication Service).



4. Da qui è possibile ordinare gli eventi in base all'ora, all'id dell'evento e così via, per facilitare la visualizzazione e la risoluzione dei problemi relativi alla configurazione di Apexx.
5. Esportazione dei registri eventi Apexx > Sotto "**Azioni**", è possibile scegliere  "**Salva tutti gli eventi come...**" per esportare i registri eventi dell'applicazione/servizio selezionato e salvarli in uno dei diversi formati (.evtx, .xml, .txt, .csv).

Punti salienti

1. Solo i server con il software locale devono essere indirizzabili via IP, mentre l'eBox no.
2. La comunicazione tra l'eBox e il software locale (traffico su intranet/Internet) è criptata con TLS.
3. Includere il server SQL nel piano di recupero in caso di catastrofe. Questo database è fondamentale per il funzionamento del sistema.



Access Automation Solutions

Entrance Automation
Entrance Security



Access Control Solutions

Electronic Access & Data
Escape and Rescue Systems
Lodging Systems



Access Hardware Solutions

Door Closers
Architectural Hardware
Mechanical Key Systems



Services

Technical Support
Installation and commissioning
Maintenance and Repair



Key & Wall Solutions

Key Systems
Movable / Sliding Walls



Safe Locks

Electronic Safe Locks
Mechanical Safe Locks
Boltworks and Accessories



Glass systems

Manual door systems
Glass fittings
Horizontal Sliding Walls

Il nostro impegno per la sostenibilità

Ci impegniamo a promuovere uno sviluppo sostenibile lungo tutta la nostra catena del valore, in linea con le nostre responsabilità economiche, ambientali e sociali nei confronti delle generazioni presenti e future. La sostenibilità a livello di prodotto è un approccio importante e orientato al futuro nel settore dell'edilizia. Al fine di fornire informazioni quantificate dell'impatto ambientale di un prodotto durante il suo intero ciclo di vita, dormakaba fornisce Dichiarazioni Ambientali di Prodotto (EPD), basate su valutazioni olistiche del ciclo di vita..

<https://www.dormakabagroup.com/en/sustainability/product-declarations>.

Guida all'architettura del sistema Axessor Apexx e alla sicurezza IT - RevB
Soggetto a modifiche senza preavviso

Dormakaba SAL GmbH

Siemensstrasse 33
42551 Velbert
safelocks.de@dormakaba.com
T +49 2051 9111 0

dormakaba USA Inc.

1525 Bull Lea Road, Suite 100
Lexington, KY 460511
sales.safelocks.us@dormakaba.com
1-800-950-4744



AXESSOR APEXX IP
INSTALLATION AND
OPERATION GUIDES

dk.world/AxessorApexxIP

Axessor Apexx

Seria oprogramowania

Przewodnik po architekturze systemu i bezpieczeństwie IT dla
Axessor Apexx IP/CIT i CenconX



Spis treści

Architektura systemu Apexx	3
Przegląd	3
System zamków Axessor Apexx.....	3
System zamków CenconX	3
Urządzenia mobilne	4
Składniki API/oprogramowania	4
Apexx API.....	4
Oprogramowanie klienckie Apexx	4
Baza danych Apexx	4
Broker/serwer MQTT.....	5
SMTP	5
SSO.....	5
Konfiguracja użytkownika – Axessor Apexx.....	5
Konfiguracja użytkownika – CenconX	6
Konfiguracja użytkownika – Użytkownicy oprogramowania.....	6
Użytkownicy oprogramowania – Axessor Apexx.....	6
Użytkownicy oprogramowania – CenconX.....	7
Licencje.....	7
Metody aktualizacji oprogramowania układowego.....	7
Aktualizacje oprogramowania sprzętowego – System zamków Axessor Apexx	7
Aktualizacje oprogramowania sprzętowego – System zamków CenconX.....	8
Transmisja danych.....	9
Bezpieczeństwo i szyfrowanie danych	11
Infrastruktura klucza publicznego (PKI)	12

Konfiguracje sprzętu komputerowego	14
Konfiguracja pojedynczego komputera (połączenie USB)	14
Konfiguracja na jednym komputerze (TCP/IP)	15
Konfiguracje na wielu komputerach	16
Uwagi dotyczące bazy danych	18
Minimalne zalecane specyfikacje komputera Apexx	18
Specyfikacja urządzenia mobilnego Apexx	18
Przewodnik dotyczący bezpieczeństwa IT Apexx	19
Uwagi dotyczące lokalnego oprogramowania	19
Parowanie lokalnego oprogramowania z modułem eBox (Axessor Apexx)	19
Odzyskiwanie po awarii	20
Przeglądanie i eksportowanie dzienników zdarzeń Apexx	21
Najważniejsze wnioski	21

Architektura systemu Apexx

Przegląd

Oprogramowanie serii Apexx może służyć do zdalnego zarządzania i konfigurowania różnych aspektów systemów zamków Axessor Apexx i CenconX. W niniejszym dokumencie opisano aspekty architektury systemu, infrastruktury komputerowej i wymagań dotyczących korzystania z oprogramowania serii Apexx do obsługi i zarządzania systemami zamków Axessor Apexx i CenconX.

System zamków Axessor Apexx

Systemy blokujące Axessor Apexx składają się z 2 zabezpieczonych sieci komunikacyjnych: **magistrala Can systemu zamka** i **sieć API/oprogramowania**.

Magistrala CAN systemu zamka obsługuje następujące komponenty:

- **Klawiatury z serii Apexx** (maksimum = 2, minimum/wymagane = 1)
 - Używane jako interfejs użytkownika do dostępu i konfiguracji systemu zamka
- **Zamki z serii Apexx** (maksimum = 16, minimum/wymagane = 1)
 - Fizyczny zamek elektromechaniczny kontrolujący dostęp użytkownika do sejfu
- **Apexx eBox** (wymagany dla trybu sieciowego/połączenia IP)
 - Działa jako konwerter protokołu (IP na magistralę CAN) pomiędzy systemem zamków Axessor Apexx a API/oprogramowaniem
 - Działa również jako skrzynka I/O (wejście/wyjście)

System zamków CenconX

Systemy zamków CenconX składają się z 2 zabezpieczonych sieci komunikacyjnych: **system zamka** i **API/sieć oprogramowania**.

System zamka obsługuje następujące komponenty:

- **Klawiatury z serii CenconX** (1)
 - Używane jako interfejs użytkownika do dostępu i konfiguracji systemu zamka
- **Zamki z serii CenconX** (1)
 - Fizyczny zamek elektromechaniczny kontrolujący dostęp użytkownika do sejfu

Urządzenia mobilne

Aplikacja mobilna Safe Lock firmy dormakaba może być używana do łączenia się z systemami zamków Axessor Apexx i CenconX. Można ją bezpłatnie pobrać w Google Play i Apple Store, ale nie będzie działać, dopóki nie zostanie zarejestrowana za pomocą oprogramowania serii Apexx. Aby uzyskać informacje na temat korzystania z aplikacji mobilnej i sposobu rejestracji urządzenia mobilnego, należy zapoznać się z Podręcznikiem użytkownika systemu CenconX (dokument nr CX003.0524) i menu pomocy oprogramowania serii Apexx.

- **Systemy zamków Axessor Apexx** > Urządzenia Axessor Apexx z oprogramowaniem sprzętowym w wersji 2.1.x.x lub wyższej mogą współpracować z urządzeniami mobilnymi za pośrednictwem **aplikacji mobilnej** dormakaba **Safe Locks**.
- **Systemy zamków CenconX** > **Aplikacja mobilna** dormakaba **Safe Locks** stanowi pomost pomiędzy systemem zamków CenconX a interfejsem API/oprogramowaniem i służy jako sposób uwierzytelniania i otwierania zamków CenconX.

Składniki API/oprogramowania

API/oprogramowanie składa się z 4 głównych komponentów:

- Apexx API
- Oprogramowanie klienckie Apexx
- Baza danych Apexx – Microsoft SQL Server 2019 Express
- Broker/serwer MQTT

Uwaga: Serwer/klienta Apexx należy skonfigurować z wykorzystaniem publicznie dostępnego adresu IP, aby ułatwić komunikację z urządzeniami mobilnymi.

Apexx API

Interfejs programowania aplikacji (API) działa zarówno jako wydawca, jak i subskrybent w architekturze MQTT.

Oprogramowanie klienckie Apexx

Oprogramowanie klienckie Apexx („Oprogramowanie z serii Apexx”) to graficzny interfejs użytkownika (GUI), który umożliwia użytkownikom oprogramowania korzystanie z interfejsu API do wykonywania czynności w systemie Apexx/CenconX (zmiana ustawień systemu, przechowywanie/pobieranie danych itp.).

Klient Apexx obsługuje wielu użytkowników, ale nie obsługuje wielu użytkowników jednocześnie na jednym kliencie. Tylko jedna osoba może być zalogowana do pojedynczej instancji klienta w danym momencie.

Baza danych Apexx

Baza danych Apexx służy jako główna lokalizacja do przechowywania danych w systemie Apexx. Baza danych Apexx wykorzystuje zastrzeżony system zarządzania relacyjnymi bazami danych Microsoft SQL Server 2019 Express jako środek do przechowywania i pobierania danych systemowych.

Broker/serwer MQTT

Message Queuing Telemetry Transport (MQTT) to protokół przesyłania wiadomości, który wykorzystuje model publikuj-subskrybuj w celu ułatwienia komunikacji między urządzeniami. Broker/serwer MQTT działa jako scentralizowane centrum przesyłania wiadomości i wykorzystuje protokół MQTT do zarządzania komunikacją między urządzeniami. Zwłaszcza protokół MQTT przekazuje wiadomości między oprogramowaniem klienckim Windows a modułem eBox.

SMTP

Oprogramowanie serii Apexx wykorzystuje protokół SMTP (Simple Mail Transport Protocol) do wysyłania następujących wiadomości: aktywne alerty, zaplanowane raporty i informacje o konfiguracji urządzenia mobilnego.

- Aktywne alerty są wysyłane do odbiorców na podstawie wystąpienia jednego lub więcej zdarzeń audytu wybranych przez użytkownika oprogramowania.
- Zaplanowane raporty mogą być wysyłane do odbiorców pocztą elektroniczną w oparciu o harmonogram zdefiniowany przez użytkownika, również przy użyciu protokołu SMTP.
- Podczas dodawania nowego urządzenia mobilnego w oprogramowaniu serii Apexx istnieje możliwość użycia wygenerowanego kodu QR do jego konfiguracji. Po zeskanowaniu kodu QR za pomocą aplikacji mobilnej Safe Locks system wykorzystuje protokół SMTP w celu wysłania informacji konfiguracyjnych do urządzenia mobilnego.
- Dodatkowe informacje na temat konfigurowania ustawień SMTP można znaleźć w menu pomocy oprogramowania serii Apexx.

SSO

Oprogramowanie serii Apexx wykorzystuje funkcję pojedynczego logowania, zapewniając, że użytkownik oprogramowania może użyć swoich danych uwierzytelniających do zalogowania się do interfejsu API przy użyciu jednego zestawu danych uwierzytelniających.

Konfiguracja użytkownika – Axessor Apexx

Użytkownicy systemu Axessor Apexx dzielą się na dwie różne kategorie: ***Użytkownicy zamków sejfowych*** i ***użytkownicy oprogramowania***

Użytkownicy zamków sejfowych to użytkownicy, którzy będą korzystać z systemu zamków Axessor Apexx (składającego się z fizycznych klawiatur, zamków i modułów eBox) oraz będą mieli unikalne poświadczenia i role z uprawnieniami, które dyktują ich dostęp do systemu zamków.

Użytkownicy zamków sejfowych używają numerycznych identyfikatorów użytkownika i kodów PIN, aby uzyskać dostęp do systemu zamka za pomocą klawiatury serii Apexx. Ten tryb działa funkcjonuje pod nazwą Tryb bankowy (lub Tryb statyczny).

Trzy domyślne typy użytkowników zamków sejfowych (Administrator, Menedżer i Użytkownik) tworzą hierarchię użytkowników, z których każdy ma wstępnie zdefiniowane role i uprawnienia w systemie blokowania. Oprócz tych typów użytkowników, za pomocą narzędzi administracyjnych oprogramowania serii Apexx można utworzyć dodatkowe role użytkownika zamków sejfowych, które mają uprawnienia zdefiniowane przez użytkownika oprogramowania. Te dodatkowe role użytkowników tworzone są przy użyciu struktury początkowych 3 rodzajów typów użytkowników, co pozwala, aby nowe typy użytkowników spełniały potrzeby klienta w zakresie personalizacji.

Urządzenia Axessor Apexx z oprogramowaniem sprzętowym w wersji 2.1.x.x lub wyższej wprowadzają dodatkowe typy użytkowników (administrator główny i administrator lokatora), a także dwa dodatkowe Tryby użytkownika (Tryb OTC i Tryb ICS), które obejmują korzystanie z urządzeń mobilnych w celu uzyskania dostępu do zamka. Więcej informacji na temat typów i trybów użytkownika blokady bezpieczeństwa można znaleźć w Przewodniku użytkownika systemu klawiatur serii Apexx (dokument nr 802.0622).

Konfiguracja użytkownika – CenconX

Użytkownicy systemu Axessor Apexx dzielą się na dwie różne kategorie: **Użytkownicy zamków sejfowych** i **użytkownicy oprogramowania**

Użytkownicy zamków sejfowych to użytkownicy, którzy będą korzystać z systemu zamków CenconX (składającego się z fizycznych klawiatur, zamków itp.) i będą mieli unikalne poświadczenia i role z uprawnieniami, które definiują ich dostęp do systemu zamków.

Typy użytkowników zamków sejfowych w systemach CenconX obejmują administratorów, menedżerów, użytkowników statycznego kodu PIN (Tryb bankowy) i użytkowników OTC (kod jednorazowy). Dodatkowe informacje na temat typów użytkowników i ich uprawnień można znaleźć w Przewodniku użytkownika systemu CenconX (dokument nr CX003.0524).

Konfiguracja użytkownika – Użytkownicy oprogramowania

Pojęcie **Użytkownicy oprogramowania** odnosi się do użytkowników, którzy uruchamiają oprogramowanie serii Apexx i używają narzędzi oprogramowania do wykonywania zadań zarządzania i administrowania. W przeciwieństwie do użytkowników sejfów, użytkownicy oprogramowania nie mają bezpośredniego dostępu do fizycznego systemu zamków (otwieranie/zamykanie drzwi sejfów), ale wykonują zadania administracyjne/zarządzające za pośrednictwem oprogramowania (dodawanie użytkowników zamków, resetowanie haseł użytkowników zamków).

Użytkownicy oprogramowania używają danych uwierzytelniających, aby uzyskać dostęp do oprogramowania serii Apexx za pomocą pojedynczego logowania (SSO). Inne typy uwierzytelniania dla użytkowników oprogramowania serii Apexx obejmują uwierzytelnianie systemu Windows (z wyjątkiem Entra ID), uwierzytelnianie domeny Windows i Google OAuth 2.0.

Użytkownicy oprogramowania posiadający uprawnienie użytkownika oprogramowania do zapisu mogą dodawać nowych użytkowników oprogramowania i konfigurować uprawnienia do odczytu/zapisu.

Użytkownicy oprogramowania – Axessor Apexx

Typy użytkowników oprogramowania w systemach Axessor Apexx obejmują administratorów i menedżerów. W przypadku zastosowań do transportu gotówki, dyspozytorzy i użytkownicy tylko do inspekcji również mają do odegrania rolę (**uwaga:** wymagane jest oprogramowanie sprzętowe urządzenia 2.1.x.x lub nowsze).

Więcej informacji na temat typów użytkowników oprogramowania i uprawnień można znaleźć w menu pomocy oprogramowania serii Apexx.

Użytkownicy oprogramowania – CenconX

Typy użytkowników oprogramowania w systemach CenconX obejmują administratorów, menedżerów, dyspozytorów i użytkowników tylko do inspekcji. Dodatkowe informacje na temat typów użytkowników i ich uprawnień można znaleźć w Przewodniku użytkownika systemu CenconX (dokument nr CX003.0524).

Podczas konfigurowania systemu zamków CenconX można skonfigurować pojedynczego klienta/bazę danych dla jednego właściciela (głównego dyspozytora) lub można wprowadzić drugiego klienta/bazę danych, aby umożliwić dodatkowemu dyspozytorowi współdzieloną kontrolę nad zarządzaniem systemem i dostępem do niego. Dodatkowe informacje można znaleźć w Podręczniku użytkownika systemu CenconX (dokument nr CX003.0524).

Licencje

Oprogramowanie serii Apexx oferuje wiele rodzajów licencji, z których każda odblokowuje różne funkcje i cechy oprogramowania. Więcej informacji można znaleźć w cennikach Axessor Apexx IP i CenconX.

Metody aktualizacji oprogramowania układowego

Proces aktualizacji oprogramowania układowego urządzenia Axessor Apexx różni się w zależności od zakupionej licencji.

Więcej informacji na temat procesu aktualizacji oprogramowania układowego można znaleźć w Przewodniku użytkownika systemu Axessor Apexx (dokument nr 802.0622), Przewodniku użytkownika CenconX (dokument nr CX003.0524) oraz w menu pomocy oprogramowania serii Apexx.

Aktualizacje oprogramowania sprzętowego – System zamków Axessor Apexx

Lokalne aktualizacje oprogramowania układowego można wykonać poprzez ustanowienie tymczasowego połączenia USB między komputerem z oprogramowaniem serii Apexx a klawiaturą systemu zamka.

Zdalne aktualizacje oprogramowania sprzętowego można wykonać z wykorzystaniem połączenia sieciowego za pośrednictwem modułu eBox. Jest to proces składający się z trzech etapów:

1. Użytkownik oprogramowania inicjuje proces zdalnej aktualizacji oprogramowania układowego, przesyłając oprogramowanie układowe z interfejsu API/oprogramowania do systemu blokującego za pośrednictwem skrzynki eBox.
2. Oprogramowanie układowe jest pobierane i zapisywane w systemie zamykania. Na wyświetlaczu klawiatury pojawi się komunikat informujący użytkowników zamków sejfowych, że trwa aktualizacja oprogramowania układowego.
3. Użytkownik zamka sejfowego wprowadza prawidłowe dane uwierzytelniające (identyfikator użytkownika i kod PIN) na klawiaturze, a następnie inicjuje aktualizację oprogramowania układowego.

Aktualizacje oprogramowania sprzętowego – System zamków CenconX

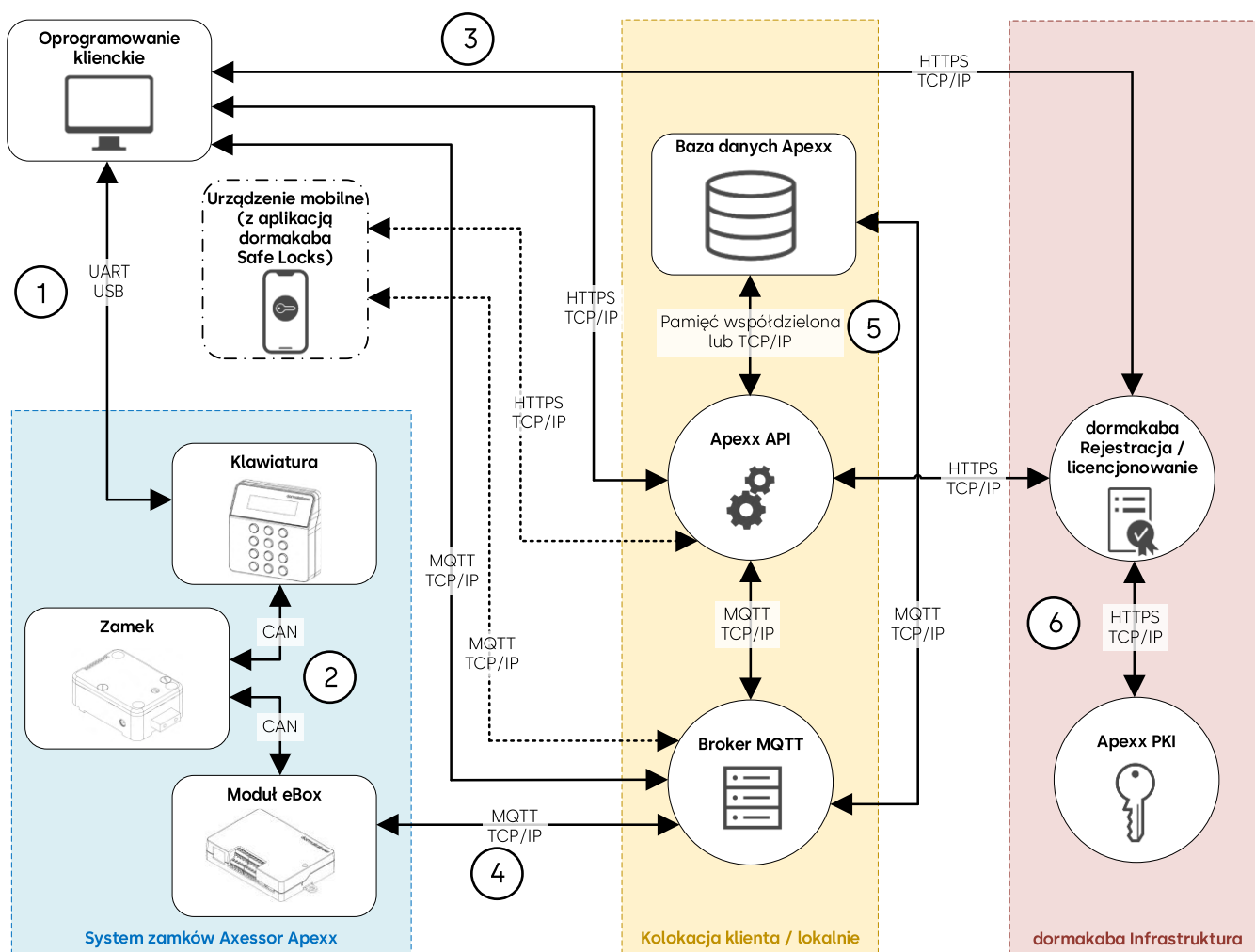
Lokalne aktualizacje oprogramowania układowego można wykonać poprzez ustanowienie tymczasowego połączenia USB między komputerem z oprogramowaniem serii Apexx a klawiaturą systemu zamka.

Użytkownicy urządzeń mobilnych CenconX mają również możliwość **mobilnej aktualizacji oprogramowania** układowego, która zakłada wykorzystanie aplikacji mobilnej Safe Locks firmy dormakaba do otrzymywania aktualizacji oprogramowania układowego. Proces ten polega na wykorzystaniu oprogramowania serii Apexx do wysyłania plików aktualizacji oprogramowania układowego na urządzenie mobilne użytkownika. Użytkownik mobilny może następnie zalogować się do aplikacji Safe Locks, pobrać wymagane pliki, a potem zainicjować proces aktualizacji oprogramowania układowego za pomocą połączenia BLE między urządzeniem mobilnym a klawiaturą CenconX.

Transmisja danych

Rysunek 1 i towarzyszący mu wykres pokazują przepływ danych między różnymi komponentami sprzętowymi i programowymi systemu zamków Axessor Apexx.

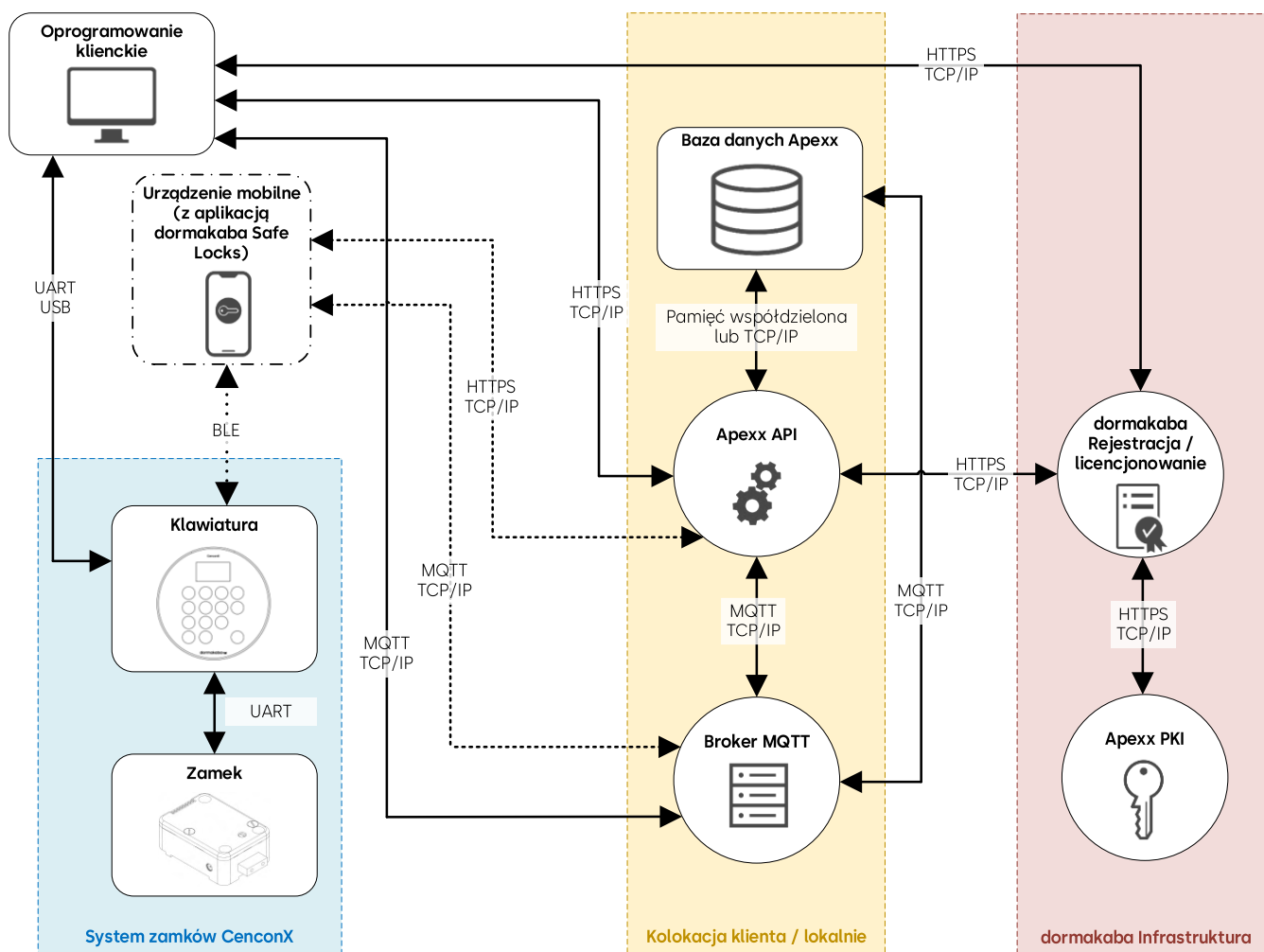
Port komunikacyjny	Opis
443	Ten port jest używany dla wychodzącego ruchu TCP/IP.
587	Ten port jest używany do komunikacji z hostem SMTP. Jest on wymagany i domyślnie ustawiony na 587.
5001	Jest to domyślny port używany do uruchamiania systemu zamków Apexx.
8883	Jest to domyślny port używany przez brokera MQTT.



Rysunek 1 – Architektura systemu Apexx w systemie zamków Axessor Apexx – komponenty systemu i transmisja danych

	Protokoły komunikacyjne	Przepływ danych	Opis / cel
1	UART przez USB	Ścieżka dwukierunkowa: Oprogramowanie klienckie do klawiatury	Bezpośrednia konfiguracja i pobieranie audytów
2	CAN	Ścieżka dwukierunkowa: - Klawiatura do zamka - Blokada do eBox	Komunikacja między urządzeniami
3	HTTPS przez TCP/IP	Ścieżka dwukierunkowa: Oprogramowanie klienckie do rejestracji/licencjonowania dormakaba	Licencjonowanie i rejestracja online
4	MQTT przez TCP/IP	Ścieżka dwukierunkowa: - Oprogramowanie klienckie dla brokera MQTT Ścieżka dwukierunkowa: - eBox do brokera MQTT Ścieżka dwukierunkowa: - Urządzenie z aplikacją mobilną dormakaba Safe Locks do brokera MQTT	Konfiguracja sieciowa i wyszukiwanie audytów
5	Pamięć współdzielona lub TCP/IP	Ścieżka dwukierunkowa: Apexx API do bazy danych Apexx	Trwałe przechowywanie danych za pomocą SQL Server
6	HTTPS przez TCP/IP	Ścieżka dwukierunkowa: - Oprogramowanie klienckie do Apexx API - Apexx API do dormakaba - Rejestracja/Licencjonowanie dormakaba - Rejestracja/licencjonowanie w Apexx PKI - Urządzenie z aplikacją mobilną dormakaba Safe Locks do Apexx API	Wydawanie certyfikatów x.509

Rysunek 2 przedstawia schemat podobny do tego przedstawionego na Rysunek 1, ale z systemem zamka CenconX zamiast systemu zamka Axessor Apexx. W tym przypadku urządzenie mobilne działa jako kanał komunikacyjny między systemem zamka CenconX a infrastrukturą oprogramowania.



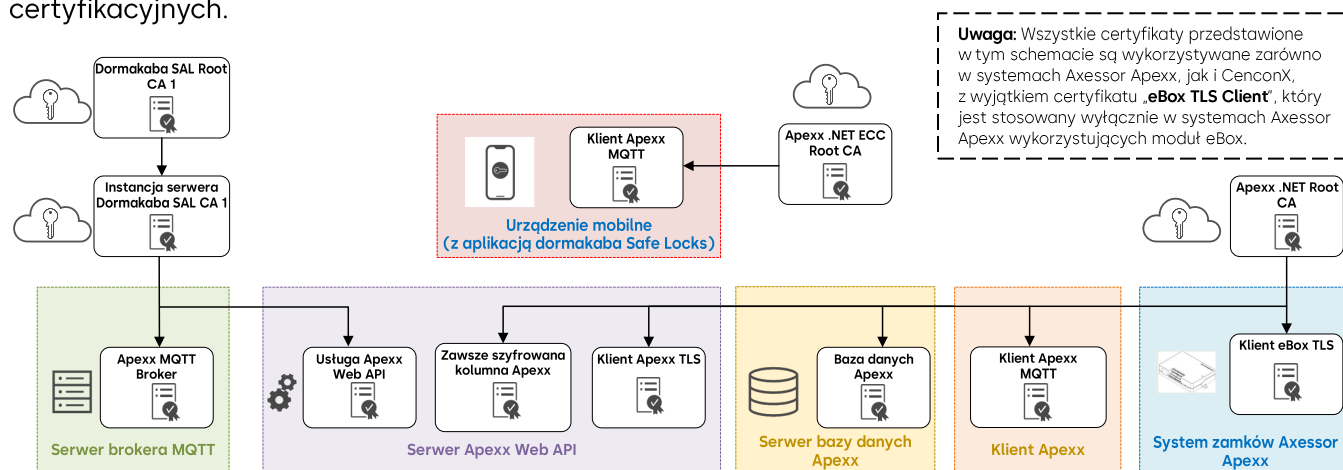
Rysunek 2 – Architektura systemu Apexx w systemie zamków CenconX – komponenty systemu i transmisja danych

Bezpieczeństwo i szyfrowanie danych

Oprogramowanie z serii Apexx, systemy zamków CenconX, systemy zamków Axessor Apexx i uruchomione urządzenia mobilne wykorzystują wiele metod szyfrowania, w tym certyfikaty AES256, PBKDF2 i TLS w celu zapewnienia bezpiecznej komunikacji i magazynowania danych.

Infrastruktura klucza publicznego (PKI)

Oprogramowanie z serii Apexx, systemy zamków CenconX, systemy zamków Axessor Apexx i uruchomione urządzenia mobilne wykorzystują infrastrukturę klucza publicznego do tworzenia, przechowywania i dystrybucji certyfikatów cyfrowych do urządzeń Apexx za pośrednictwem organów certyfikacyjnych.



Rysunek 3 – Infrastruktura klucza publicznego

Typ certyfikatu	Opis
Dormakaba SAL Root CA	- Certyfikat ten jest fabrycznie wgrany do urządzeń i wymieniany poprzez aktualizację oprogramowania układowego - W trakcie instalacji oprogramowania serii Apexx certyfikat ten jest także instalowany podczas uruchamiania pliku instalatora wymagań wstępnych na komputerach klienckich i serwerowych (pliki te przechowywane są w folderze Zaufane główne urzędy certyfikacji)
Instancja serwera dormakaba SAL CA	- Serwery uruchamiające lokalne usługi oprogramowania dla Apexx wymagają certyfikatów podpisanych przez dormakaba SAL PKI, aby urządzenia mogły im zaufać - Certyfikat ten musi zostać wdrożony na wszystkich serwerach z uruchomionymi lokalnymi usługami oprogramowania - W trakcie instalacji oprogramowania serii Apexx certyfikat ten jest także instalowany podczas uruchamiania pliku instalatora wymagań wstępnych na komputerach klienckich i serwerowych (pliki te przechowywane są w folderze Pośrednie urzędy certyfikacji)
Apexx MQTT Broker	- Utworzony podczas instalacji oprogramowania - Używany do połączeń TLS i uwierzytelniania
Usługa Web API Apexx	- Utworzona podczas instalacji oprogramowania - Zawiera nazwę serwera (komputer, na którym zainstalowana jest ta usługa), zaufaną instytucję certyfikującą i publiczny klucz szyfrowania serwera
Klient Apexx TLS	- Służy do uwierzytelniania klienta Apexx - Certyfikat jest zweryfikowanym użytkownikiem, jeśli wystawca jest zgodny z Apexx .NET Root CA zainstalowanym na serwerze brokera
Baza danych Apexx	- SQL Server w systemie Windows jest jedynym obsługiwanym silnikiem bazy danych - Następujące ustawienia są włączone w instancji/bazie danych: - Uwierzytelnianie systemu Windows - Kontrola dostępu oparta na rolach (RBAC) jest używana wraz z uwierzytelnianiem systemu Windows do kontrolowania uprawnień
Klient eBox TLS	- Służy do uwierzytelniania eBox - Certyfikat jest zweryfikowanym użytkownikiem, jeśli wystawca jest zgodny z Apexx .NET Root CA zainstalowanym na serwerze brokera

Typ certyfikatu	Opis
Apexx .NET Root CA	• Utworzony podczas instalacji oprogramowania i przechowywany w magazynie certyfikatów maszyny lokalnej w folderze Zaufane główne urzędy certyfikacji • Podczas procesu instalacji API jest on przechowywany w folderze Certyfikaty osobiste maszyny lokalnej (ML\Osobiste\Certyfikaty) • Każdy komputer z uruchomionym oprogramowaniem (klient, serwer, baza danych itp.) wymaga kopii tego certyfikatu do celów bezpieczeństwa/identyfikacji • Lokalne oprogramowanie PKI podpisuje żądania certyfikatów dla wszystkich klientów brokera MQTT • Certyfikaty te są używane zarówno do ustanawiania połączeń wzajemnego zaufania Transport Layer Security (TLS), jak i uwierzytelniania z brokerem MQTT • Może również podpisywać certyfikaty używane przez SQL Server dla TLS • Używa RSA do podpisów
Apexx .NET ECC Root CA	• Utworzony podczas instalacji oprogramowania i przechowywany w magazynie certyfikatów maszyny lokalnej w folderze Zaufane główne urzędy certyfikacji • Podczas procesu instalacji API jest on przechowywany w folderze Certyfikaty osobiste maszyny lokalnej (ML\Osobiste\Certyfikaty) • Każdy komputer z uruchomionym oprogramowaniem (klient, serwer, baza danych itp.) wymaga kopii tego certyfikatu do celów bezpieczeństwa/identyfikacji • Lokalne oprogramowanie PKI podpisuje żądania certyfikatów dla wszystkich klientów brokera MQTT • Certyfikaty te są używane zarówno do ustanawiania połączeń wzajemnego zaufania Transport Layer Security (TLS), jak i uwierzytelniania z brokerem MQTT • Może również podpisywać certyfikaty używane przez SQL Server dla TLS • Używa ECDSA do podpisów
Klient MQTT Apexx	• Utworzony podczas logowania klienta oprogramowania • Używany do połączeń TLS i uwierzytelniania
Zawsze szyfrowana kolumna Apexx	• Szyfrowanie danych na poziomie API, które trafiają do zaszyfrowanej kolumny w bazie danych • Podczas procesu instalacji API jest on przechowywany w folderze Certyfikaty osobiste maszyny lokalnej (ML\Osobiste\Certyfikaty)

Uwaga: Certyfikaty można odnowić 60 dni przed ich wygaśnięciem poprzez odnowienie licencji za pomocą narzędzia do rejestracji online Apexx Series Software.

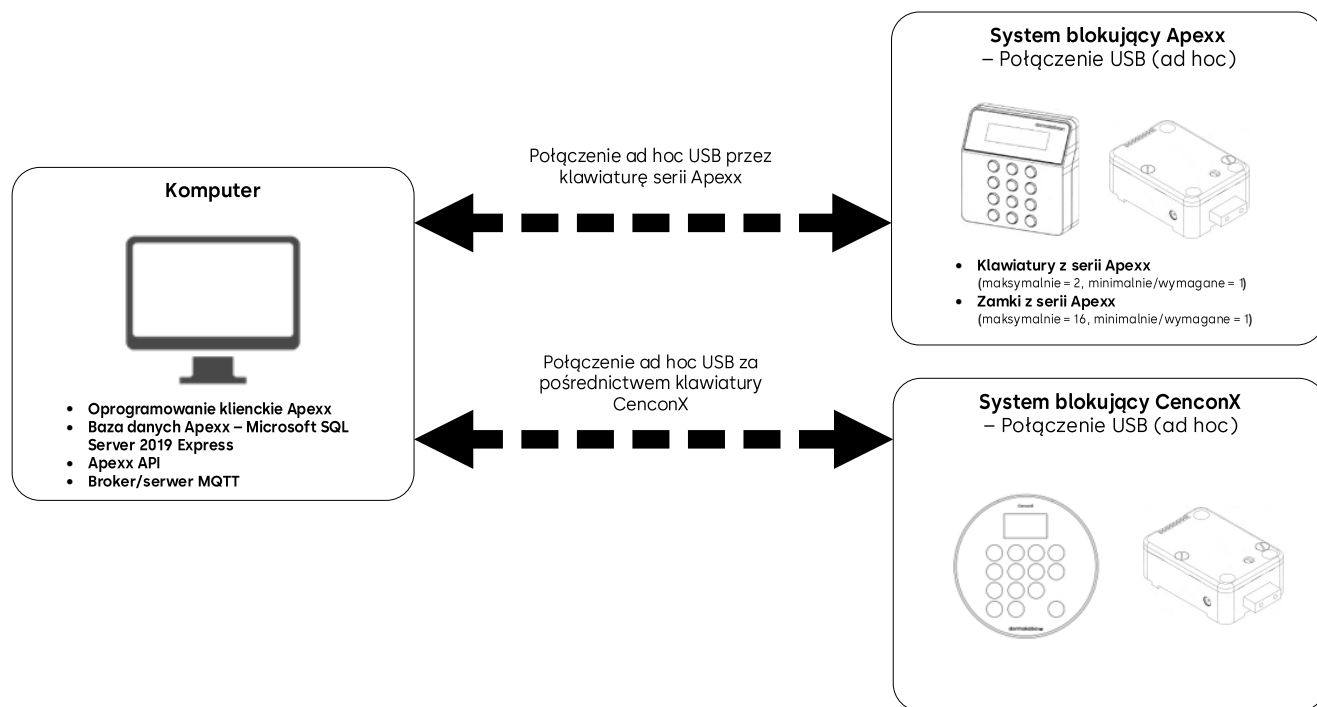
Konfiguracje sprzętu komputerowego

Sprzęt komputerowy/API/oprogramowanie systemu Apexx można skonfigurować na wiele sposobów, w zależności od złożoności systemu (liczby systemów blokujących Apexx, ich lokalizacji itp.). W tej sekcji przedstawiono tylko kilka z możliwych konfiguracji. Więcej informacji na temat wymagań licencyjnych dla różnych konfiguracji komputerowych/sprzętowych można znaleźć w cennikach Axessor Apexx lub CenconX.

Uwaga: W razie potrzeby każdy z komponentów oprogramowania (klient, baza danych, API lub MQTT) może być hostowany na maszynie wirtualnej.

Konfiguracja pojedynczego komputera (połączenie USB)

Rysunek 4 ilustruje podstawową konfigurację obejmującą tylko jeden komputer i jeden system blokujący Axessor Apexx i/lub system blokujący CenconX. W tej konfiguracji wszystkie elementy API/oprogramowania są hostowane na jednym komputerze z połączeniem USB używanym do tymczasowego połączenia z systemem blokującym Axessor Apexx lub CenconX w celu programowania/konfiguracji systemu.



Rysunek 4 – Konfiguracja pojedynczego komputera – połączenie USB ad hoc

Systemy zamków Axessor Apexx – Połączenie USB

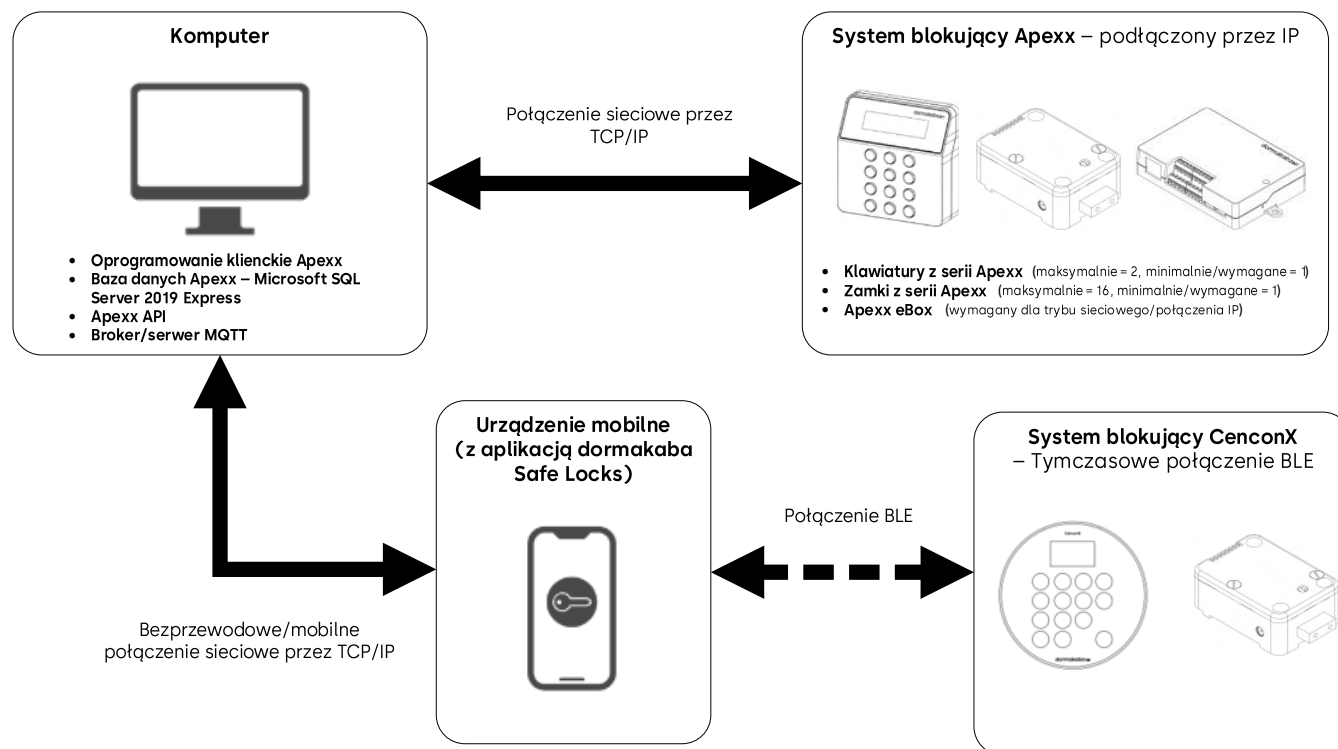
W przypadku Axessor Apexx ta konfiguracja sprawdza się dobrze w małych obiektach, w których komputer i wszystkie komponenty systemu blokującego (klawiatury i zamki) znajdują się w tej samej fizycznej lokalizacji, ale brakuje mu wszechstronności i wygody oferowanej przez konfiguracje sieciowe wykorzystujące Apexx eBox.

Systemy zamków CenconX – Połączenie USB

W przypadku CenconX połączenia tylko przez USB nie są zalecane dla systemów korzystających z funkcji OTC.

Konfiguracja na jednym komputerze (TCP/IP)

Rysunek 5 pokazuje inną prostą konfigurację obejmującą tylko jeden komputer i jeden system blokujący Axessor Apexx i/lub system blokujący CenconX.



Rysunek 5 – Konfiguracja na jednym komputerze – Sieć przez moduł eBox (TCP/IP)

Systemy zamków Axessor Apexx – Konfiguracja na jednym komputerze (TCP/IP)

Apexx eBox służy do zapewnienia łączności sieciowej/IP w celu ciągłej/bieżącej komunikacji między komputerem a systemem blokującym Axessor Apexx.

W przypadku systemów blokujących Axessor Apexx ta konfiguracja jest również przydatna w mniejszych konfiguracjach, w których cały sprzęt znajduje się w tej samej fizycznej lokalizacji, ale włączenie eBox pozwala administratorowi systemu korzystać ze wszystkich funkcji, które zapewnia aktywne połączenie IP (audyty na żywo, aktywne monitorowanie systemu, zdalne aktualizacje oprogramowania układowego i inne dodatkowe funkcje sprzętowe / programowe).

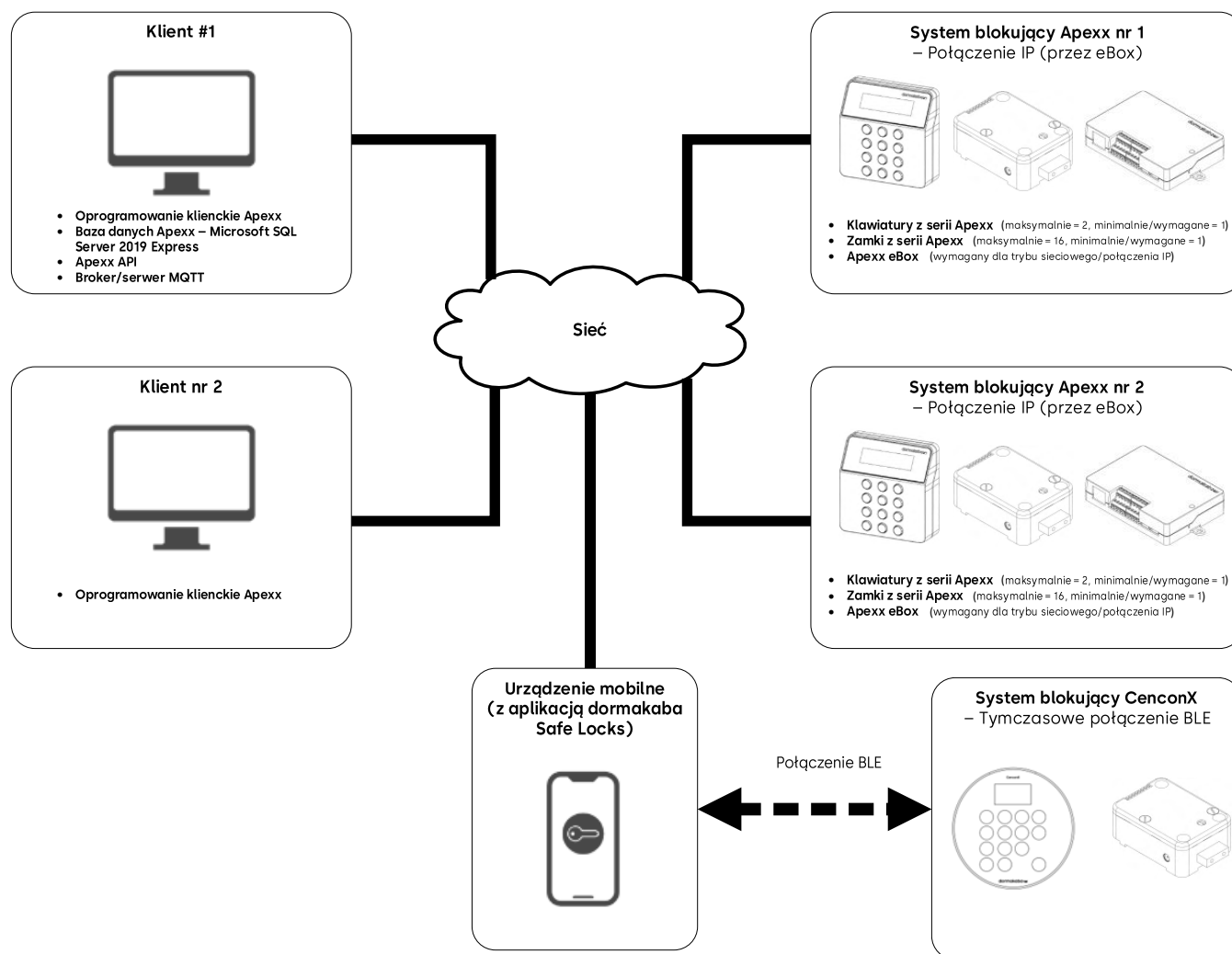
Systemy zamków CenconX – Konfiguracja na jednym komputerze (TCP/IP)

W przypadku systemu blokującego CenconX urządzenie mobilne łączy się z serwerem/klientem komputera za pośrednictwem połączenia sieciowego/IP, a tymczasowe połączenie „mostkowe” BLE łączy urządzenie mobilne z systemem blokującym CenconX.

Konfiguracje na wielu komputerach

W przypadku większych obiektów obejmujących duże budynki i/lub wiele systemów blokujących, konfiguracja na wielu komputerach pokazana na Rysunek 6 zapewnia dodatkową elastyczność.

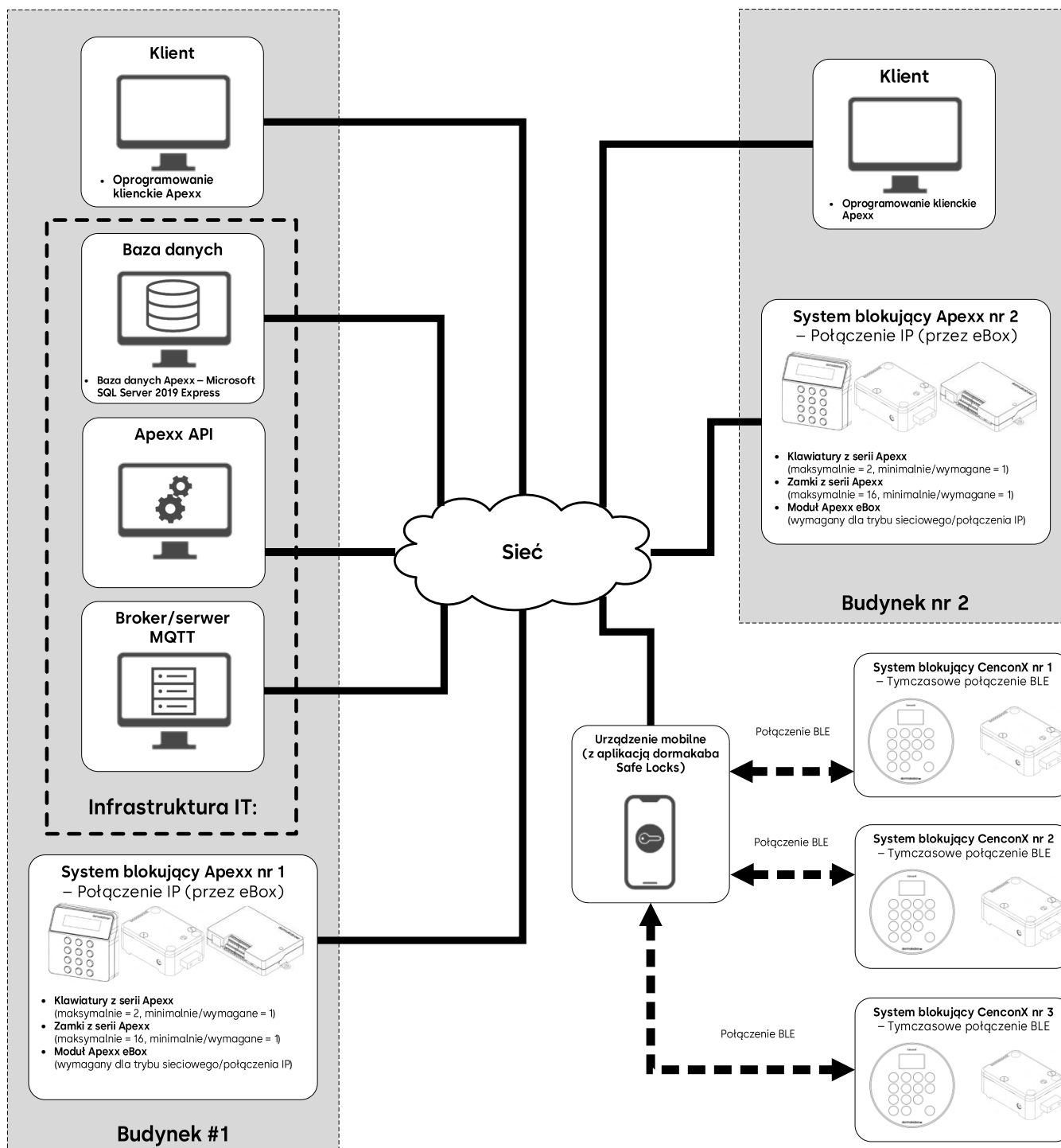
Uwaga: W systemie tym dozwolony jest tylko jeden interfejs API, broker MQTT i baza danych SQL Server.



Rysunek 6 – Konfiguracja na wielu komputerach i z wieloma systemami blokującymi

W takiej konfiguracji dowolny lub wszystkie komponenty oprogramowania mogą być zainstalowane na jednym lub kilku komputerach (lub maszynach wirtualnych), co pozwala na dodatkową wygodę i elastyczność, jeśli chodzi o uruchamianie i konfigurowanie systemów zamka. Należy pamiętać, że każdy system blokujący Axessor Apexx łączy się z siecią za pośrednictwem Apexx eBox.

Koncepcja ta jest dalej rozwijana w systemie pokazanym na Rysunek 7, który obejmuje wiele komputerów i systemów zamków rozmieszczonych w wielu budynkach.



Rysunek 7 – Konfiguracja na wielu komputerach/systemu blokującego z konfiguracją wielu serwerów

Jedną zauważalną różnicą między tą konfiguracją a wszystkimi innymi jest to, że obejmuje ona wiele komputerów obsługujących różne komponenty oprogramowania. Zwróć uwagę, że dwa komputery w Budyńku #1 obsługują odpowiednio Apexx API i bazę danych Apexx. Te dwa komputery można skonfigurować tak, aby służyły jako interfejs API i baza danych dla systemów zamykania w budynku nr 1, budynku nr 2 i/lub dowolnym innym systemie zamków w całej sieci.

Ostatni przykład ilustruje, że możliwe jest wiele różnych konfiguracji w zależności od potrzeb organizacyjnych i konfiguracji infrastruktury IT.

Uwagi dotyczące bazy danych

Oprogramowanie serii Apexx zawiera Microsoft SQL Server 2019 Express jako dedykowany wewnętrzny silnik bazy danych.

	Microsoft SQL Server 2019 Express (64-bitowy)
Limit bazy danych	10 GB
Liczba procesorów	1 procesor fizyczny
RAM	1 GB
Obsługiwane systemy operacyjne	Windows 10, Windows Server 2016, Windows Server 2019

Minimalne zalecane specyfikacje komputera Apexx

*Rozważ podwojenie tych wartości w przypadku większych instalacji.

Stacja robocza klienta Apexx

- Procesor 2,0 GHz z 4 rdzeniami*
- 16 GB RAM
- Dysk twardy 500 GB
- Windows 10 Professional 64bit

Apexx Broker Server

- Procesor 2,0 GHz z 4 rdzeniami*
- 16 GB RAM
- Dysk twardy 500 GB
- Windows 2019 Server Standard 64bit

Serwer bazy danych Apexx i interfejs API Apexx

- Procesor 2,0 GHz z 6 rdzeniami*
- 32 GB RAM*
- Dysk twardy 1 TB
- Windows 2019 Server Standard 64bit
- Microsoft SQL Server Standard lub Enterprise

Uwaga: W razie potrzeby każdy z komponentów oprogramowania (klient, baza danych, API lub broker MQTT) może być hostowany na maszynie wirtualnej.

Specyfikacja urządzenia mobilnego Apexx

(Stan na dzień publikacji dokumentu.)

- System operacyjny urządzenia mobilnego: Android 8+ lub iOS 15+
- Musi być kompatybilny z BLE

Uwaga: Sprawdź Google Play i Apple Store, aby uzyskać najnowsze wersje aplikacji mobilnej dormakaba Safe Locks oraz informacje o kompatybilności urządzeń/systemów operacyjnych.

Przewodnik dotyczący bezpieczeństwa IT Apexx

Uwagi dotyczące lokalnego oprogramowania

- Wszystkie części oprogramowania (MQTT, klient i API) zaprojektowano jako aplikacje systemu Windows. Aby móc z nich korzystać w środowisku chmurowym, istnieje konieczność zarządzania kanałami komunikacji między nimi.
- Kanały komunikacyjne są ustanawiane podczas instalacji – bazują na DNS (lub statycznych adresach IP). Po zakończeniu instalacji zostaną ustanowione certyfikaty dla celów bezpieczeństwa. Należy odpowiednio zarządzać tymi certyfikatami, aby zapobiec jakimkolwiek atakom.
- Komunikacja z i do systemu zamka odbywa się za pośrednictwem protokołu MQTT przez SSL, więc muszą być dostępne standardowe porty.
- Oprogramowanie wymaga do działania podsystemu certyfikatów Windows i bazy danych SQL19.
- Oprogramowanie nie jest obsługiwane w systemach Mac i Linux.
- Testowane środowiska chmurowe to Azure i AWS.
- Ten sam użytkownik nie może być zalogowany do wielu klientów jednocześnie.

Parowanie lokalnego oprogramowania z modułem eBox (Axessor Apexx)

Przed nawiązaniem połączenia należy sparować oprogramowanie lokalne i Apexx eBox. Kiedy trzeba zainstalować zupełnie nowy moduł eBox:

1. Moduł eBox jest fizycznie zainstalowany na magistrali CAN.
2. Upoważniony użytkownik musi zalogować się do klawiatury i uruchomić eBox na magistrali CAN (żadne nieautoryzowane urządzenia nie mogą nasłuchiwać magistrali CAN).
3. Po uruchomieniu modułu eBox będzie on w stanie uzyskać klucze szyfrowania magistrali CAN (AES-256 z kluczami specyficznymi dla systemu).
4. Gdy moduł eBox znajdzie się na magistrali CAN, należy nawiązać połączenie z oprogramowaniem lokalnym. W menu zaawansowanym ustawień sieciowych klawiatury można wyświetlić i zmienić adres IP. Jeśli istnieje takie ustawienie, zostanie ono użyte. W przeciwnym razie moduł eBox wykorzysta protokół DHCP w celu uzyskania adresu IP.
5. Po wprowadzeniu prawidłowych ustawień sieci Ethernet moduł eBox podejmie próbę połączenia się z serwerem MQTT w oprogramowaniu lokalnym (za pośrednictwem bezpośredniej komunikacji IP w oparciu o ustawienia lub transmisję w sieci lokalnej w przypadku DHCP). Odbywa się to za pośrednictwem protokołu TLS.

6. Jeśli oprogramowanie lokalne wykryje nowy moduł eBox, przed pomyślnym zalogowaniem musi on zostać autoryzowany w oprogramowaniu przy użyciu kodu roszczenia. Po autoryzacji modułu eBox w oprogramowaniu, wygeneruje ono kod PIN do weryfikacji, który należy zatwierdzić na klawiaturze (weryfikacja oprogramowania do eBox i eBox do oprogramowania).
7. Po zweryfikowaniu systemu ustanawiany jest bezpieczny kanał. Odbywa się to za pomocą fabrycznie zainstalowanych certyfikatów (infrastruktura PKI). Późniejsza komunikacja jest szyfrowana przy użyciu protokołu TLS.
8. TLS 1.2. eBox początkowo komunikuje się również przez port TCP 5001 (API) w celu zweryfikowania, czy oprogramowanie jest aktywne, a następnie przez port 8883 (domyślny) w celu komunikacji.
9. Oprogramowanie musi być aktywowane i posiadać odpowiednie certyfikaty, aby moduł eBox został prawidłowo aktywowany. Nieaktywne oprogramowanie spowoduje blokadę usługi.

Więcej informacji na temat instalacji, podłączania i konfigurowania Apexx eBox można znaleźć w instrukcji instalacji Axessor Apexx (dokument nr 801.0622), instrukcji obsługi systemu klawiatury serii Apexx (dokument nr 802.0622) oraz w menu pomocy oprogramowania serii Apexx.

Odzyskiwanie po awarii

Oprogramowanie lokalne łączy się z bazą danych SQL19 w celu przechowywania danych (SQL19 Express firmy Microsoft – dodatkowe informacje: <https://www.microsoft.com/en-ca/sql-server/sql-server-2019-pricing>). Konfiguracja bazy danych musi zostać wprowadzona do oprogramowania lokalnego w postaci pliku konfiguracyjnego. Szyfrowanie/ochrona i odzyskiwanie danych będą następnie podążać ścieżką bazy danych SQL19. Oczekuje się, że lokalny dział IT będzie zarządzać bazą danych.

W takim wypadku ścieżka odzyskiwania będzie polegała na ponownej instalacji API, MQTT i klienta albo ze świeżej kopii od firmy dormakaba, albo z wykorzystaniem lokalnej kopii zapasowej. Wszystkie dane są przechowywane w bazie danych SQL. API, MQTT i klient nie przechowują żadnych danych zamka ani użytkownika, a jedynie ustawienia połączenia i konfiguracji.

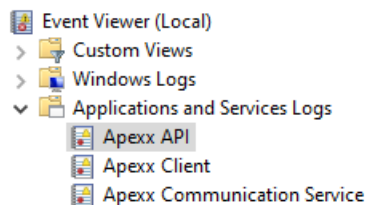
Po raz pierwszy baza danych jest tworzona automatycznie przez usługę API. Baza danych wykorzystuje domyślne loginy usługi NT (API lub BROKER), a uwierzytelnienie następuje za pośrednictwem kanałów Kerberos. Domyślne ustawienia DB to Uwierzytelnianie Windows, Szyfrowanie kolumn. Zalecamy, ale nie wymagamy szyfrowania na poziomie silnika.

Przeglądanie i eksportowanie dzienników zdarzeń Apexx



Można wykorzystać „Podgląd zdarzeń” systemu Windows do przeglądania i rozwiązywania problemów związanych z aplikacjami i usługami Apexx.

1. Należy otworzyć przeglądarkę zdarzeń > wpisać **„Podgląd zdarzeń”** w pasku wyszukiwania systemu Windows, a następnie otworzyć program.
2. Należy kliknąć strzałkę obok > **„Dzienniki aplikacji i usług”**, aby rozwinąć listę.
3. Należy kliknąć aplikację/usługę Apexx, aby wyświetlić wszystkie zdarzenia związane z tą aplikacją lub usługą (Apexx API, Apexx Client, Apexx Communication Service).



4. Z tego miejsca można sortować zdarzenia według czasu, identyfikatora zdarzenia itp., co jest pomocne w przeglądaniu i rozwiązywaniu problemów z konfiguracją Apexx.
5. Można wyeksportować dzienniki zdarzeń Apexx > w sekcji **„Akcje”**, jak również można wybrać opcję **„Zapisz wszystkie zdarzenia jako...”**, aby wyeksportować dzienniki zdarzeń wybranej aplikacji/usługi i zapisać je w jednym z kilku formatów (.evtx, .xml, .txt, .csv).

Najważniejsze wnioski

1. Tylko serwery z oprogramowaniem lokalnym muszą mieć adres IP – moduł eBox nie ma takiego wymagania.
2. Komunikacja między modułem eBox a oprogramowaniem lokalnym (ruch przez intranet/Internet) jest szyfrowana przy użyciu protokołu TLS.
3. Należy uwzględnić serwer SQL w planie odzyskiwania po awarii. Ta baza danych ma kluczowe znaczenie dla działania systemu.



Access Automation Solutions

Entrance Automation
Entrance Security



Access Control Solutions

Electronic Access & Data
Escape and Rescue Systems
Lodging Systems



Access Hardware Solutions

Door Closers
Architectural Hardware
Mechanical Key Systems



Services

Technical Support
Installation and commissioning
Maintenance and Repair



Key & Wall Solutions

Key Systems
Movable / Sliding Walls



Safe Locks

Electronic Safe Locks
Mechanical Safe Locks
Boltworks and Accessories



Glass systems

Manual door systems
Glass fittings
Horizontal Sliding Walls

Nasze zaangażowanie w zrównoważony rozwój

Jesteśmy zobowiązani do wspierania zrównoważonego rozwoju w całym naszym łańcuchu wartości zgodnie z naszą odpowiedzialnością ekonomiczną, środowiskową i społeczną wobec obecnych i przyszłych pokoleń. Zrównoważony rozwój na poziomie produktu jest ważnym, zorientowanym na przyszłość podejściem w dziedzinie budownictwa. Aby zapewnić ilościowe ujawnienia wpływu produktu na środowisko w całym cyklu jego życia, dormakaba dostarcza Deklaracje Środowiskowe Produktu (EPD) oparte na holistycznych ocenach cyklu życia.

<https://www.dormakabagroup.com/en/sustainability/product-declarations>.

Axessor Apexx System Architecture & IT Security Guide - RevB
Może ulec zmianie bez powiadomienia

Dormakaba SAL GmbH

Siemensstrasse 33
42551 Velbert
safelocks.de@dormakaba.com
T +49 2051 9111 0

dormakaba USA Inc.

1525 Bull Lea Road, Suite 100
Lexington, KY 460511
sales.safelocks.us@dormakaba.com
1-800-950-4744



AXESSOR APEXX IP
INSTALLATION AND
OPERATION GUIDES

dk.world/AxessorApexxIP

Série de Softwares Axessor Apexx

Guia de Arquitetura de Sistema e Segurança de TI para Axessor Apexx IP/CIT e CenconX



Índice

Arquitetura do sistema Apexx.....	3
Visão geral	3
Sistema de fechaduras Axessor Apexx	3
Sistema de fechaduras CenconX.....	3
Dispositivos móveis	4
Componentes de API/Software.....	4
API Apexx.....	4
Software cliente Apexx	4
Base de dados Apexx.....	4
Mediador/Servidor MQTT.....	5
SMTP	5
SSO.....	5
Configuração do utilizador - Axessor Apexx	5
Configuração do utilizador - CenconX.....	6
Configuração do utilizador - Utilizadores do software.....	6
Utilizadores do software - Axessor Apexx.....	6
Utilizadores do software - CenconX.....	7
Licenças	7
Métodos de atualização do firmware	7
Atualizações de firmware - sistema de fechaduras Axessor Apexx	7
Atualizações de firmware - sistema de fechaduras CenconX.....	8
Transmissão de dados.....	9
Segurança e encriptação de dados	11
Infraestrutura de Chave Pública (PKI).....	12

Configurações de hardware de computador	14
Configuração com um único computador (ligação USB)	14
Configuração com um único computador (TCP/IP)	15
Configurações com vários computadores	16
Considerações sobre a base de dados	18
Especificações mínimas recomendadas para o computador Apexx.....	18
Especificações do dispositivo móvel Apexx	18
Manual de segurança de TI da Apexx	19
Notas sobre o software local	19
Emparelhamento do software local com a eBox (Axessor Apexx)	19
Recuperação de desastres	20
Visualização e exportação de registos de eventos Apexx.....	20
Principais conclusões	21

Arquitetura do sistema Apexx

Visão geral

O **software da série Apexx** pode ser utilizado para gerir e configurar remotamente vários aspetos dos sistemas de fechaduras Axessor Apexx e CenconX. Este documento descreve aspetos da arquitetura do sistema, da infraestrutura informática e dos requisitos para a utilização do software da série Apexx para suportar e gerir os sistemas de fechaduras Axessor Apexx e CenconX.

Sistema de fechaduras Axessor Apexx

Os sistemas de fecho Axessor Apexx consistem em duas redes de comunicação seguras: O **CAN Bus do sistema de fecho** e a **rede da API (Software)**

O **CAN Bus do sistema de fecho** suporta os seguintes componentes:

- **Teclados da série Apexx** (máximo = 2, mínimo/necessário = 1)
 - Utilizado(s) como interface de utilizador para acesso e configuração do sistema de fecho
- **Fechaduras da série Apexx** (máximo = 16, mínimo/necessário = 1)
 - Fechadura eletromecânica física que controla o acesso do utilizador ao cofre
- **Apexx eBox** (necessária para funcionamento em modo de rede/com ligação IP)
 - Funciona como um conversor de protocolo (IP para CAN Bus) entre o sistema de fechaduras Axessor Apexx e a API (Software)
 - Também funciona como uma caixa de E/S (entrada/saída)

Sistema de fechaduras CenconX

Os sistemas de fecho CenconX consistem em duas redes de comunicação seguras: O **sistema de fechaduras** e a **rede da API (Software)**

O **sistema de fechaduras** suporta os seguintes componentes:

- **Teclados da série CenconX** (1)
 - Utilizado(s) como interface de utilizador para acesso e configuração do sistema de fecho
- **Fechaduras da série CenconX** (1)
 - Fechadura eletromecânica física que controla o acesso do utilizador ao cofre

Dispositivos móveis

A aplicação móvel Safe Locks da dormakaba pode ser utilizada para estabelecer uma interface com os sistemas de fecho Axessor Apexx e CenconX. Está disponível para transferência gratuita no Google Play e na Apple Store, mas não é funcional enquanto não for registada com recurso ao software da série Apexx. Para obter informações sobre como utilizar a aplicação móvel e como registar um dispositivo móvel, consulte o Manual do Utilizador do Sistema CenconX (documento nº. CX003.0524) e o menu de ajuda do software da série Apexx.

- **Sistemas de fechaduras Axessor Apexx** > os dispositivos Axessor Apexx com a versão de firmware 2.1.x.x ou superior podem incorporar dispositivos móveis através da **aplicação móvel Safe Locks** da dormakaba.
- **CenconX Lock Systems** > a **aplicação móvel Safe Locks** da dormakaba funciona como uma ponte entre o sistema de fechaduras CenconX e a API (Software), servindo como forma de autenticar e abrir fechaduras CenconX.

Componentes de API/Software

A **API (Software)** é constituída por 4 componentes principais:

- API Apexx
- Software cliente Apexx
- Base de dados Apexx - Microsoft SQL Server 2019 Express
- Mediador/Servidor MQTT

Nota: O servidor/cliente Apexx deve ser configurado utilizando um IP acessível ao público para facilitar a comunicação com os dispositivos móveis.

API Apexx

A Interface de Programação de Aplicações, ou API, atua como publicador e subscritor na arquitetura MQTT.

Software cliente Apexx

O software cliente Apexx ("software da série Apexx") é uma interface gráfica do utilizador (GUI) que permite aos Utilizadores do software utilizar a API para realizar ações no sistema Apexx/CenconX (alterar as definições do sistema, armazenar/recuperar dados, etc.)

O cliente Apexx suporta vários utilizadores, mas não suporta vários utilizadores em simultâneo num único cliente. Apenas uma pessoa pode estar ligada a uma única instância de cliente num determinado momento.

Base de dados Apexx

A base de dados Apexx é o principal local de armazenamento de dados no sistema Apexx. A base de dados Apexx utiliza o sistema de gestão de bases de dados relacionais proprietário da Microsoft, o Microsoft SQL Server 2019 Express, como meio de armazenar e recuperar dados do sistema.

Mediador/Servidor MQTT

O Message Queuing Telemetry Transport, ou MQTT, é um protocolo de mensagens que utiliza um modelo de publicação-subscrição para facilitar a comunicação entre dispositivos. O Mediador/Servidor MQTT atua como um hub de mensagens centralizado e utiliza o protocolo MQTT para gerir a comunicação entre dispositivos. Mais concretamente, o MQTT transmite mensagens entre o software cliente Windows e a eBox.

SMTP

O software da série Apexx utiliza o Protocolo de Transporte de Correio Simples (SMTP) para enviar o seguinte: Alertas ativos, relatórios programados e informações de configuração de dispositivos móveis.

- Os alertas ativos são enviados para os destinatários com base na ocorrência de um ou mais eventos de auditoria selecionados pelo Utilizador do software.
- Os relatórios agendados podem ser enviados por correio eletrónico aos destinatários com base numa programação definida pelo utilizador, utilizando também o SMTP.
- Ao adicionar um novo dispositivo móvel no software da série Apexx, tem a opção de utilizar o código QR gerado para a configuração do dispositivo móvel. Quando utiliza a aplicação móvel Safe Locks para digitalizar o código QR, o sistema utiliza SMTP para enviar as informações de configuração para o dispositivo móvel.
- Consulte o menu de ajuda do software da série Apexx para obter informações sobre como configurar as definições de SMTP.

SSO

O software da série Apexx utiliza o início de sessão único (SSO), garantindo que um Utilizador do software pode utilizar as suas credenciais para iniciar sessão na API utilizando um único conjunto de credenciais.

Configuração do utilizador - Axessor Apexx

Os utilizadores do sistema Axessor Apexx dividem-se em duas categorias distintas: **Utilizadores do Safe Lock** e **Utilizadores do software**

Os **Utilizadores do Safe Lock** são utilizadores que irão utilizar o sistema de fechaduras Axessor Apexx (composto por teclados físicos, fechaduras e eBox) e possuirão credenciais e funções únicas, com permissões que definem o respetivo nível de acesso ao sistema.

Os Utilizadores do Safe Lock utilizam IDs de utilizador e PINs para aceder ao sistema de fechaduras utilizando o teclado da série Apexx. Este modo de funcionamento é conhecido como Modo de Banco (também conhecido como Modo Estático).

Os três tipos de utilizadores predefinidos do Safe Lock (Administrador, Gestor e Utilizador) constituem uma hierarquia de utilizadores, cada um com funções e privilégios predefinidos no âmbito do sistema de fecho. Para além destes tipos de utilizadores, podem ser criadas funções de Utilizador do Safe Lock adicionais utilizando as ferramentas administrativas do software da série Apexx que têm permissões definidas por um Utilizador do software. Estas funções de utilizador adicionais são criadas utilizando uma estrutura dos três tipos de utilizador iniciais, permitindo assim que novos tipos de utilizador satisfaçam as necessidades de personalização do cliente.

Os dispositivos Axessor Apexx com versões de firmware 2.1.x.x ou superiores introduzem tipos de utilizadores adicionais (um Administrador Principal e um Administrador de Inquilinos), bem como dois Modos de Utilizador adicionais (Modo OTC e Modo ICS) que incorporam a utilização de dispositivos móveis para acesso a fechaduras. Consulte o Manual do Utilizador do Sistema de teclados da série Apexx (documento nº. 802.0622) para obter mais detalhes sobre os tipos de Utilizador do Safe Lock e os Modos de Utilizador.

Configuração do utilizador - CenconX

Os utilizadores do sistema Axessor Apexx dividem-se em duas categorias distintas: **Utilizadores do Safe Lock** e **Utilizadores do software**

Os **Utilizadores do Safe Lock** são utilizadores que irão utilizar o sistema de fechaduras CenconX (composto por teclados físicos, fechaduras, etc.) e possuirão credenciais e funções únicas, com permissões que definem o respetivo nível de acesso ao sistema.

Os tipos de Utilizadores do Safe Lock nos sistemas CenconX incluem Administradores, Gestores, Utilizadores de PIN estático (Modo de Banco) e Utilizadores de OTC (Código de Utilização Única). Consulte o Manual do Utilizador do Sistema CenconX (documento nº. CX003.0524) para obter mais informações sobre os tipos de utilizadores e as respetivas permissões.

Configuração do utilizador - Utilizadores do software

Utilizadores do software refere-se aos utilizadores que executam o software da série Apexx e utilizam as ferramentas de software para realizar tarefas de gestão e administração. Ao contrário dos Utilizadores do Safe Lock, os Utilizadores do software não acedem diretamente ao sistema de fechaduras físico (abrir/fechar portas de cofres), mas executam tarefas administrativas/gerenciais através do software (adicionar utilizadores de fechaduras, repor palavras-passe de utilizadores de fechaduras).

Os Utilizadores do software utilizam credenciais para aceder ao software da série Apexx utilizando o início de sessão único (SSO). Outros tipos de autenticação para Utilizadores do software da série Apexx incluem a autenticação do Windows (com exceção do Entra ID), a autenticação do domínio do Windows e o Google OAuth 2.0.

Os Utilizadores do software que têm uma permissão de "escrita" podem adicionar novos utilizadores do software e configurar as permissões de leitura/escrita.

Utilizadores do software - Axessor Apexx

Os tipos de Utilizadores do software nos sistemas Axessor Apexx incluem Administradores e Gestores. Nas aplicações de transporte de dinheiro, os Distribuidores e os Auditores também desempenham um papel importante (**nota:** requer firmware do dispositivo na versão 2.1.x.x ou superior).

Consulte o menu de ajuda do software da série Apexx para obter mais detalhes sobre os tipos de Utilizadores do software e as respetivas permissões.

Utilizadores do software - CenconX

Os tipos de Utilizadores do software nos sistemas CenconX incluem Administradores, Gestores, Distribuidores e Auditores. Consulte o Manual do Utilizador do Sistema CenconX (documento n.º CX003.0524) para obter mais informações sobre os tipos de utilizadores e as respetivas permissões.

Ao configurar o seu sistema de fechaduras CenconX, tem a possibilidade de configurar um único cliente/base de dados para um único Proprietário (Distribuidor Principal), ou pode introduzir um segundo cliente/base de dados para permitir que um Distribuidor Secundário tenha controlo partilhado sobre a gestão e acesso ao sistema. Consulte o Manual do Utilizador do Sistema CenconX para obter mais informações (documento n.º CX003.0524).

Licenças

O software da série Apexx tem vários tipos de licenças disponíveis, cada uma das quais desbloqueia diferentes funções e características do software. Para mais informações, consulte os catálogos de preços do Axessor Apexx IP e CenconX.

Métodos de atualização do firmware

O processo de atualização do firmware do seu dispositivo Axessor Apexx varia consoante a licença adquirida.

Para obter mais informações sobre o processo de atualização do firmware, consulte o Manual do Utilizador do Sistema Axessor Apexx (documento n.º 802.0622), o Manual do Utilizador CenconX (documento n.º CX003.0524) e o menu de ajuda do Software da Série Apexx.

Atualizações de firmware - sistema de fechaduras Axessor Apexx

As **atualizações locais de firmware** podem ser realizadas através de uma ligação USB temporária entre o computador que executa o software da série Apexx e o teclado do seu sistema de fechaduras.

As **atualizações remotas de firmware** podem ser realizadas com recurso a uma ligação de rede através da eBox. Trata-se de um processo em três etapas:

1. Um Utilizador do software inicia o processo de atualização remota do firmware, enviando o firmware da API (Software) para o sistema de fecho através da eBox.
2. O firmware é transferido e armazenado no sistema de fecho. Será apresentada uma mensagem no ecrã do teclado informando os Utilizadores do Safe Lock que existe uma atualização de firmware pendente.
3. Um Utilizador do Safe Lock introduz credenciais válidas (ID de Utilizador e PIN) no teclado e, em seguida, inicia a atualização do firmware.

Atualizações de firmware - sistema de fechaduras CenconX

As **atualizações locais de firmware** podem ser realizadas através de uma ligação USB temporária entre o computador que executa o software da série Apexx e o teclado do seu sistema de fechaduras.

Os utilizadores móveis do CenconX têm igualmente a opção de realizar **atualizações do firmware em dispositivos móveis**, em que a aplicação móvel Safe Locks da dormakaba pode ser utilizada para receber atualizações de firmware. O processo envolve a utilização do software da série Apexx para enviar os ficheiros de atualização do firmware para o dispositivo móvel do utilizador. O utilizador móvel pode então iniciar sessão na aplicação Safe Locks, descarregar os ficheiros necessários e iniciar o processo de atualização do firmware utilizando uma ligação BLE entre o dispositivo móvel e o teclado CenconX.

Transmissão de dados

A Figura 1 e o gráfico que a acompanha mostram o fluxo de dados entre os vários componentes de hardware e software do sistema de fechaduras Axessor Apexx.

Porta de comunicação	Descrição
443	Esta porta é utilizada para o tráfego TCP/IP de saída.
587	Esta porta é utilizada para comunicar com o host SMTP. É obrigatório indicar e o valor por defeito é 587.
5001	Esta é a porta predefinida utilizada para a colocação em funcionamento de um sistema de fechaduras Apexx.
8883	Esta é a porta predefinida utilizada pelo Mediador MQTT.

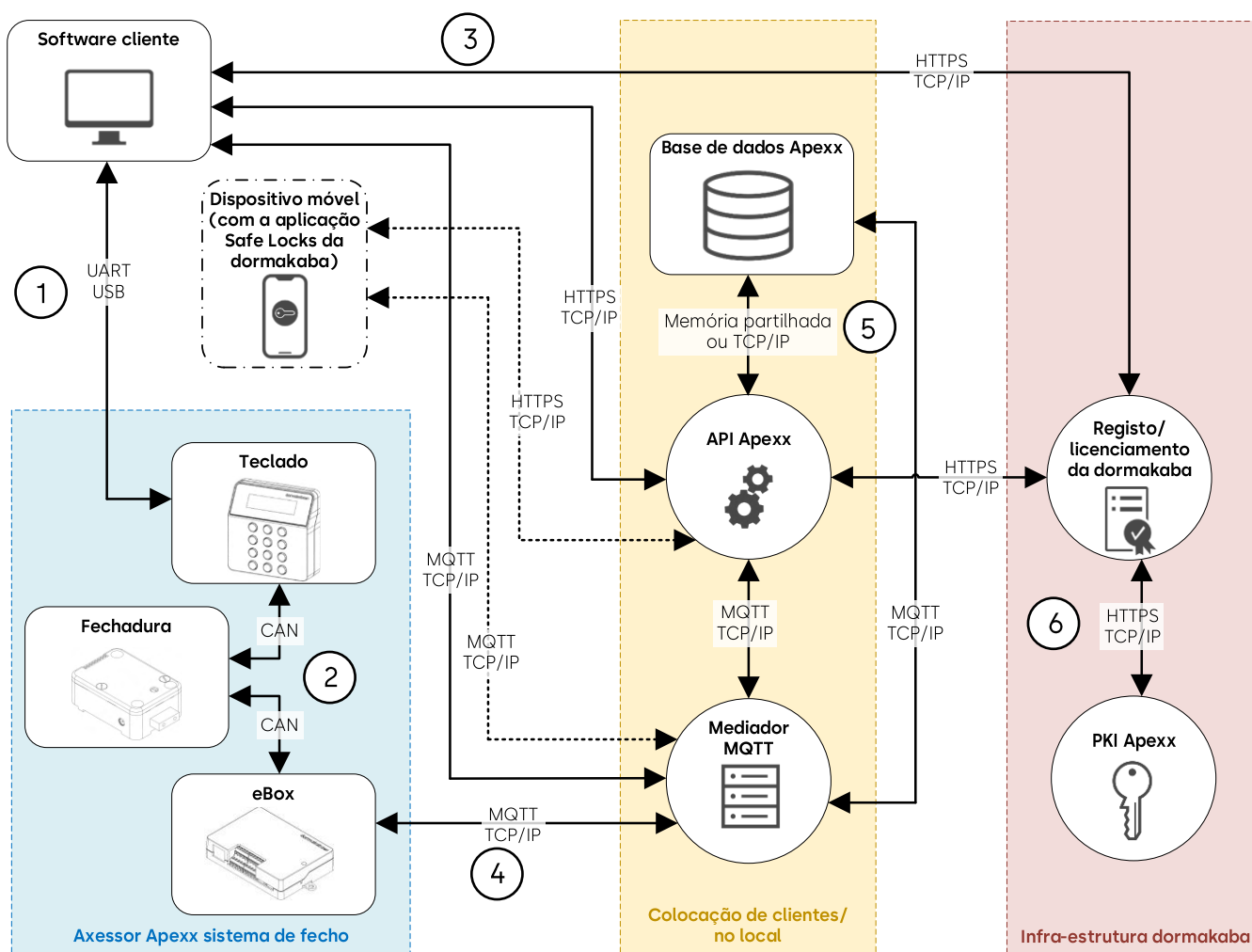


Figura 1 - arquitetura do sistema Apexx com sistema de fecho Apexx - componentes do sistema e transmissão de dados

	Protocolos de comunicação	Fluxo de dados	Descrição/objetivo
1	UART via USB	Caminho bidirecional: Software cliente para teclado	Configuração direta e recuperação para auditoria
2	CAN	Caminho bidirecional: - Do teclado para a fechadura - Da fechadura para a eBox	Comunicação dispositivo-a-dispositivo
3	HTTPS via TCP/IP	Caminho bidirecional: Do software cliente para o registo/licenciamento da dormakaba	Licenciamento e registo online
4	MQTT via TCP/IP	Caminho bidirecional: - Do software cliente para o Mediador MQTT Caminho bidirecional: - Da eBox para o Mediador MQTT Caminho bidirecional: - Dispositivo com a aplicação móvel dormakaba Safe Locks para o Mediador MQTT	Configuração em rede e recuperação para auditoria
5	Memória partilhada ou TCP/IP	Caminho bidirecional: Da API Apexx para a base de dados Apexx	Armazenamento persistente de dados com o SQL Server
6	HTTPS via TCP/IP	Caminho bidirecional: - Do software cliente para a Apexx API - Da API Apexx para o registo/licenciamento da dormakaba - Do registo/licenciamento da dormakaba para a Apexx PKI - Do dispositivo com a aplicação móvel Safe Locks da dormakaba para a API Apexx	Emissão de certificado x.509

A Figura 2 mostra um diagrama semelhante ao descrito em Figura 1, mas com um sistema de fechaduras CenconX em vez do sistema de fecho Axessor Apexx. Neste caso, o dispositivo móvel atua como o canal de comunicação entre o sistema de fechaduras CenconX e a infraestrutura de software.

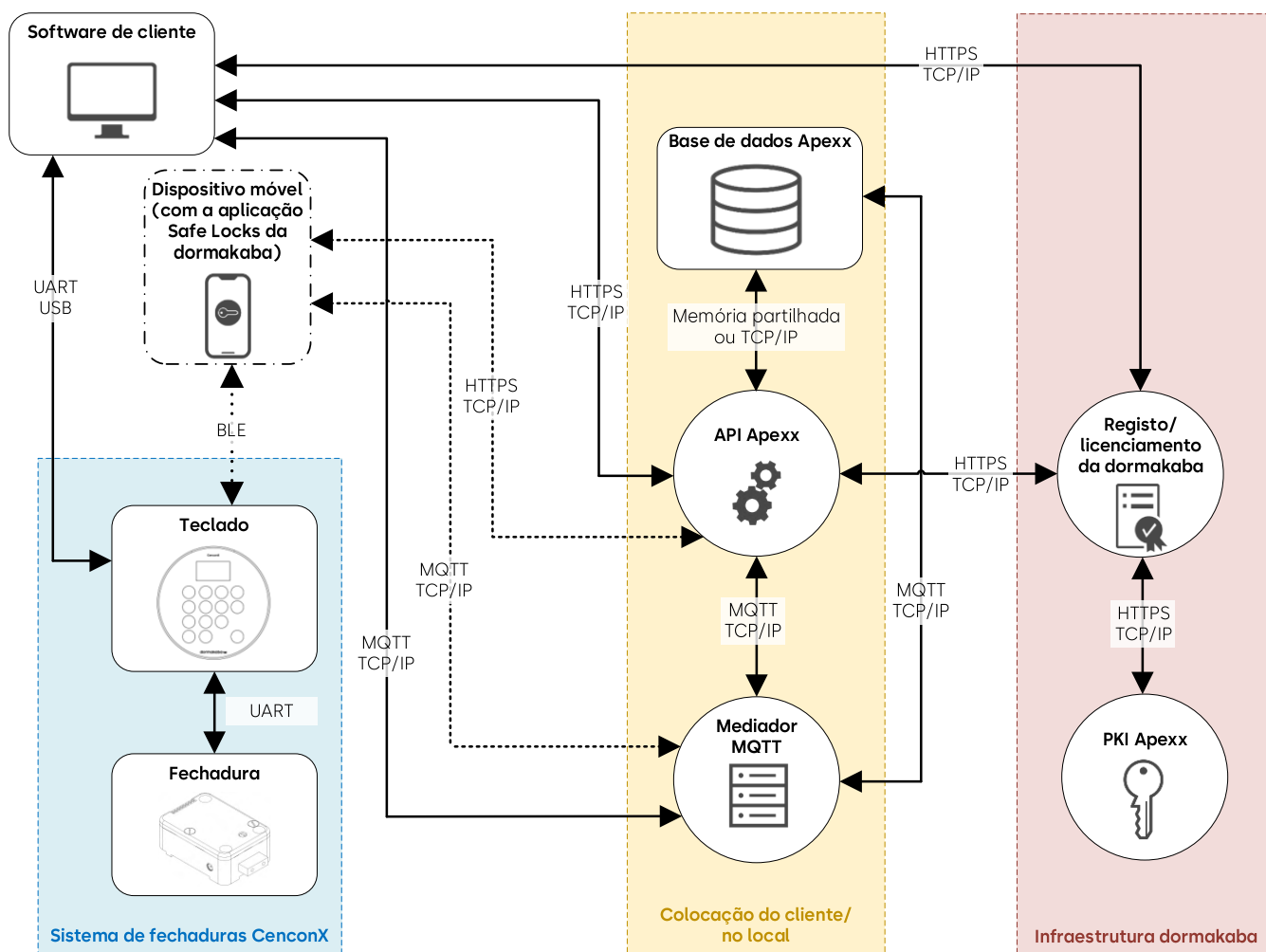


Figura 2 - arquitetura do sistema Apexx com sistema de fechaduras CenconX - componentes do sistema e transmissão de dados

Segurança e encriptação de dados

O software da série Apexx, os sistemas de fechaduras CenconX, os sistemas de fechaduras Axessor Apexx e os dispositivos móveis autorizados utilizam vários métodos de encriptação, incluindo os certificados AES256, PBKDF2 e TLS, para garantir a comunicação e o armazenamento seguros dos dados.

Infraestrutura de Chave Pública (PKI)

O software da série Apexx, os sistemas de fechaduras CenconX, os sistemas de fechaduras Axessor Apexx e os dispositivos móveis comissionados utilizam uma Infraestrutura de Chave Pública para criar, armazenar e distribuir certificados digitais para dispositivos Apexx através de autoridades de certificação.

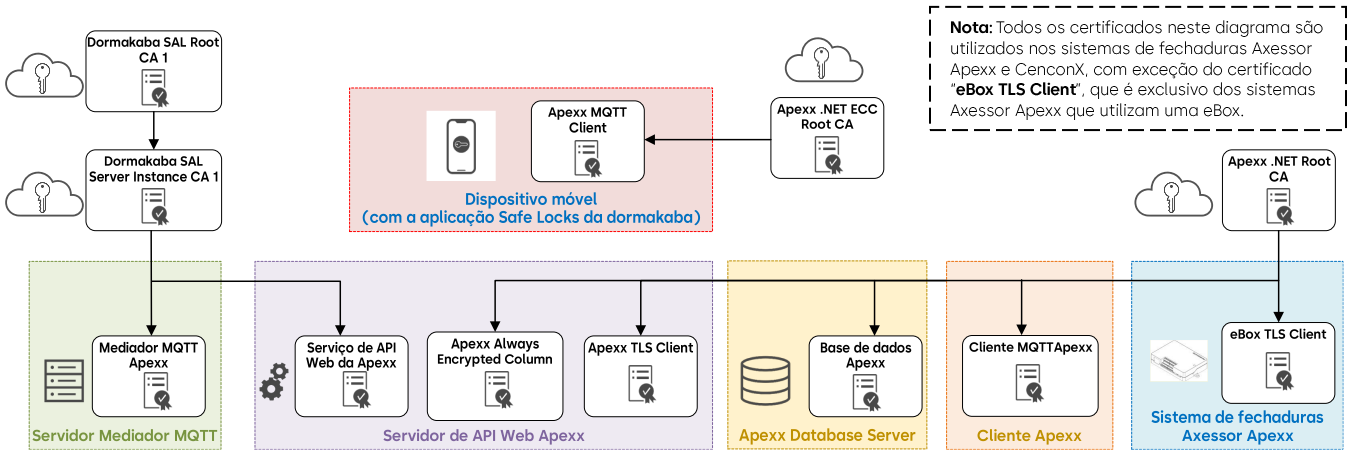


Figura 3 - Infraestrutura de Chave Pública

Tipo de certificado	Descrição
Dormakaba SAL Root CA	- Este certificado é pré-instalado nos dispositivos na fábrica e substituído através de uma atualização de firmware - Durante a instalação do software da série Apexx, este certificado também é instalado ao executar o ficheiro do Instalador de Pré-requisitos nos computadores do cliente e do servidor (armazenado na pasta Trusted Root Certification Authorities)
Dormakaba SAL Server Instance CA	- Os servidores que executam serviços de software locais para o Apexx necessitam de certificados assinados pela PKI SAL da dormakaba para que os dispositivos confiem neles - Este certificado deve ser implantado em todos os servidores que executam serviços de software locais - Durante a instalação do software da série Apexx, este certificado também é instalado quando se executa o ficheiro do Instalador de Pré-requisitos nas máquinas cliente e servidor (armazenado na pasta Intermediate Certification Authorities)
Apexx MQTT Broker	- Criado durante a instalação do software - Utilizado para ligações TLS e autenticação
Apexx Web API Service	- Criado durante a instalação do software - Contém o nome do servidor (computador onde este serviço está instalado), a autoridade de certificação de confiança e a chave de encriptação pública do servidor
Apexx TLS Client	- Utilizado para autenticação do cliente Apexx - O certificado é um utilizador verificado se o emissor corresponder ao Apexx .NET Root CA no servidor mediador
Apexx Database	- O SQL Server no Windows é o único motor de base de dados suportado - As seguintes definições estão ativadas na instância/base de dados: - Autenticação do Windows - O controlo de acesso baseado em funções (RBAC) é utilizado, juntamente com a autenticação do Windows, para controlar as permissões
eBox TLS Client	- Utilizado para a autenticação da eBox - O certificado é um utilizador verificado se o emissor corresponder ao Apexx .NET Root CA no servidor mediador

Tipo de certificado	Descrição
Apexx .NET Root CA	• Criado durante a instalação do software e armazenado no arquivo de certificados da máquina local, na pasta Trusted Root Certification Authorities • Durante o processo de instalação da API, é armazenado na pasta certificados pessoais da máquina local (LM\Personal\Certificates) • Qualquer computador que execute o software (cliente, servidor, base de dados, etc.) necessita de uma cópia deste certificado para efeitos de segurança/identificação • A PKI de software local assina pedidos de certificados para todos os clientes do mediador MQTT • Esses certificados são utilizados para estabelecer ligações TLS (Transport Layer Security) de confiança mútua e autenticação com o mediador MQTT • Também pode assinar os certificados utilizados pelo SQL Server para TLS • Utiliza RSA para assinaturas
Apexx .NET ECC Root CA	• Criado durante a instalação do software e armazenado no arquivo de certificados da máquina local, na pasta Trusted Root Certification Authorities • Durante o processo de instalação da API, é armazenado na pasta certificados pessoais da máquina local (LM\Personal\Certificates) • Qualquer computador que execute o software (cliente, servidor, base de dados, etc.) necessita de uma cópia deste certificado para efeitos de segurança/identificação • A PKI de software local assina pedidos de certificados para todos os clientes do mediador MQTT • Esses certificados são utilizados para estabelecer ligações TLS (Transport Layer Security) de confiança mútua e autenticação com o mediador MQTT • Também pode assinar os certificados utilizados pelo SQL Server para TLS • Utiliza ECDSA para assinaturas
Apexx MQTT Client	• Criado durante o início de sessão do cliente de software • Utilizado para ligações TLS e autenticação
Apexx Always Encrypted Column	• Encriptação de dados na API que vai para a coluna encriptada na base de dados • Durante o processo de instalação da API, é armazenado na pasta certificados pessoais da máquina local (LM\Personal\Certificates)

Nota: Os certificados podem ser renovados 60 dias antes da expiração, renovando a sua licença através da ferramenta de registo online do software da série Apexx.

Configurações de hardware de computador

A parte de hardware/API/software do sistema Apexx pode ser configurada de várias formas, dependendo da complexidade do seu sistema (número de sistemas de fecho Apexx, as suas localizações, etc.). Esta secção descreve apenas algumas das várias configurações possíveis. Consulte os catálogos de preços Axessor Apexx ou CenconX para obter mais informações sobre os requisitos de licença para as várias configurações de computador/hardware.

Nota: Se desejar, qualquer um dos componentes de software (cliente, base de dados, API ou MQTT) pode ser alojado numa máquina virtual.

Configuração com um único computador (ligação USB)

A Figura 4 ilustra uma configuração básica que envolve apenas um único computador e um sistema de fecho Axessor Apexx e/ou um sistema de fecho CenconX. Nesta configuração, todos os elementos API/software estão alojados num único computador, sendo utilizada uma ligação USB para ligar temporariamente ao sistema de fecho Axessor Apexx ou CenconX para efeitos de programação/configuração do sistema.

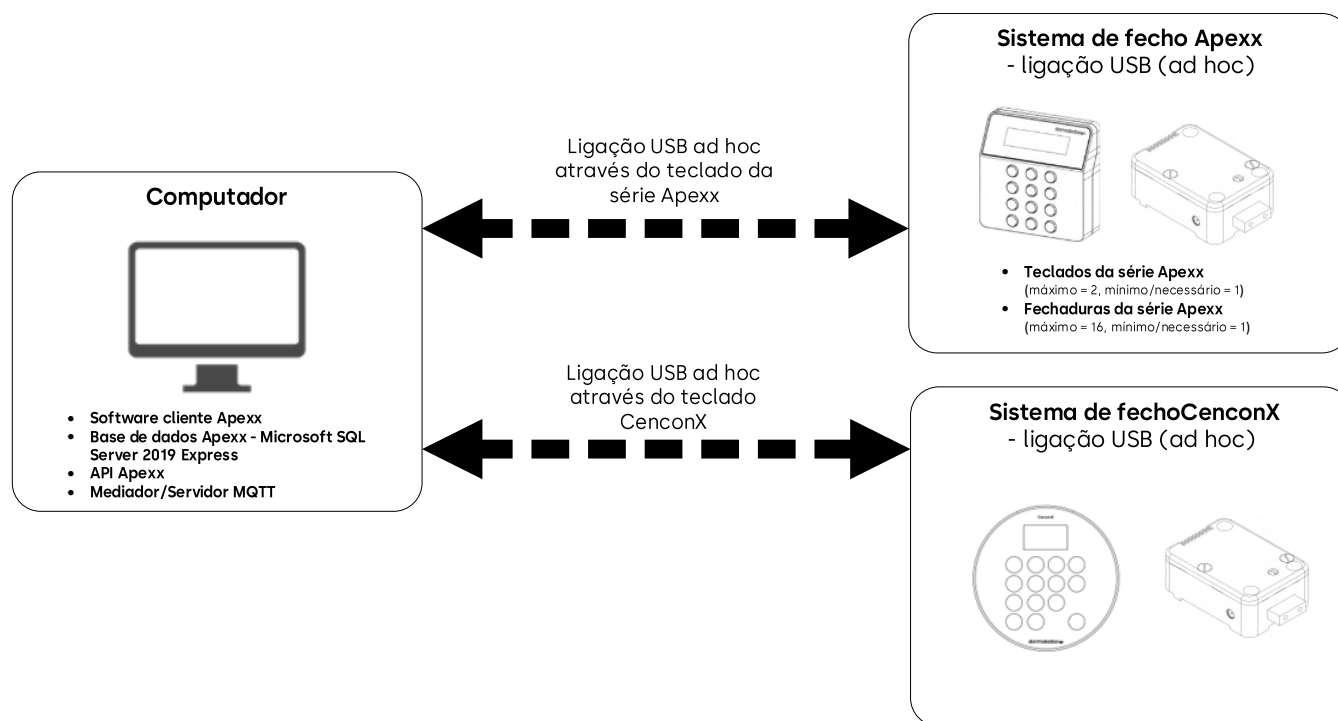


Figura 4 - configuração com um único computador - ligação USB ad hoc

Sistemas de fechaduras Axessor Apexx - ligação USB

Para o Axessor Apexx, esta configuração funciona bem em locais pequenos, onde o computador e todos os componentes do sistema de fecho (teclados e fechaduras) estão no mesmo local físico, mas não tem a versatilidade e a comodidade oferecidas pelas configurações em rede que utilizam a Apexx eBox.

Sistemas de fechaduras CenconX - ligação USB

No caso do CenconX, as ligações exclusivamente por USB não são recomendadas para sistemas que utilizam a funcionalidade OTC.

Configuração com um único computador (TCP/IP)

A Figura 5 mostra outra configuração simples que envolve apenas um computador e um sistema de fecho Axessor Apexx e/ou um sistema de fecho CenconX.

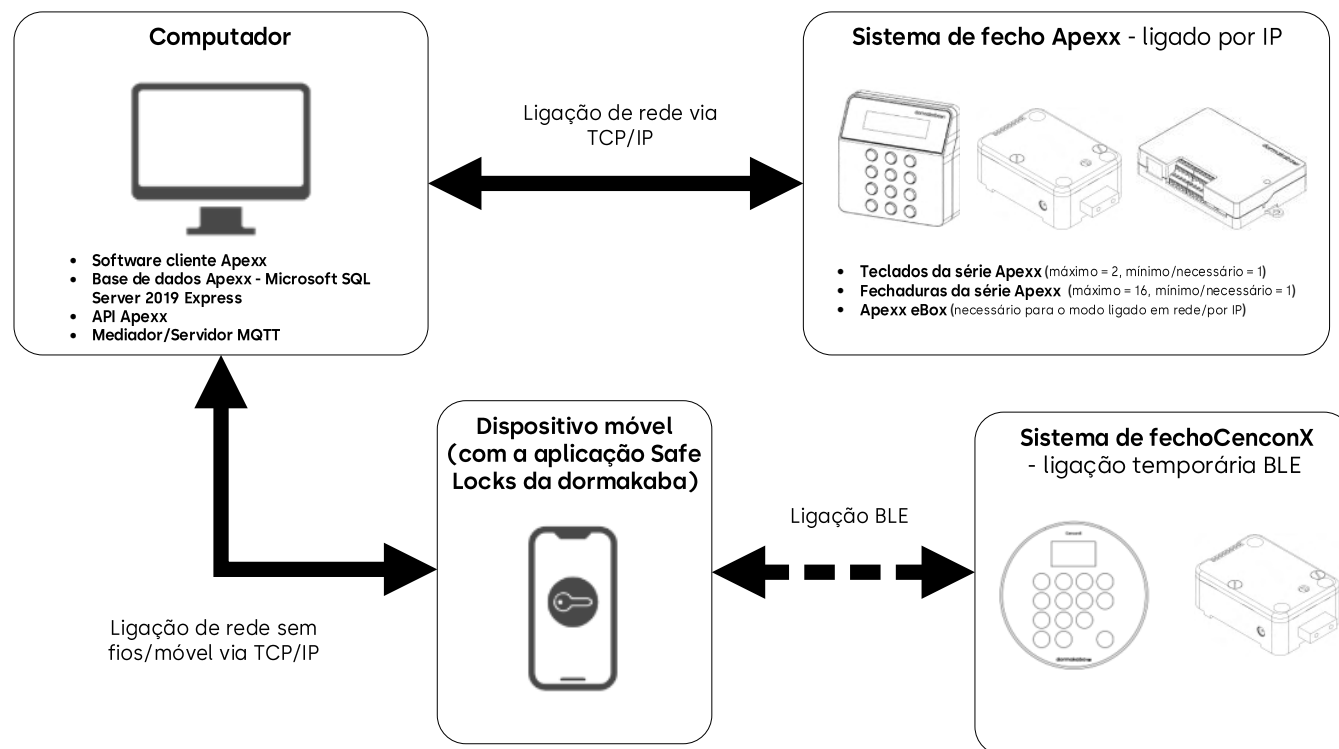


Figura 5 - configuração com um único computador - rede via eBox (TCP/IP) e móvel

Sistemas de fechaduras Axessor Apexx - configuração com um único computador (TCP/IP)

A Apexx eBox é utilizada para fornecer uma ligação de rede/IP para uma comunicação contínua/em direto entre o computador e o sistema de fecho Axessor Apexx.

Para os sistemas de fecho Axessor Apexx, esta configuração também é útil para configurações mais pequenas em que todo o equipamento se encontra no mesmo local físico, mas a inclusão da eBox permite ao administrador do sistema tirar partido de todas as funcionalidades que uma ligação IP ativa proporciona (auditorias em tempo real, monitorização ativa do sistema, atualizações remotas de firmware e outras funcionalidades adicionais de hardware/software)

Sistemas de fechaduras CenconX - configuração com um único computador (TCP/IP)

No caso do sistema de fecho CenconX, o dispositivo móvel liga-se ao computador servidor/cliente através de uma ligação de rede/IP e uma ligação temporária de "ponte" BLE liga o dispositivo móvel ao sistema de fecho CenconX.

Configurações com vários computadores

Para instalações de maior dimensão que envolvam edifícios maiores e/ou vários sistemas de fecho, a configuração com vários computadores apresentada na Figura 6 oferece uma flexibilidade adicional.

Nota: Apenas uma API, um Mediador MQTT e uma base de dados SQL Server são permitidos no sistema.

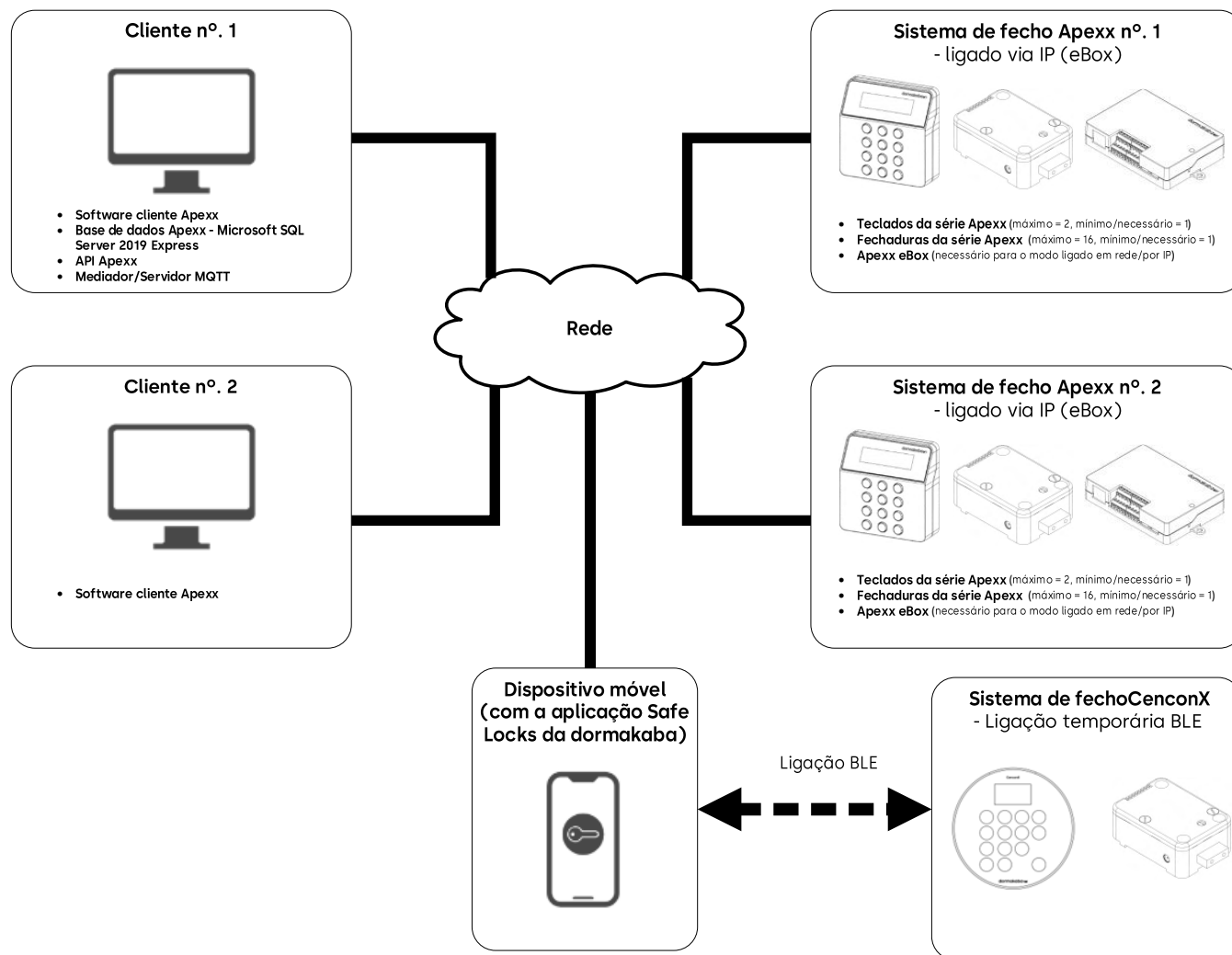


Figura 6 - configuração de vários computadores com vários sistemas de fecho

Neste tipo de configuração, qualquer um ou todos os componentes de software podem ser instalados num ou mais computadores (ou máquinas virtuais), permitindo uma maior comodidade e flexibilidade quando se trata de executar e configurar os seus sistemas de fecho. Tenha em atenção que cada sistema de fecho Axessor Apexx se liga à rede através de uma Apexx eBox.

Este conceito é alargado no sistema apresentado na Figura 7, que inclui vários computadores e sistemas de fechaduras espalhados por vários edifícios.

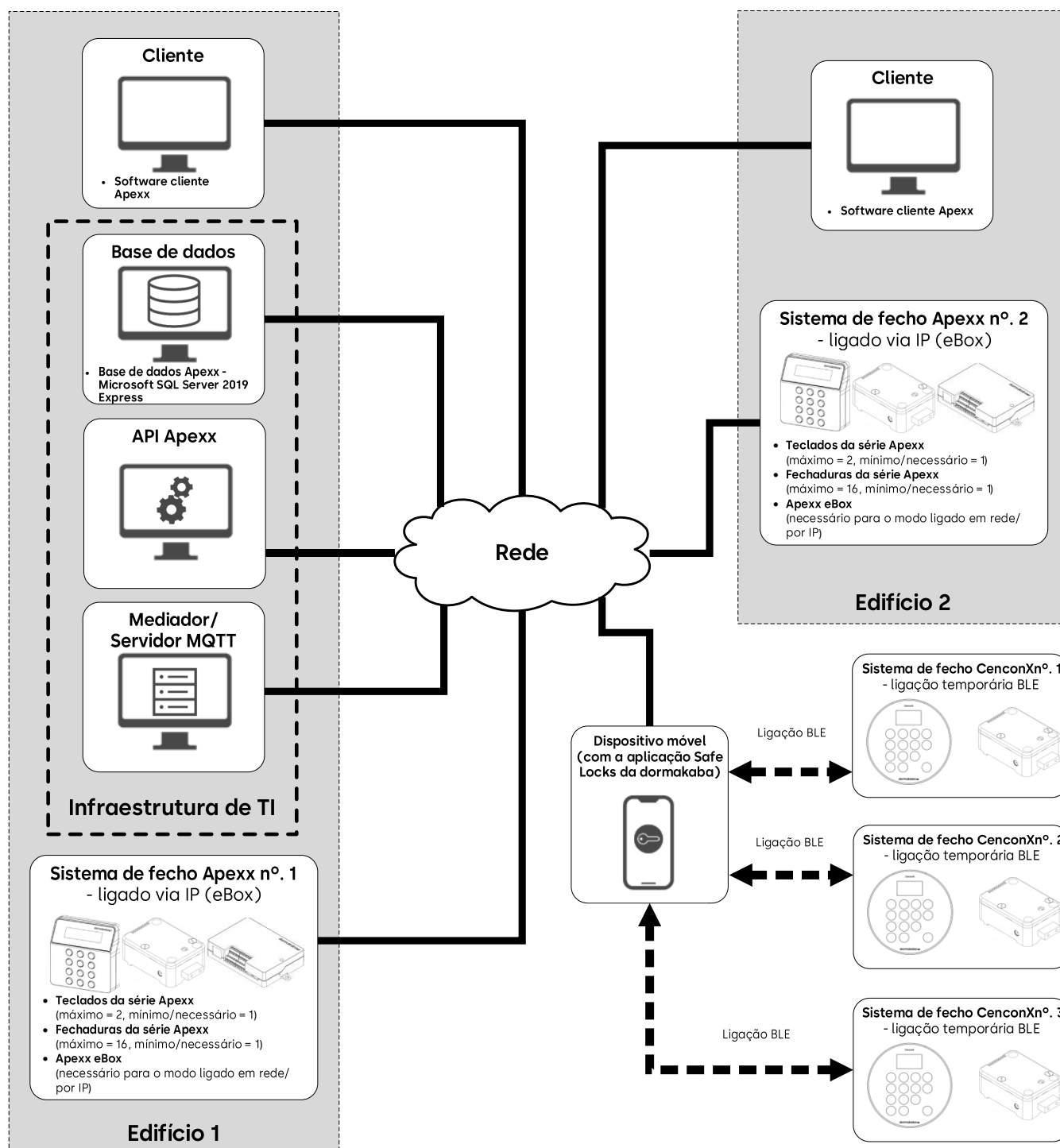


Figura 7 - configuração com múltiplos computadores/sistema de fecho com configuração multi-servidor

Uma diferença notável entre esta configuração e todas as outras é o facto de incluir vários computadores que alojam diferentes componentes de software. Repare como dois dos computadores no edifício 1 alojam a API Apexx e a base de dados Apexx, respetivamente. Estes dois computadores podem ser configurados para serem utilizados como API e base de dados para os sistemas de fecho no edifício 1, edifício 2 e/ou qualquer outro sistema de fecho em toda a rede.

Este exemplo final ilustra que são possíveis muitas configurações diferentes, dependendo das necessidades organizacionais e da configuração da infraestrutura de TI.

Considerações sobre a base de dados

O software da série Apexx inclui o Microsoft SQL Server 2019 Express como motor de base de dados interno dedicado.

	Microsoft SQL Server 2019 Express (64 bits)
Limite da base de dados	10 GB
Número de CPUs	1 processador físico
RAM	1 GB
Sistemas operativos suportados	Windows 10, Windows Server 2016, Windows Server 2019

Especificações mínimas recomendadas para o computador Apexx

*Considerar a duplicação para instalações maiores

Estação de trabalho do cliente Apexx

- Processador de 2,0 GHz com 4 núcleos*
- 16 GB RAM
- Disco rígido de 500 GB
- Windows 10 Professional 64 bits

Servidor Mediador Apexx

- Processador de 2,0 GHz com 4 núcleos*
- 16 GB RAM
- Disco rígido de 500 GB
- Windows 2019 Server Standard 64 bits

Servidor de Base de Dados Apexx e API Apexx

- Processador de 2,0 GHz com 6 núcleos*
- 32 GB RAM*
- Disco rígido de 1 TB
- Windows 2019 Server Standard 64 bits
- Microsoft SQL Server Standard ou Enterprise

Nota: Se desejar, qualquer um dos componentes de software (cliente, base de dados, API ou mediador MQTT) pode ser alojado numa máquina virtual.

Especificações do dispositivo móvel Apexx

(a partir da data de publicação do documento)

- Sistema operativo móvel: Android 8+ ou iOS 15+
- Deve ser compatível com BLE

Nota: Consulte o Google Play e a Apple Store para obter as versões mais recentes da aplicação móvel Safe Locks da dormakaba e informações de compatibilidade com dispositivos/OS.

Manual de segurança de TI da Apexx

Notas sobre o software local

- Todos os componentes do software (MQTT, cliente e API) foram concebidos como aplicações para Windows. Para os poder utilizar num ambiente de nuvem, é necessário poder gerir os canais de comunicação entre eles.
- Os canais de comunicação são estabelecidos durante a instalação - eles dependem do DNS (ou de endereços IP estáticos). Quando a instalação estiver concluída, serão criados certificados para efeitos de segurança. Estes certificados têm de ser geridos corretamente para evitar possíveis vias de ataque.
- A comunicação de e para o sistema de fecho é MQTT sobre SSL, pelo que as portas padrão têm de estar acessíveis.
- O software requer o subsistema de certificados do Windows e uma base de dados SQL19 para funcionar.
- O software não é suportado em sistemas Mac ou Linux.
- Os ambientes de nuvem testados são Azure e AWS.
- O mesmo utilizador não pode ter sessão iniciada em vários clientes ao mesmo tempo.

Emparelhamento do software local com a eBox (Axessor Apexx)

O software local e a Apexx eBox têm de ser emparelhados antes de se poder estabelecer uma ligação. Quando for necessário instalar uma nova eBox:

1. A eBox é fisicamente instalada no CAN Bus.
2. Um utilizador autorizado tem de iniciar sessão no teclado e colocar a eBox em funcionamento no CAN Bus (dispositivos não autorizados não podem aceder ao CAN Bus).
3. Após a colocação em funcionamento da eBox, esta obtém as chaves de encriptação para o CAN Bus (AES-256 com chaves específicas do sistema).
4. Quando a eBox estiver ligada ao CAN Bus, é necessário estabelecer uma ligação com o software local. O endereço IP pode ser visualizado e alterado nas definições de rede no menu avançado do teclado. Se existir uma definição, esta será utilizada. Caso contrário, a eBox assume o DHCP para obter o endereço IP.
5. Assim que existirem definições de Ethernet válidas, a eBox tentar-se-á ligar ao servidor MQTT no software local (quer através de comunicação IP direta com base nas configurações, quer através de difusão na rede local no caso de DHCP). Isto é feito através de TLS.
6. Se o software local detetar uma nova eBox, esta tem de ser autorizada no software antes de se iniciar a sessão com sucesso utilizando o código de reclamação. Quando a eBox é autorizada no software, o software emite um PIN de verificação que deve ser validado no teclado (verificação do software para a eBox e da eBox para o software).

7. Depois de o sistema ser verificado, é estabelecido um canal seguro. Isto é feito utilizando certificados assinados de fábrica e pré-instalados (infraestrutura PKI). Qualquer comunicação posterior é encriptada utilizando TLS.
8. TLS 1.2. A eBox também comunica inicialmente através da porta TCP 5001 (API) para verificar se o software está ativado e depois através da porta 8883 (por defeito) para comunicação.
9. O software tem de ser ativado e ter certificados adequados para que a eBox seja ativada corretamente. Se o software não estiver ativado, vai levar a uma negação de serviço.

Para mais informações sobre a instalação, ligação e configuração da Apexx eBox, consulte o Manual de Instalação do Sistema Axessor Apexx (Documento nº. 801.0622), o Manual do Utilizador do Sistema de teclados da série Apexx (Documento nº. 802.0622) e o menu de ajuda do software da série Apexx.

Recuperação de desastres

O software local liga-se à base de dados SQL19 para armazenamento de dados (SQL19 Express da Microsoft - referência: <https://www.microsoft.com/en-ca/sql-server/sql-server-2019-pricing>).

A configuração da base de dados tem de ser introduzida no software local sob a forma de um ficheiro de configuração. A encriptação/proteção e a recuperação de dados seguirão então o caminho da base de dados SQL19. Prevê-se que a base de dados seja gerida pelo departamento local de TI.

O caminho de recuperação será então reinstalar a API, o MQTT e o cliente com uma nova cópia da dormakaba ou utilizar uma cópia de segurança local. Todos os dados estão armazenados na base de dados SQL. A API, o MQTT e o cliente não armazenam quaisquer dados de bloqueio ou do utilizador, apenas definições de ligação e configuração.

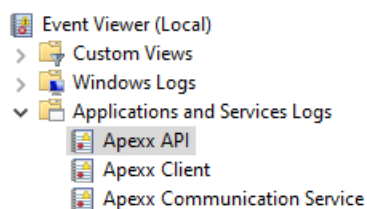
A base de dados é criada automaticamente pelo serviço API aquando da primeira vez. A base de dados utiliza inícios de sessão de serviço NT predefinidos específicos (API ou MEDIADOR) e autentica-se através de canais Kerberos. As definições predefinidas da BD são autenticação do Windows e colunas encriptadas. Recomendamos, mas não exigimos, a encriptação ao nível da base de dados.

Visualização e exportação de registos de eventos Apexx



O "Visualizador de Eventos" do Windows pode ser utilizado para ajudar a visualizar e resolver problemas relacionados com as aplicações e serviços Apexx.

1. Abrir o visualizador de eventos > digite "**Visualizador de eventos**" na barra de pesquisa do Windows e, em seguida, abra o programa.
2. Clique na seta junto a > 📁 "**Registos de aplicações e serviços**" para expandir a lista.
3. Clique na aplicação/serviço Apexx para ver todos os eventos relacionados com essa aplicação ou serviço (API Apexx, cliente Apexx, serviço de comunicação Apexx).



4. A partir daqui, pode ordenar os eventos por hora, ID do evento, etc., para ajudar na visualização e resolução de problemas com a configuração do Apexx.
5. Exportar registos de eventos Apexx > em **"Ações"**, pode escolher  **"Guardar todos os eventos como..."** para exportar os registos de eventos da aplicação/serviço selecionado e guardá-los num dos formatos suportados (.evtx, .xml, .txt, .csv).

Principais conclusões

1. Apenas os servidores com software local precisam de ter endereço IP - a eBox não precisa.
2. A comunicação entre a eBox e o software local (transmissão de dados através da intranet/Internet) é encriptada por TLS.
3. Inclua o servidor SQL no seu plano de recuperação de desastres. Esta base de dados é crucial para o funcionamento do sistema.



Access Automation Solutions

Entrance Automation
Entrance Security



Access Control Solutions

Electronic Access & Data
Escape and Rescue Systems
Lodging Systems



Access Hardware Solutions

Door Closers
Architectural Hardware
Mechanical Key Systems



Services

Technical Support
Installation and commissioning
Maintenance and Repair



Key & Wall Solutions

Key Systems
Movable / Sliding Walls



Safe Locks

Electronic Safe Locks
Mechanical Safe Locks
Boltworks and Accessories



Glass systems

Manual door systems
Glass fittings
Horizontal Sliding Walls

Nosso Compromisso com a Sustentabilidade

Estamos comprometidos em promover o desenvolvimento sustentável em toda a nossa cadeia de valor, em linha com nossas responsabilidades econômicas, ambientais e sociais para com as gerações atuais e futuras. A sustentabilidade em nível de produto é uma abordagem importante e voltada para o futuro na área da construção. Para fornecer divulgações quantificadas do impacto ambiental de um produto ao longo de todo o seu ciclo de vida, a dormakaba fornece Declarações Ambientais de Produto (DAP), baseadas em avaliações holísticas do ciclo de vida.

<https://www.dormakabagroup.com/en/sustainability/product-declarations>.

Guia de Arquitetura e Segurança de TI do Sistema Axessor
Apexx - RevB
Sujeito a alterações sem aviso prévio

Dormakaba SAL GmbH

Siemensstrasse 33
42551 Velbert
safelocks.de@dormakaba.com
T +49 2051 9111 0

dormakaba USA Inc.

1525 Bull Lea Road, Suite 100
Lexington, KY 460511
sales.safelocks.us@dormakaba.com
1-800-950-4744



AXESSOR APEXX IP
INSTALLATION AND
OPERATION GUIDES

dk.world/AxessorApexxIP