

# Select a Language

- **EN** - Apexx System Architecture
- **ES** - Apexx Arquitectura del sistema
- **FR** - Architecture du système
- **DE** - Apexx Systemarchitektur
- **IT** - Apexx Architettura del sistema
- **PT** - Arquitetura do sistema do Apexx
- **PL** - Architektura systemu Apexx

# Axessor Apexx System Architecture



# Table of Contents

- Apexx System Architecture - Overview ..... 2
- Apexx API ..... 2
- Apexx Client Software ..... 2
- Apexx Database ..... 2
- MQTT Broker/Server ..... 3
- SMTP ..... 3
- SSO ..... 3
- User Configuration ..... 3
- Licenses ..... 4
- Local vs Remote Firmware Updates ..... 4
- Data Transit ..... 5
- Security & Data Encryption ..... 6
- Public Key Infrastructure (PKI) ..... 6
- Computer Hardware Configurations ..... 7
- Database Considerations ..... 10
- Apexx Recommended Computer Specifications ..... 10

# Apexx System Architecture

## Overview

Apexx locking systems can be broken into 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 bridge between the Lock System and the API/Software

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

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

## 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 is a graphical user interface (GUI) that allows Software Users to use the API to perform actions in the 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.

## SMTP

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

- 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.

## 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

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

**Safe Lock Users** are users who will be utilizing the Lock System (consisting of the physical Keypads, Locks, eBox, etc.), 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.

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.

**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). Software Users who have a Software User "Write" permission can add new Software Users and configure the read/write permissions.

## Licenses

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

### Local vs Remote Firmware Updates

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

The "Apexx Local" license allows for local firmware updates only, which can be done by establishing a temporary USB connection between the computer hosting the Apexx Series Software and the Keypad of your lock system.

The "Apexx IP" license allows you to perform **Remote Firmware Updates**, that 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.

For more information on the firmware update process, consult the **Axessor Apexx System User Guide** and the **Apexx Series Software's** help menu.

# Data Transit

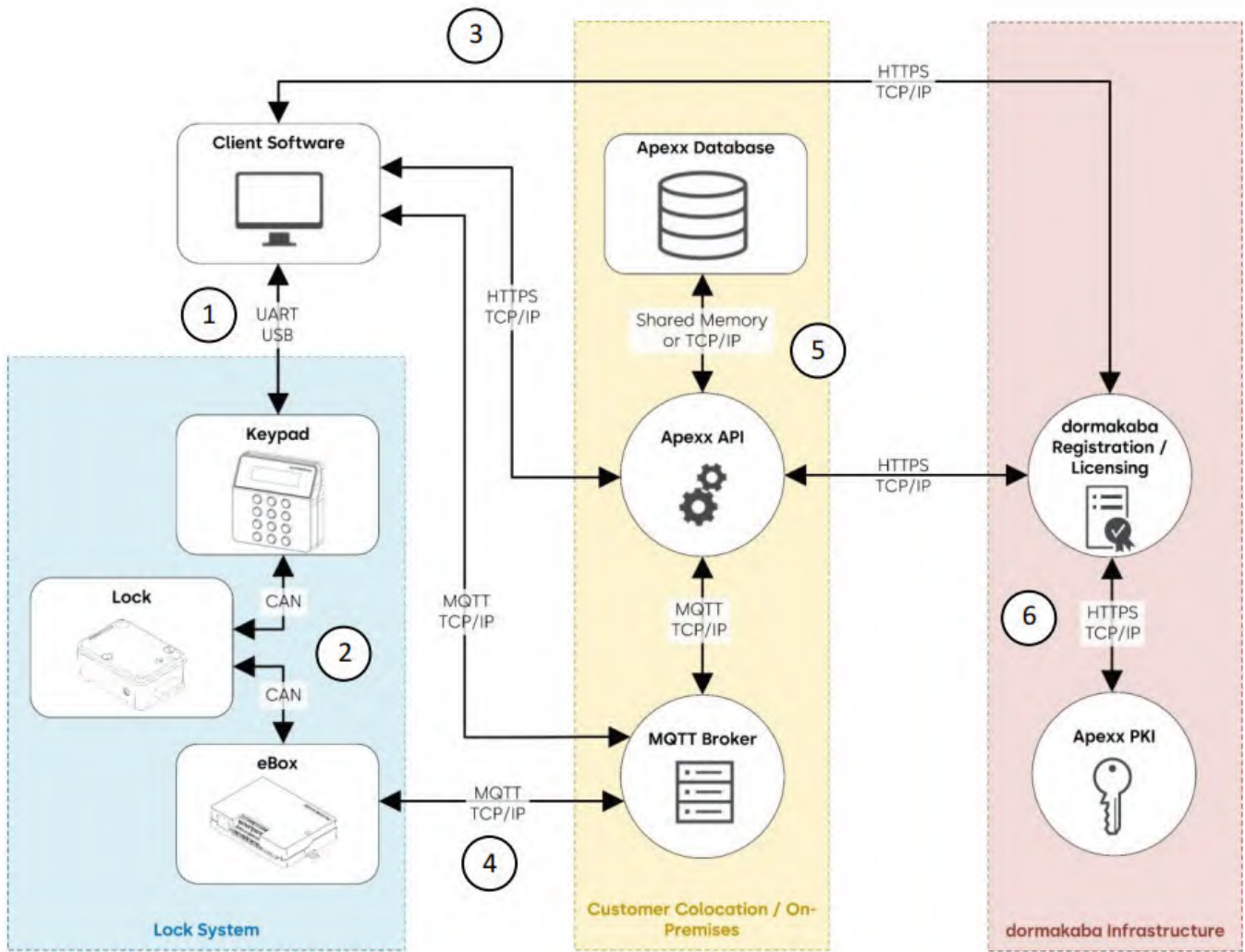


Figure 1 - Apex System Architecture - System Components and Data Transit

	Communication Protocols	Data flow	Description / Purpose
1	UART over USB	Bidirectional path: <ul style="list-style-type: none"> <li>Client Software to Keypad</li> </ul>	Direct configuration and audit retrieval
2	CAN	Bidirectional path: <ul style="list-style-type: none"> <li>Keypad to Lock</li> <li>Lock to eBox</li> </ul>	Device-to-device communication
3	HTTPS over TCP/IP	Bidirectional path: <ul style="list-style-type: none"> <li>Client Software to dormakaba Registration/Licensing</li> </ul>	Online licensing and registration
4	MQTT over TCP/IP	Bidirectional path: <ul style="list-style-type: none"> <li>Client Software to MQTT Broker</li> </ul> Bidirectional path: <ul style="list-style-type: none"> <li>eBox to MQTT Broker</li> </ul>	Networked configuration and audit retrieval
5	Shared memory or TCP/IP	Bidirectional path: <ul style="list-style-type: none"> <li>Apex API to Apex Database</li> </ul>	Persistent data storage with SQL Server

Bidirectional path:

- Client Software to Apexx API
- Apexx API to dormakaba Registration/Licensing
- dormakaba Registration/Licensing to Apexx PKI

x.509 certificate issuance

## Security & Data Encryption

The Apexx System employs 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 System utilizes a Public Key Infrastructure to create, store, and distribute digital certificates to Apexx devices via a certificate authority.

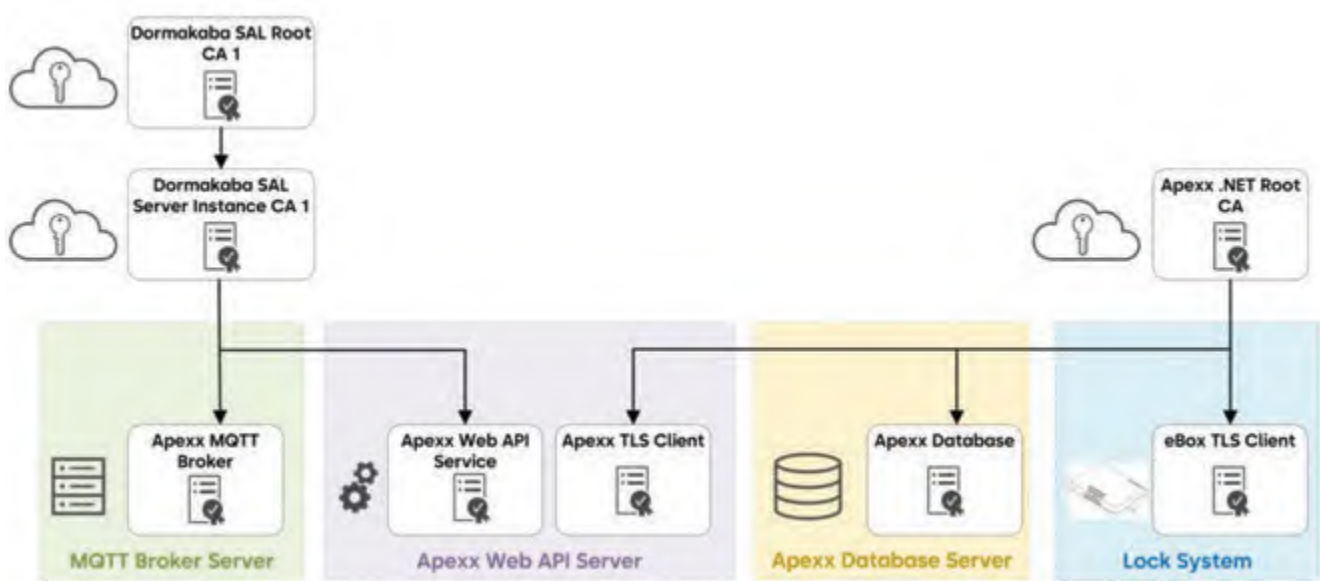


Figure 2 – Public Key Infrastructure

Certificate Type	Description
dormakaba SAL Root CA	<ul style="list-style-type: none"> <li>• This certificate is preloaded on the devices at the factory and replaced via firmware update</li> </ul>
dormakaba SAL Server Instance CA	<ul style="list-style-type: none"> <li>• Servers running local software services for Apexx require certificates signed by the dormakaba SAL PKI for devices to trust them</li> <li>• This certificate must be deployed to all servers running local software services</li> <li>• The local software PKI signs certificate requests for all clients of the MQTT broker.</li> <li>• Those certificates are used for both establishing mutual trust Transport Layer Security (TLS) connections and authentication with the MQTT broker.</li> <li>• It can also sign the certificates used by SQL Server for TLS.</li> <li>• If all services are hosted on a single server, multiple certificates are not required to be signed by the Dormakaba SAL PKI.</li> <li>• Even the database can use that certificate if hosted on the same server.</li> </ul>



<b>Apexx MQTT Broker</b>	<ul style="list-style-type: none"> <li>• Created during software installation</li> <li>• Used for TLS connections and authentication</li> </ul>
<b>Apexx Web API Service</b>	<ul style="list-style-type: none"> <li>• Created during software installation</li> <li>• Contains the server's name (computer where this service is installed), the trusted certificate authority, and the server's public encryption key</li> </ul>
<b>Apexx TLS Client</b>	<ul style="list-style-type: none"> <li>• Used for authentication of the Apexx Client</li> <li>• The certificate is a verified user if the issuer matches the installed Apexx .NET Root CA installed on the broker server</li> </ul>
<b>Apexx Database</b>	<ul style="list-style-type: none"> <li>• SQL Server on Windows is the only supported database engine</li> <li>• The following settings are enabled on the instance/database: <ul style="list-style-type: none"> <li>• Windows Authentication</li> </ul> </li> <li>• Role-based access control (RBAC) is used within, along with Windows Authentication to control permissions</li> </ul>
<b>eBox TLS Client</b>	<ul style="list-style-type: none"> <li>• Used for authentication of the eBox</li> <li>• The certificate is a verified user if the issuer matches the installed Apexx .NET Root CA installed on the broker server</li> </ul>
<b>Apexx .NET Root CA</b>	<ul style="list-style-type: none"> <li>• Created during software installation</li> <li>• Any computer running the software (client, server, database, etc.) requires a copy of this certificate for security/identification purposes</li> </ul>

## 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 setups. Refer to the Axessor Apexx Price Book 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.

Figure 3 illustrates a basic setup involving just a single computer and one Apexx 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 Apexx Locking System for programming/system configuration purposes.

This sort of 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.

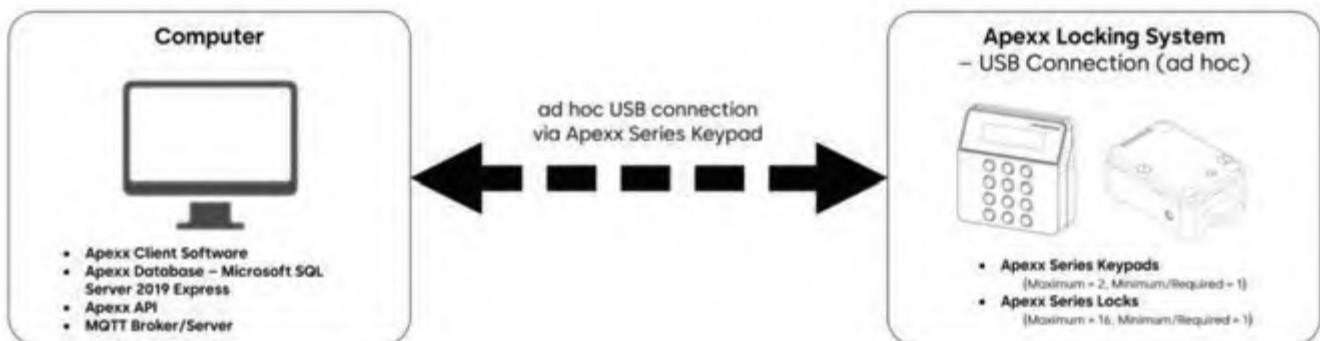


Figure 3 – Single Computer Setup - ad hoc USB connection

Figure 4 shows another simple setup involving just one computer and one Apex Locking System, but this time the Apex eBox is used to provide a network/IP connection for continuous/live communication between the computer and locking system.

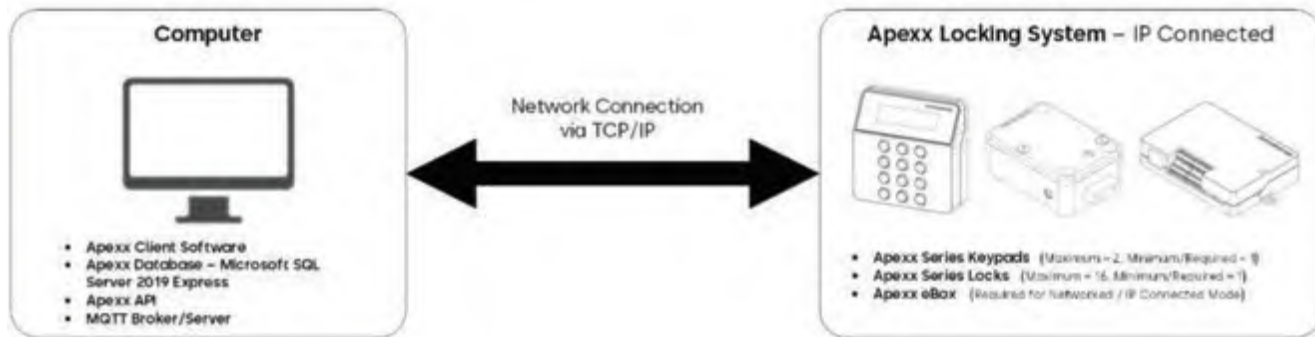


Figure 4 – Single Computer setup - Network via eBox (TCP/IP)

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)

For larger sites involving bigger buildings and/or multiple Locking Systems, the multiple-computer setup shown in Figure 5 offers additional flexibility.

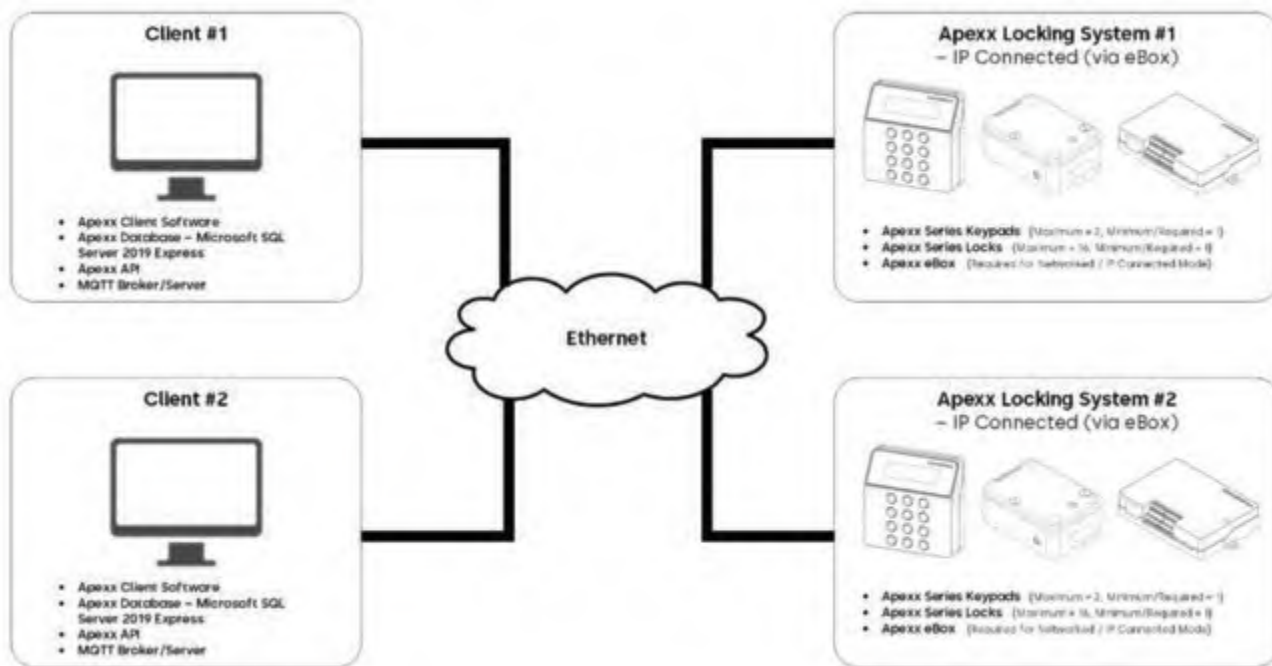


Figure 5 – Multiple Computer Setup with Multiple Locking Systems

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 locking system connects to the network via an Apex eBox.

This concept is expanded further in the system shown in Figure 6, which includes multiple computers and lock systems spread out over multiple buildings.

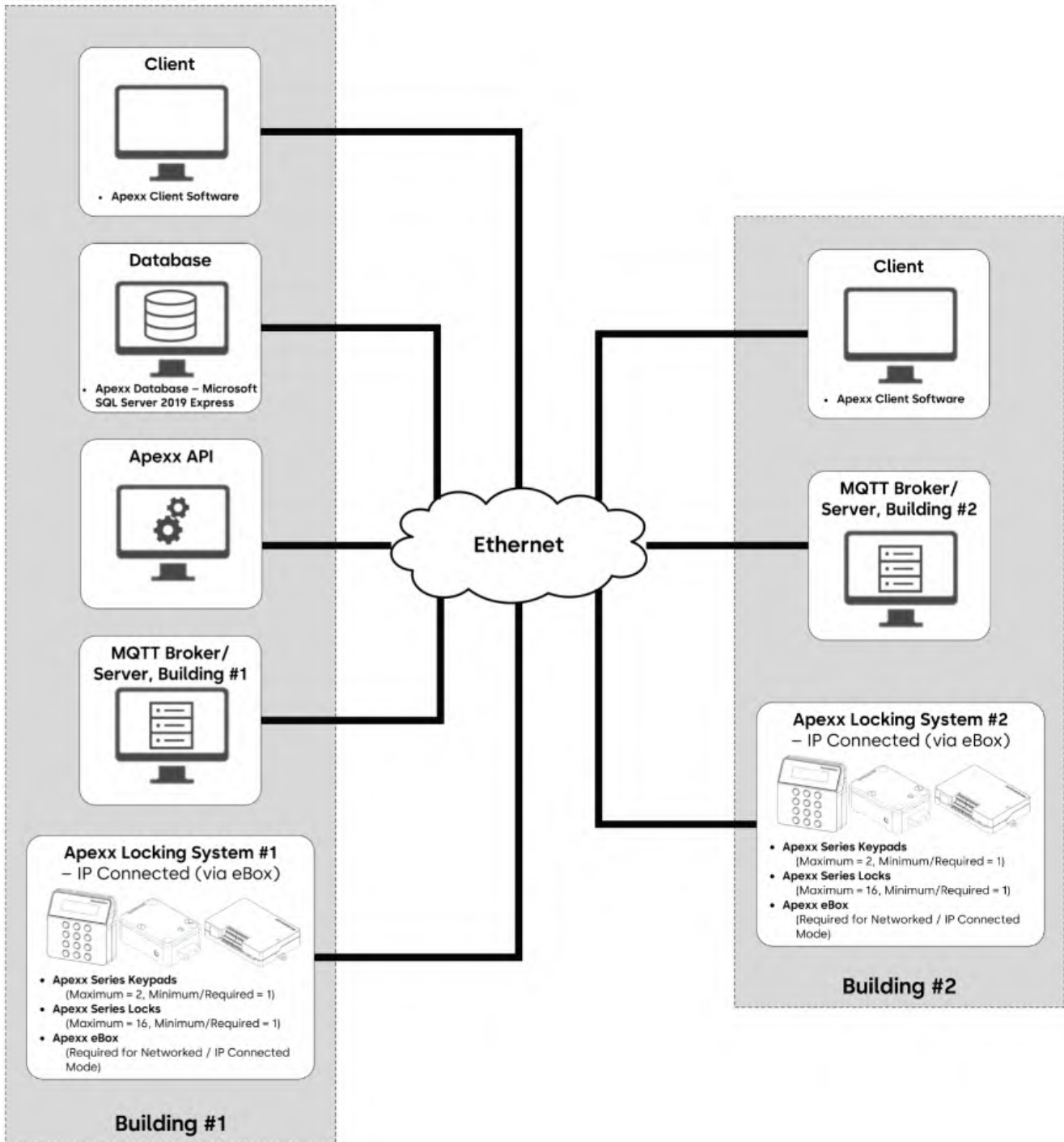


Figure 6 – Multiple Computer/Locking System Setup with multi-server setup

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 Apex API and Apex 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 Apex 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 Recommended Computer Specifications

### Apexx Client Workstation

- Intel Core i7 – 4470 3.40GHz with 4 cores
- 16GB RAM 1600MHz DDR3 NON-ECC
- 500GB Hard Drive
- Windows 10 Professional 64bit
- AMD RADEON HD 8490 1GB Dual Monitor or AMD RADEON HD8570 1GB Dual Monitor
- USB 2.0 Ports
- Ethernet Port - 1Gb Network Card
- Keyboard & Mouse
- UPS Backup

### Apexx Broker Server

- Intel Xeon E5 – 2403, 1.80GHz, 10MB Cache
- 16GB RAM 1333MHz, RDIMM
- 500GB Hard Drive
- Windows 2019 Server Standard 64bit
- Integrated HD Graphics Card
- Ethernet Port – 1Gb Network Card
- Keyboard & Mouse
- UPS Backup

### Apexx Database Server & Apexx API

- Intel Xeon E5 – 2420, 1.90GHz, 15MB Cache with 6 cores
- 32GB RAM 1333MHz, RDIMM
- 2 x 1TB 7.2K RPM SATA 3Gbps 3.5in Hard Drive
- RAID 1 Configuration
- Dual, Hot-Plug, Redundant Power Supply
- Windows 2019 Server Standard 64bit
- Integrated HD Graphics Card
- Ethernet Port – Gb Network Card
- Keyboard & Mouse
- UPS Backup

## 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.

[www.dormakaba.com/sustainability](http://www.dormakaba.com/sustainability)



## Our offering

### 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



Apexx System Architecture, EN, 02/2024  
Subject to change without notice

### dormakaba USA Inc.

1525 Bull Lea Road, Suite 100  
Lexington, KY 40511  
[sales.safelocks.us@dormakaba.com](mailto:sales.safelocks.us@dormakaba.com)  
T +1 800 950 4744  
+1 888 950 4715 (tech support)  
[dormakaba.com](http://dormakaba.com)

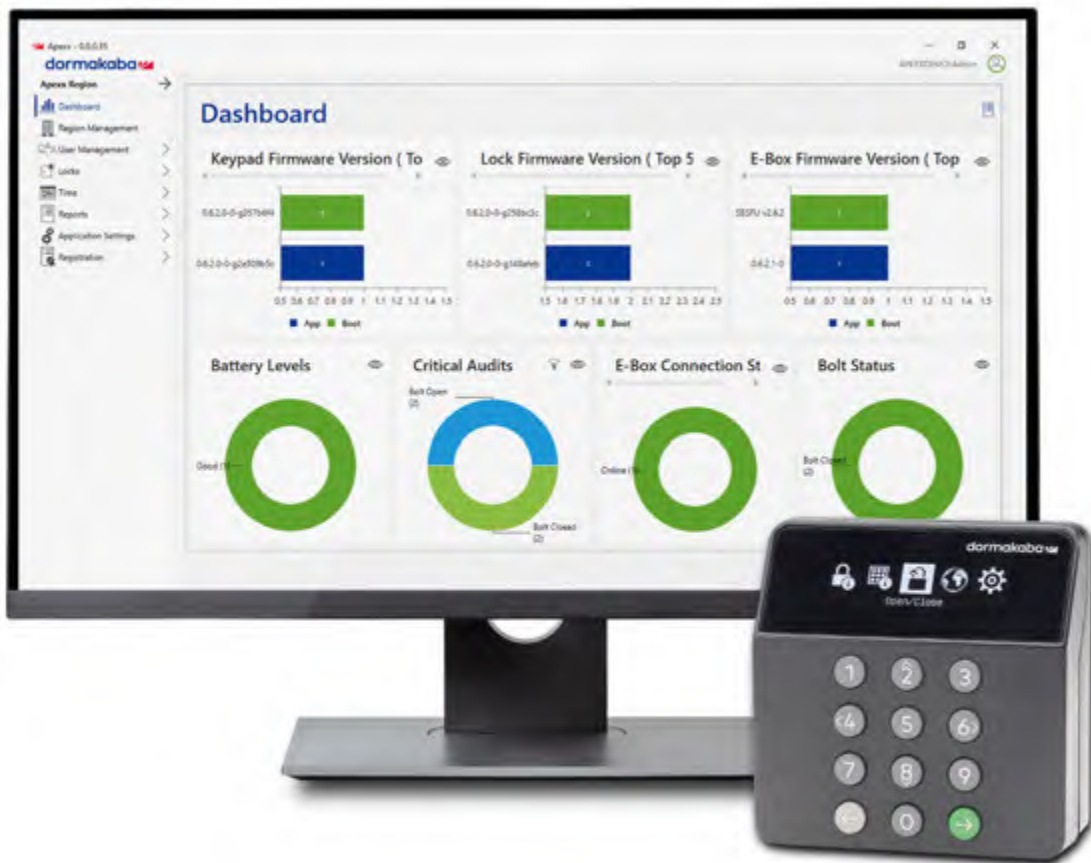


AXESSOR APEXX IP  
INSTALLATION AND  
OPERATION GUIDES

[dk.world/AxessorApexxIP](http://dk.world/AxessorApexxIP)

# Arquitectura del sistema

# Axessor Apexx



# Índice

- Arquitectura del sistema Apexx - Resumen ..... 2
- API Apexx..... 2
- Software de cliente Apexx ..... 2
- Base de datos Apexx ..... 2
- Bróker/Servidor MQTT ..... 3
- SMTP..... 3
- SSO..... 3
- Configuración de usuarios ..... 3
- Licencias ..... 4
- Actualizaciones de firmware locales y remotas..... 4
- Tránsito de datos ..... 5
- Seguridad y cifrado de datos ..... 6
- Infraestructura de clave pública (PKI)..... 6
- Configuraciones del hardware informático ..... 7
- Consideraciones sobre la base de datos ..... 10
- Especificaciones de ordenador recomendadas por Apexx ..... 10



# Arquitectura del sistema Apexx

## Resumen

Los sistemas de bloqueo Apexx pueden dividirse en 2 redes de comunicación seguras: **el sistema de bloqueo bus CAN y la red de API/software.**

**El bus CAN del sistema de bloqueo** 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 Apexx** (obligatoria para el modo de conexión a la red/IP)
  - Sirve como un puente entre el sistema de bloqueo y la API/software

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

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

## 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 es una interfaz gráfica de usuario (GUI) que permite a los usuarios del software utilizar la API para realizar acciones en el sistema (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.

## SMTP

el software de la serie Apexx utiliza el protocolo simple de transferencia de correo (SMTP) para enviar alertas activas e informes programados.

- 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.

## 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 usuarios

Los usuarios del sistema 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 (compuesto por los teclados numéricos, las cerraduras, la eBox, etc.) y tendrán credenciales y funciones exclusivas con permisos que determinarán su acceso al sistema de bloqueo.

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.

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.

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

## 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 para obtener más información.

## Actualizaciones de firmware locales y remotas

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

La licencia «Apexx Local» solo permite actualizaciones locales de firmware, que pueden realizarse estableciendo una conexión USB temporal entre el ordenador que aloja el software de la serie Apexx y el teclado de su sistema de cerradura.

La licencia «Apexx IP» le permite realizar **actualizaciones remotas de firmware** 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.

Para más información sobre el proceso de actualización del firmware, consulte la **Guía del usuario del sistema Axessor Apexx** y el menú de ayuda del **software de la serie Apexx**.

# Tránsito de datos

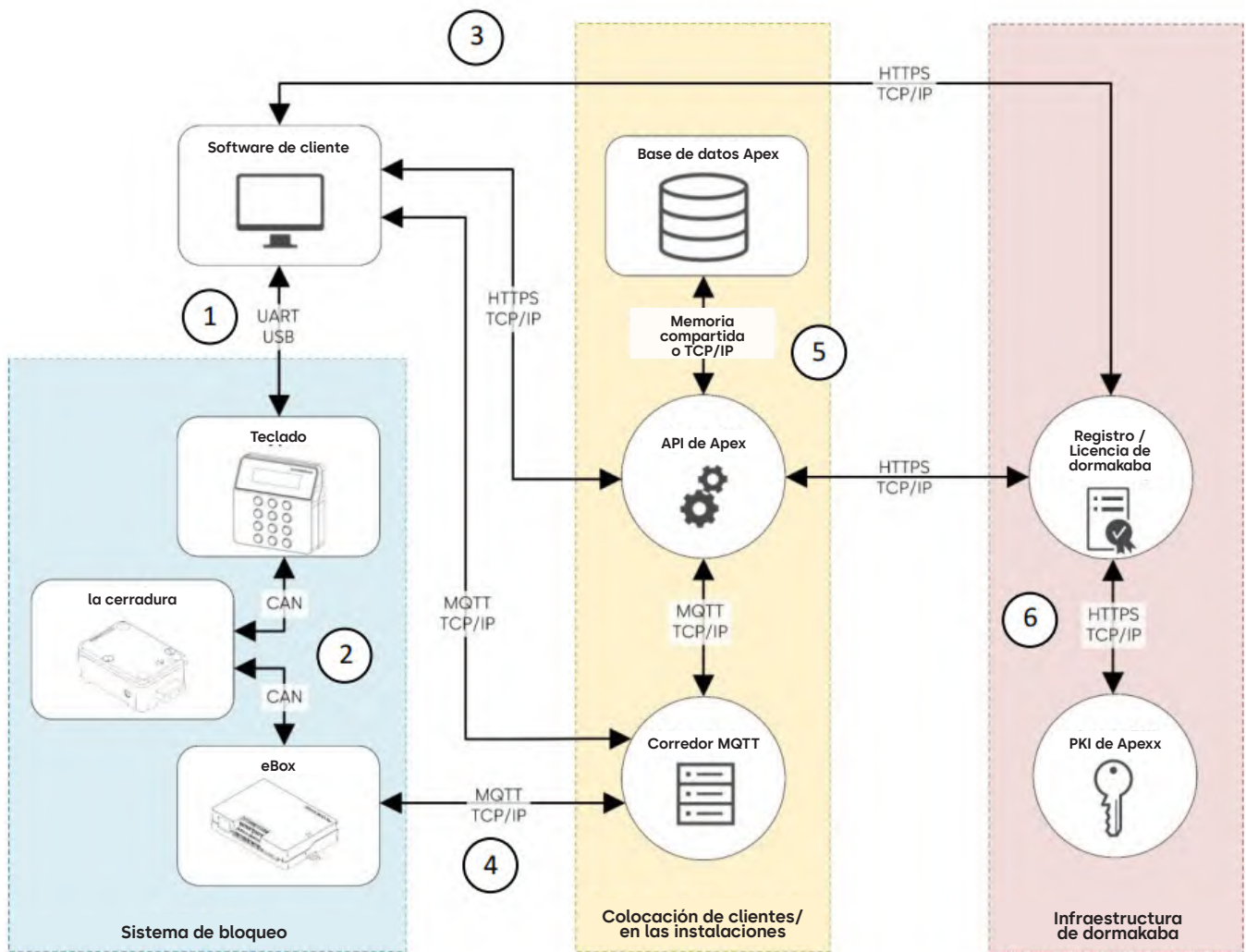


Figura 1: Arquitectura del sistema Apex - Componentes del sistema y tránsito de datos

	Protocolos de comunicación	Flujo de datos	Descripción / Finalidad
1	UART a USB	Ruta bidireccional: <ul style="list-style-type: none"> <li>Software de cliente a teclado numérico</li> </ul>	Configuración directa y recuperación de auditorías
2	CAN	Ruta bidireccional: <ul style="list-style-type: none"> <li>Teclado numérico a cerradura</li> <li>Cerradura a eBox</li> </ul>	Comunicación entre dispositivos
3	HTTPS a TCP/IP	Ruta bidireccional: <ul style="list-style-type: none"> <li>Software de cliente a registro/licencias dormakaba</li> </ul>	Licencias y registro en línea
4	MQTT a TCP/IP	Ruta bidireccional: <ul style="list-style-type: none"> <li>Software de cliente a bróker MQTT</li> </ul> Ruta bidireccional: <ul style="list-style-type: none"> <li>eBox a bróker MQTT</li> </ul>	Configuración en red y recuperación de auditorías
5	Memoria compartida o TCP/IP	Ruta bidireccional: <ul style="list-style-type: none"> <li>API Apex a base de datos Apex</li> </ul>	Almacenamiento persistente de datos con SQL Server

	Protocolos de comunicación	Flujo de datos	Descripción / Finalidad
6	HTTPS a TCP/IP	Ruta bidireccional: <ul style="list-style-type: none"> <li>• Software de cliente a API Apexx</li> <li>• API Apexx a registros/licencias dormakaba</li> <li>• Registros/licencias dormakaba a PKI Apexx</li> </ul>	Emisión de certificados x.509

## Seguridad y cifrado de datos

El sistema Apexx emplea varios métodos de cifrado, como AES256, PBKDF2 y certificados TLS, para garantizar la seguridad de la comunicación y el almacenamiento de datos.

## Infraestructura de clave pública (PKI)

El sistema Apexx utiliza una infraestructura de clave pública para crear, almacenar y distribuir certificados digitales a los dispositivos Apexx a través de una autoridad de certificación.

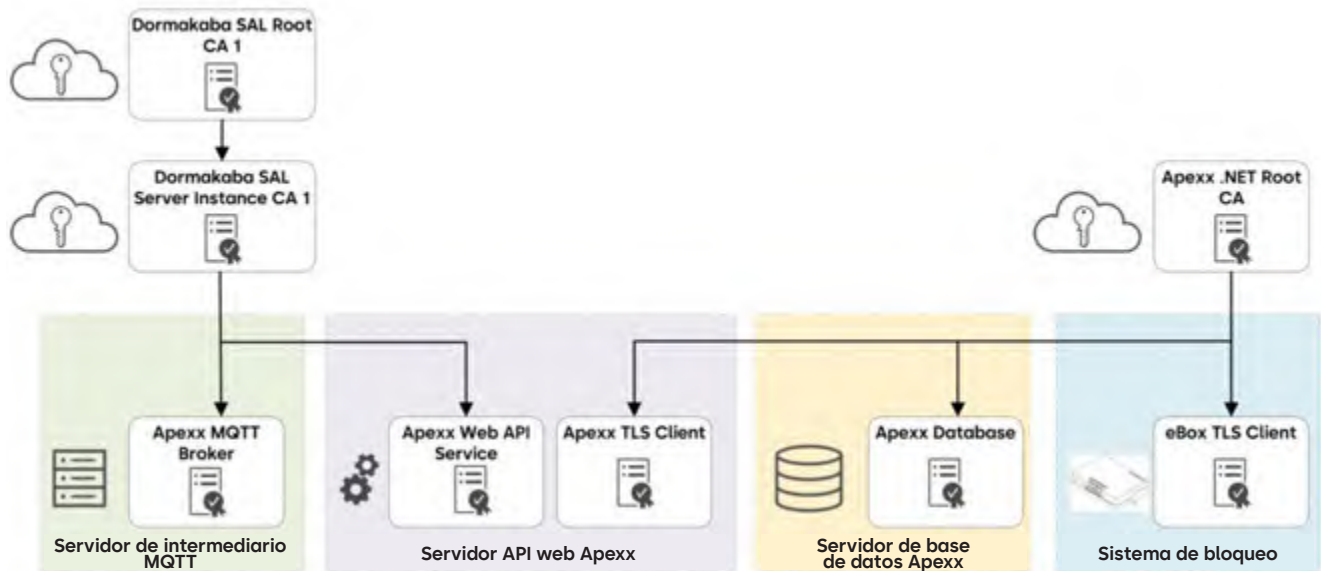


Figura 2: Infraestructura de clave pública

Tipo de certificado	Descripción
<b>Autoridad de certificación raíz SAL dormakaba</b>	<ul style="list-style-type: none"> <li>• Este certificado viene instalado de fábrica en los dispositivos y se sustituye mediante actualización del firmware</li> </ul>
<b>Autoridad de certificación de la instancia de servidor SAL dormakaba</b>	<ul style="list-style-type: none"> <li>• 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</li> <li>• Este certificado debe instalarse en todos los servidores que ejecuten servicios de software locales</li> <li>• La PKI del software local firma las solicitudes de certificados para todos los clientes del bróker MQTT</li> <li>• Estos certificados se utilizan tanto para establecer conexiones TLS (Transport Layer Security) de confianza mutua como para la autenticación con el bróker MQTT</li> <li>• También puede firmar los certificados utilizados por SQL Server para TLS</li> <li>• Si todos los servicios están alojados en un único servidor, no es necesario que la PKI SAL dormakaba firme varios certificados</li> <li>• La base de datos también puede utilizar ese certificado si se aloja en el mismo servidor</li> </ul>

Tipo de certificado	Descripción
<b>Bróker MQTT Apexx</b>	<ul style="list-style-type: none"> <li>• Se crea durante la instalación del software</li> <li>• Se utiliza para conexiones TLS y autenticación</li> </ul>
<b>Servicio API Web Apexx</b>	<ul style="list-style-type: none"> <li>• Se crea durante la instalación del software</li> <li>• 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</li> </ul>
<b>Cliente TLS Apexx</b>	<ul style="list-style-type: none"> <li>• Se utiliza para la autenticación del cliente Apexx</li> <li>• El certificado es un usuario verificado si el emisor coincide con la autoridad de certificación raíz Apexx .NET instalada en el servidor bróker</li> </ul>
<b>Base de datos Apexx</b>	<ul style="list-style-type: none"> <li>• SQL Server en Windows es el único motor de base de datos compatible</li> <li>• Los siguientes ajustes están activados en la instancia/base de datos: <ul style="list-style-type: none"> <li>• Autenticación de Windows</li> </ul> </li> <li>• El control de acceso basado en roles (RBAC) se utiliza junto con la autenticación de Windows para controlar los permisos</li> </ul>
<b>Cliente TLS de eBox</b>	<ul style="list-style-type: none"> <li>• Se utiliza para la autenticación de la eBox</li> <li>• El certificado es un usuario verificado si el emisor coincide con la autoridad de certificación raíz Apexx .NET instalada en el servidor bróker</li> </ul>
<b>Autoridad de certificación raíz .NET Apexx</b>	<ul style="list-style-type: none"> <li>• Se crea durante la instalación del software</li> <li>• Cualquier ordenador que ejecute el software (cliente, servidor, base de datos, etc.) necesita una copia de este certificado por motivos de seguridad/identificación</li> </ul>

## Configuraciones del hardware informático

La parte 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 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.

La figura 3 ilustra una configuración básica con un solo ordenador y un sistema de bloqueo Apexx. 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 Apexx con fines de programación/configuración del sistema.

Este tipo de configuración funciona bien en lugares pequeños en los que el ordenador y todos los componentes del sistema de bloqueo (teclados 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 Apexx.



Figura 3: Configuración de un solo ordenador - Conexión USB ad hoc

La figura 4 muestra otra configuración sencilla en la que solo intervienen un ordenador y un sistema de bloqueo Apexx, pero esta vez se utiliza la eBox Apexx para proporcionar una conexión de red/IP para la comunicación continua/en directo entre el ordenador y el sistema de bloqueo.

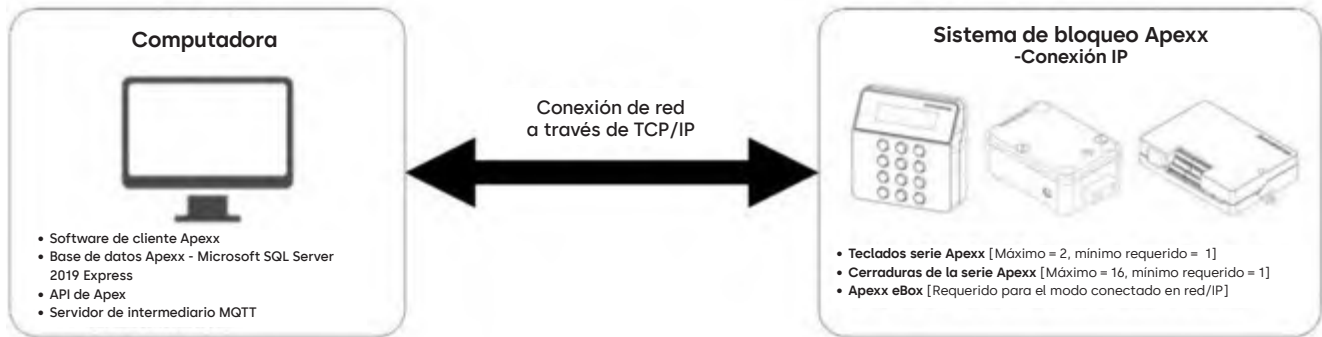


Figura 4: Configuración de un solo ordenador - Red a través de eBox (TCP/IP)

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).

Para instalaciones de mayor tamaño, con edificios más grandes y/o varios sistemas de bloqueo, la configuración de varios ordenadores que se muestra en la figura 5 ofrece una flexibilidad adicional.

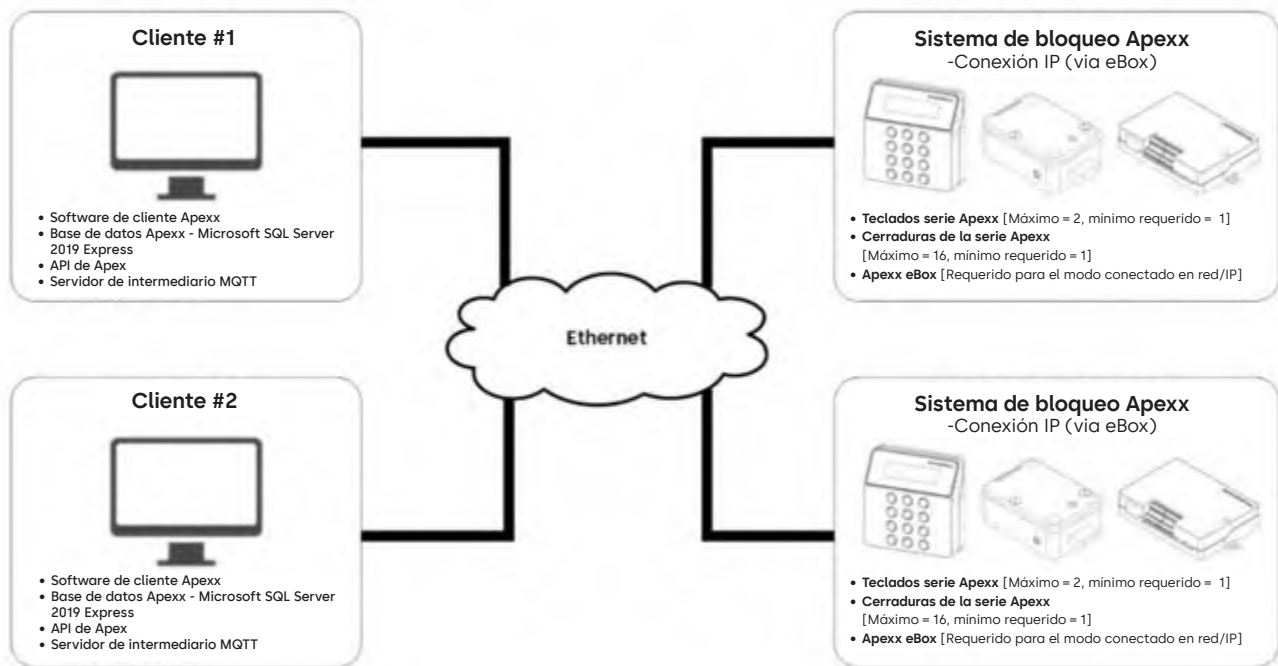


Figura 5: Configuración de varios ordenadores con varios sistemas de bloqueo

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 se conecta a la red a través de una eBox Apexx.

Este concepto se amplía aún más en el sistema de la figura 6, que incluye varios ordenadores y sistemas de bloqueo repartidos por varios edificios.



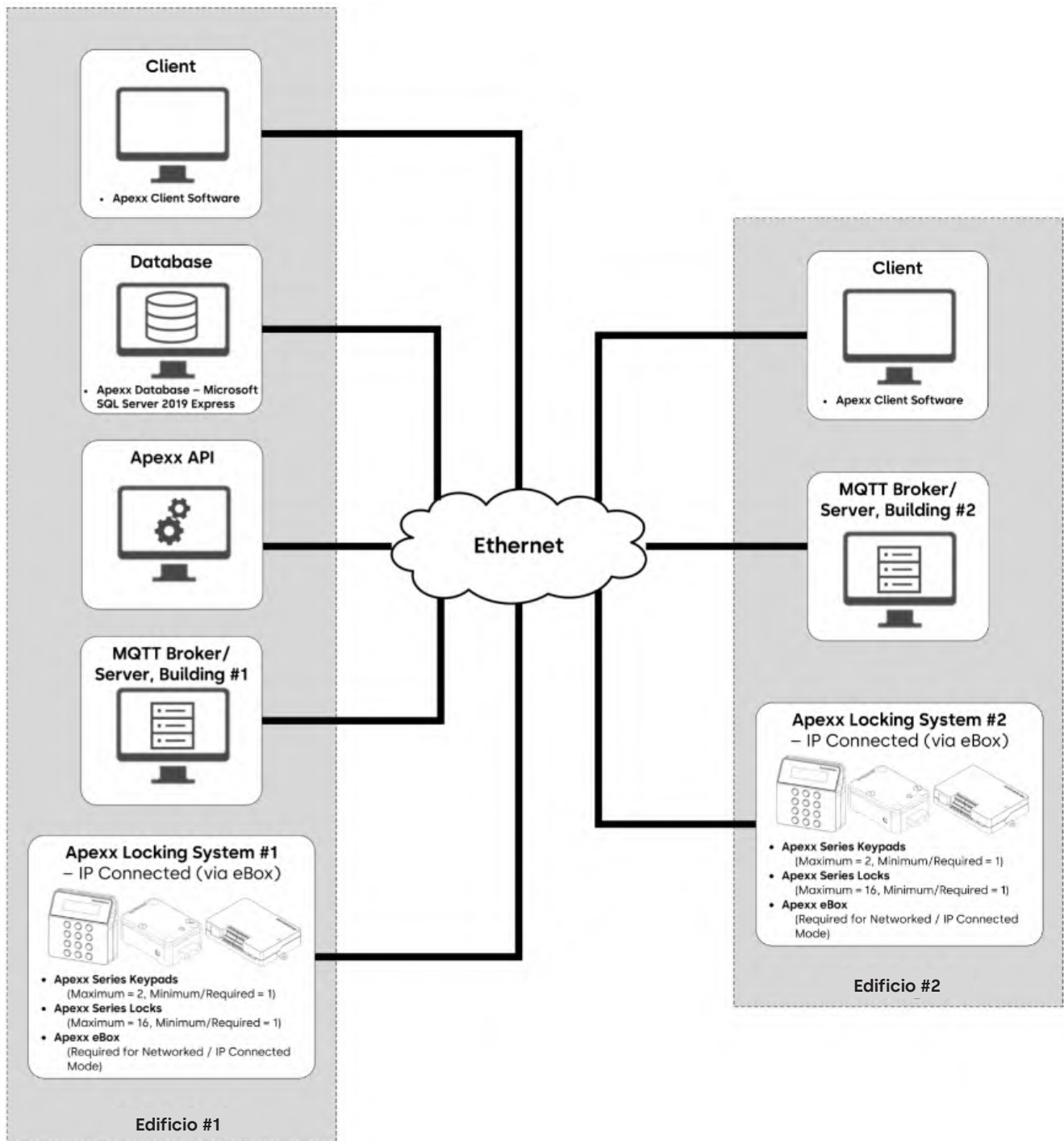


Figura 6: Configuración de varios ordenadores/sistemas de bloqueo con configuración multiservidor

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 ser configurados para ser utilizados como API y base de datos para los sistemas de bloqueo en el edificio n.º1, edificio n.º 2, y/o cualquier otro sistema Apexx 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 de ordenador recomendadas por Apexx

### Estación de trabajo del cliente Apexx

- Intel Core i7 - 4470 a 3,40 GHz con 4 núcleos
- 16 GB RAM 1600 MHz DDR3 NON-ECC
- Disco duro de 500 GB
- Windows 10 Professional (64 bits)
- AMD RADEON HD 8490 1 GB Dual Monitor o AMD RADEON HD8570 1 GB Dual Monitor
- Puertos USB 2.0
- Puerto Ethernet - Tarjeta de red de 1 GB
- Teclado numérico y ratón
- Copia de seguridad UPS

### Servidor del bróker Apexx

- Intel Xeon E5 - 2403, 1,80 GHz, 10 MB de caché
- 16 GB de RAM a 1333 MHz, RDIMM
- Disco duro de 500 GB
- Windows 2019 Server Standard (64 bits)
- Tarjeta gráfica HD integrada
- Puerto Ethernet - Tarjeta de red de 1 GB
- Teclado numérico y ratón
- Copia de seguridad UPS

### Servidor de base de datos Apexx y API Apexx

- Intel Xeon E5 - 2420, 1,90 GHz, 15 MB de caché con 6 núcleos
- 32 GB de RAM a 1333 MHz, RDIMM
- 2 x 1 TB 7.2K RPM SATA 3 GBPS 3,5 pulgadas disco duro
- Configuración RAID 1
- Doble fuente de alimentación redundante con conexión en caliente
- Windows 2019 Server Standard (64 bits)
- Tarjeta gráfica HD integrada
- Puerto Ethernet - Tarjeta de red GB
- Teclado numérico y ratón
- Copia de seguridad UPS



## Nuestro compromiso con la sostenibilidad

Nos comprometemos a promover un desarrollo sostenible, junto con toda nuestra cadena de valores acorde con las responsabilidades económicas, medioambientales y sociales que tenemos para con las generaciones presentes y futuras. La sostenibilidad a nivel de producto es un enfoque importante y orientado al futuro en el ámbito de la construcción. Con el fin de proporcionar información cuantificada sobre el impacto medioambiental de un producto a lo largo de todo su ciclo de vida, dormakaba ofrece declaraciones medioambientales de producto (DMP), basadas en evaluaciones holísticas del ciclo de vida.

[www.dormakaba.com/sustainability](http://www.dormakaba.com/sustainability)



## Nuestra oferta

### Soluciones de automatización de accesos

Automatización de entradas  
Seguridad de entradas



### Soluciones de control de accesos

Acceso electrónico y datos  
Sistemas de evacuación y rescate  
Sistemas de alojamiento



### Soluciones de hardware de acceso

Muelles de puertas  
Hardware de arquitectura  
Sistemas mecánicos de llaves



### Servicios

Servicio técnico  
Instalación y activación  
Mantenimiento y reparación



### Soluciones de llave y pared

Sistemas de llave  
Paredes móviles / correderas



### Cerraduras de caja fuerte

Cerraduras electrónicas de caja fuerte  
Cerraduras mecánicas de caja fuerte  
Tornillería y accesorios



### Sistemas de vidrio

Sistemas de puertas manuales  
Accesorios de vidrio  
Paredes correderas horizontales



Apexx System Architecture, ES, 02/2024  
Sujeto a cambios sin previo aviso

### dormakaba USA Inc.

1525 Bull Lea Road, Suite 100  
Lexington, KY 40511, EE. UU.  
[sales.safelocks.us@dormakaba.com](mailto:sales.safelocks.us@dormakaba.com)  
T +1 800 950 4744  
+1 888 950 4715 (Servicio técnico)  
[dormakaba.com](http://dormakaba.com)

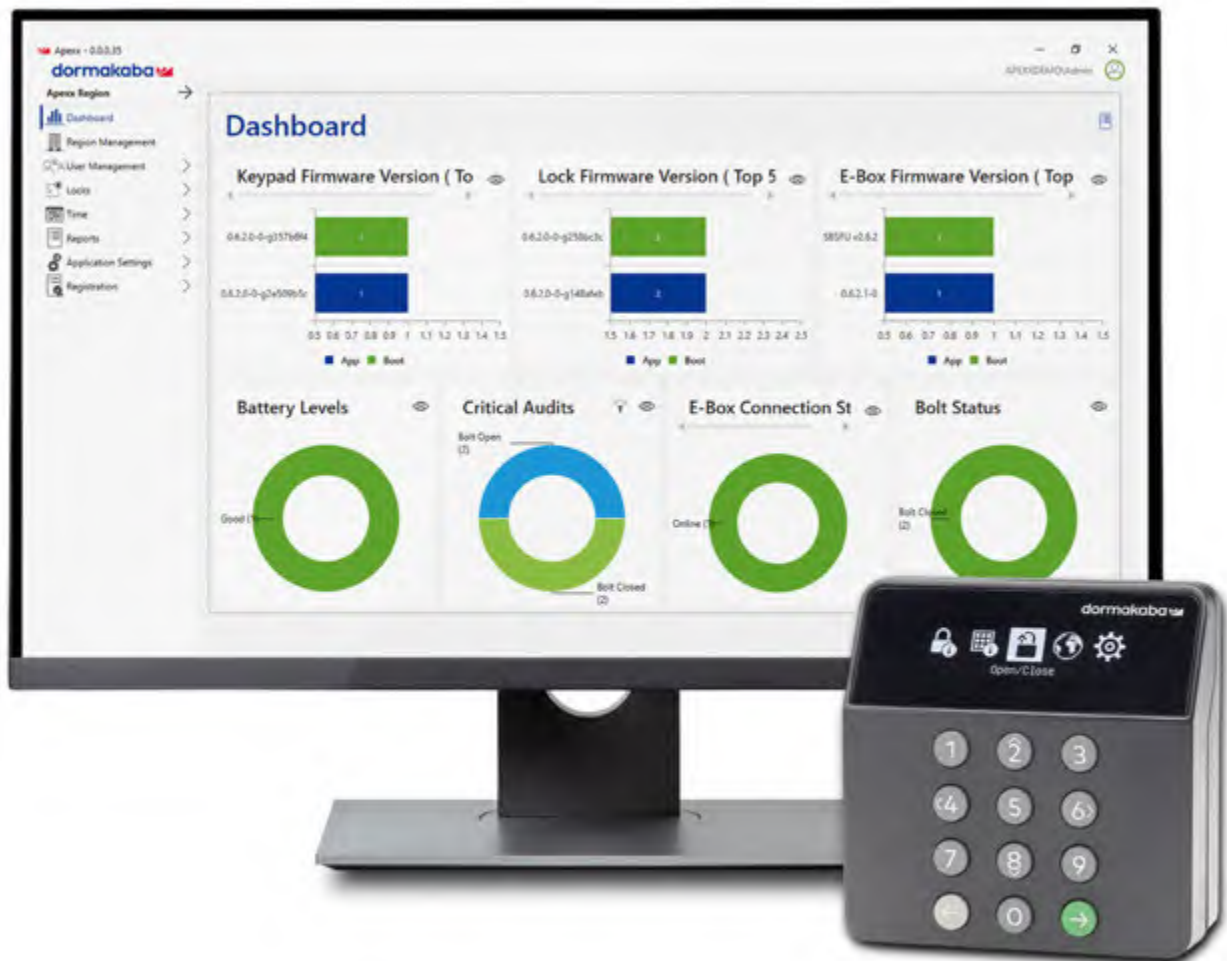


AXESSOR APEXX IP  
INSTALLATION AND  
OPERATION GUIDES

[dk.world/AxessorApexxIP](http://dk.world/AxessorApexxIP)

# Axessor Apexx

## Architecture du système



# Table des matières

Architecture du système Apexx – Vue d'ensemble . . . . .	3
API Apexx. . . . .	3
Logiciel client Apexx. . . . .	3
Base de données Apexx. . . . .	3
Broker/serveur MQTT . . . . .	3
SMTP. . . . .	4
SSO. . . . .	4
Configuration de l'utilisateur. . . . .	4
Licences. . . . .	4
Mises à jour locales ou à distance du firmware. . . . .	4
Transit des données . . . . .	5
Sécurité et chiffrement des données. . . . .	6
Infrastructure à clé publique (PKI) . . . . .	6
Configurations du matériel informatique . . . . .	7
Points à prendre en considération concernant la base de données. . . . .	10
Spécifications informatiques recommandées par Apexx. . . . .	10

# Architecture du système Apexx

## Présentation

Les systèmes de verrouillage Apexx peuvent être divisés en 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 une passerelle entre le système de serrures et l'API/le logiciel

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

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

## 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 est une interface utilisateur graphique (GUI) qui permet à ses utilisateurs de se servir de l'API pour effectuer des actions dans le système (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.

## SMTP

Le logiciel de la série Apexx utilise le protocole de communication SMTP (Simple Mail Transport Protocol) pour envoyer les éléments suivants : les alertes actives et les rapports programmés.

- 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.

## 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 de l'utilisateur

Les utilisateurs du système 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 (composé des claviers physiques, des serrures, de l'eBox, etc.), 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.

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.

Les **utilisateurs du logiciel** désignent les personnes 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 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.

## 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 le Catalogue de prix Axessor Apexx IP.

## Mises à jour locales ou à distance du firmware

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

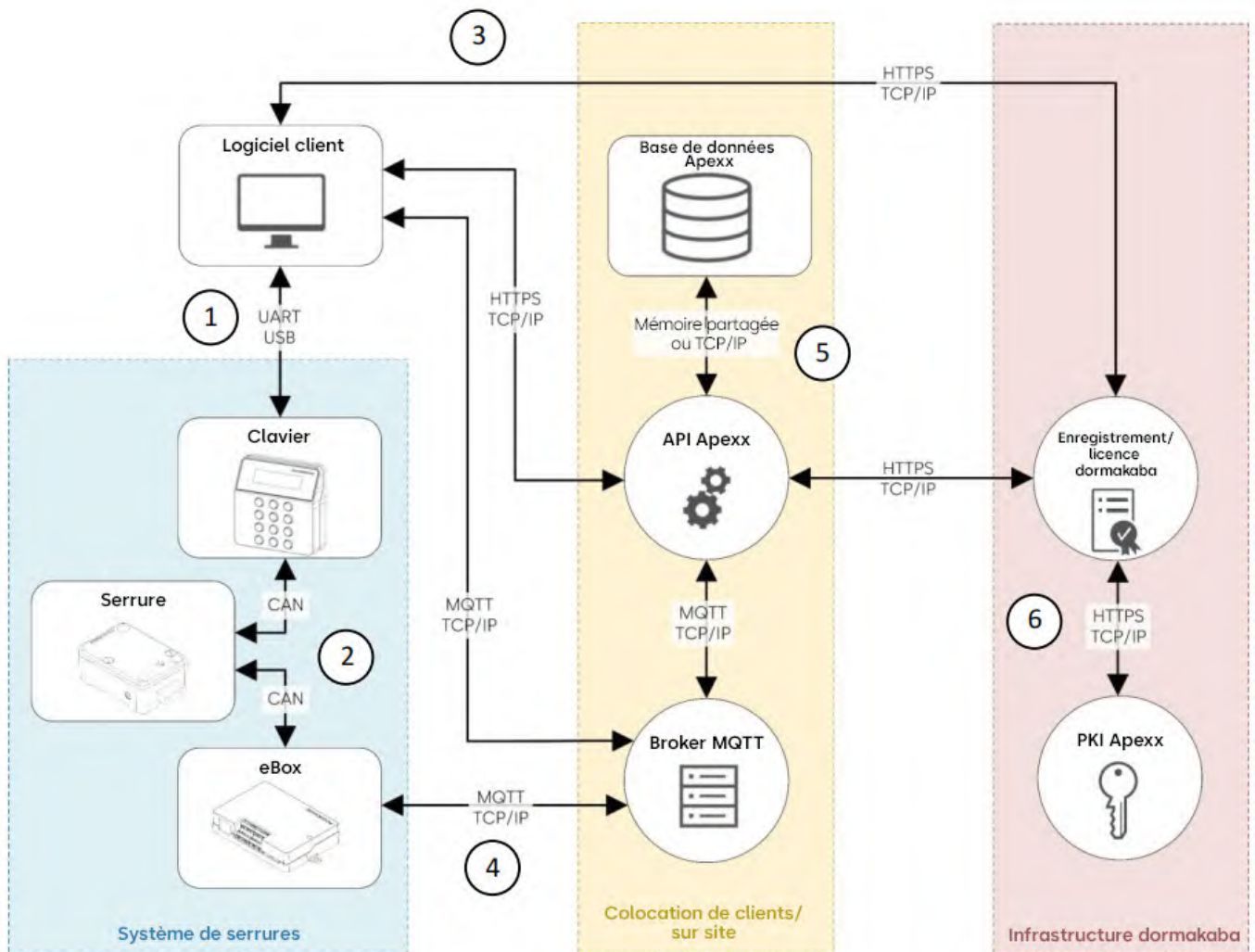
La licence « Apexx Local » ne permet que des mises à jour locales du firmware. Elles peuvent être effectuées en établissant une connexion USB temporaire entre l'ordinateur hébergeant le logiciel de la série Apexx et le clavier de votre système de serrures.

La licence « Apexx IP » vous permet d'effectuer des **mise à jour à distance du firmware**, que vous pouvez 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.

Pour plus d'informations sur le processus de mise à jour du firmware, consultez le **Guide d'utilisation du système Axessor Apexx** et le menu d'aide du **logiciel de la série Apexx**.

## Transit de données



## Transit de données

	Protocoles de communication	Flux de données	Description/Objectif
1	UART sur USB	Chemin bidirectionnel : <ul style="list-style-type: none"> <li>Logiciel client vers clavier</li> </ul>	Configuration directe et récupération des audits
2	CAN	Chemin bidirectionnel : <ul style="list-style-type: none"> <li>Clavier vers serrure</li> <li>Serrure vers eBox</li> </ul>	Communication d'appareil à appareil
3	HTTPS sur TCP/IP	Chemin bidirectionnel : <ul style="list-style-type: none"> <li>Logiciel client vers enregistrement/licence dormakaba</li> </ul>	Licence et enregistrement en ligne
4	MQTT sur TCP/IP	Chemin bidirectionnel : <ul style="list-style-type: none"> <li>Logiciel client vers broker MQTT</li> </ul> Chemin bidirectionnel : <ul style="list-style-type: none"> <li>eBox vers broker MQTT</li> </ul>	Configuration en réseau et récupération des audits
5	Mémoire partagée ou TCP/IP	Chemin bidirectionnel : <ul style="list-style-type: none"> <li>API Apexx vers base de données Apexx</li> </ul>	Stockage de données persistantes avec SQL Server
6	HTTPS sur TCP/IP	Chemin bidirectionnel : <ul style="list-style-type: none"> <li>Logiciel client vers API Apexx</li> <li>API Apexx vers enregistrement/licence dormakaba</li> <li>Enregistrement/licence dormakaba vers PKI Apexx</li> </ul>	Délivrance de certificats x.509

## Sécurité et chiffrement des données

Le système Apexx utilise plusieurs méthodes de chiffrement, notamment les certificats AES256, PBKDF2 et TLS, afin de garantir la communication et le stockage sûrs et sécurisés des données.

## Infrastructure à clé publique (PKI)

Le système Apexx utilise une infrastructure à clé publique pour créer, stocker et distribuer des certificats numériques aux appareils Apexx par l'intermédiaire d'une autorité de certification.

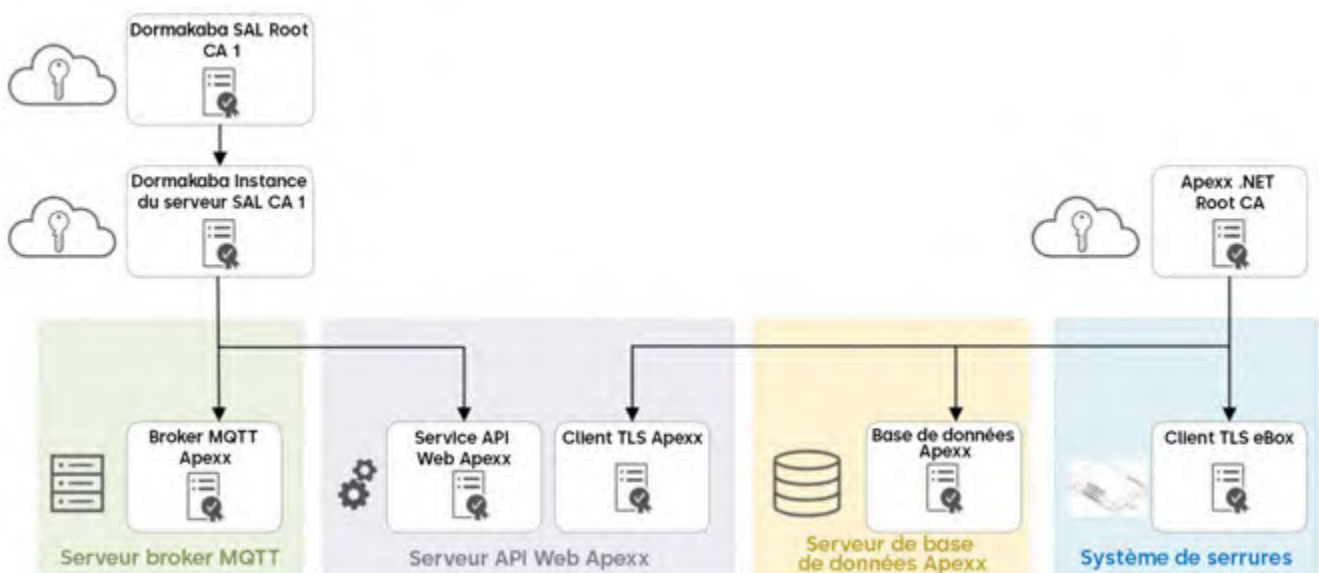


Figure 2 – Infrastructure à clé publique



## Infrastructure à clé publique (PKI)

Type de certificat	Description
dormakaba SAL Root CA	<ul style="list-style-type: none"><li>• Ce certificat est préchargé sur les appareils en usine et remplacé en mettant à jour le firmware</li></ul>
dormakaba Instance du serveur SAL CA	<ul style="list-style-type: none"><li>• 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</li><li>• Ce certificat doit être déployé sur tous les serveurs qui exécutent des services logiciels locaux</li><li>• La PKI du logiciel local signe les demandes de certificats pour tous les clients du broker MQTT</li><li>• Ces certificats sont utilisés pour établir des connexions TLS (<i>Transport Layer Security</i>) approuvées mutuellement et l'authentification avec le broker MQTT</li><li>• Il est également possible de signer les certificats utilisés par SQL Server pour les connexions TLS</li><li>• Si tous les services sont hébergés sur un seul serveur, il n'est pas nécessaire que plusieurs certificats soient signés par la PKI dormakaba SAL</li><li>• Même la base de données peut utiliser ce certificat si elle est hébergée sur le même serveur</li></ul>
Broker MQTT Apexx	<ul style="list-style-type: none"><li>• Créé lors de l'installation du logiciel</li><li>• Utilisé pour les connexions TLS et l'authentification</li></ul>
Service API Web Apexx	<ul style="list-style-type: none"><li>• Créé lors de l'installation du logiciel</li><li>• 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</li></ul>
Client TLS Apexx	<ul style="list-style-type: none"><li>• Utilisé pour l'authentification du client Apexx</li><li>• Le certificat est un utilisateur vérifié si l'émetteur correspond au .NET Root CA Apexx installé sur le serveur du broker</li></ul>
Base de données Apexx	<ul style="list-style-type: none"><li>• SQL Server sous Windows est le seul moteur de base de données pris en charge</li><li>• Les paramètres suivants sont activés sur l'instance/la base de données :<ul style="list-style-type: none"><li>• Authentification Windows</li></ul></li><li>• Le contrôle d'accès basé sur les rôles (RBAC) est utilisé dans le cadre de l'authentification Windows pour contrôler les autorisations</li></ul>
Client TLS eBox	<ul style="list-style-type: none"><li>• Utilisé pour l'authentification de l'eBox</li><li>• Le certificat est un utilisateur vérifié si l'émetteur correspond au .NET Root CA Apexx installé sur le serveur du broker</li></ul>
Apexx .NET Root CA	<ul style="list-style-type: none"><li>• Créé lors de l'installation du logiciel</li><li>• 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</li></ul>

## 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 d'informations sur les licences requises pour les différentes configurations informatiques et matérielles, reportez-vous au Catalogue de prix Axessor Apexx.

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

La figure 3 illustre une configuration de base impliquant un seul ordinateur et un seul système de verrouillage Apexx. 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 Apexx à des fins de programmation et de configuration du système.



Ce type de 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.

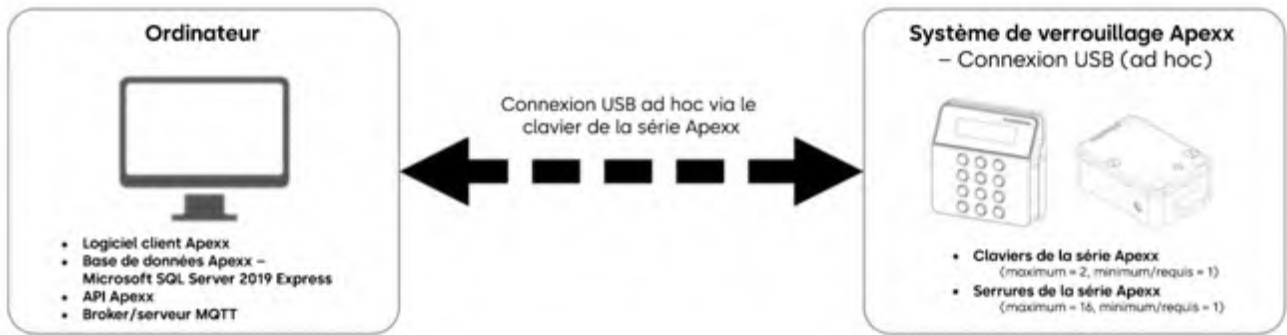


Figure 3 – Configuration d'un seul ordinateur - connexion USB ad hoc

La figure 4 montre une autre configuration simple avec un seul ordinateur et un seul système de verrouillage Apexx, mais cette fois-ci, l'eBox Apexx est utilisée pour fournir une connexion réseau/IP pour une communication continue/en direct entre l'ordinateur et le système de verrouillage.



Figure 4 – Configuration d'un seul ordinateur - réseau via eBox (TCP/IP)

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). 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 5 offre une plus grande flexibilité.

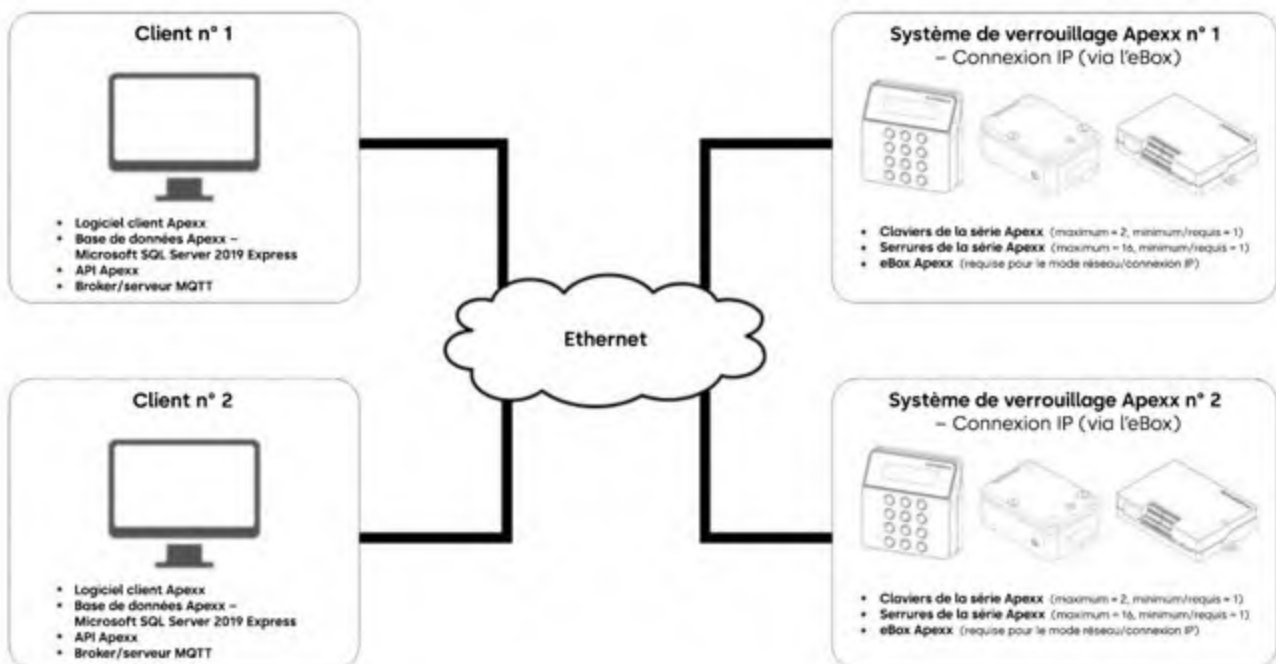


Figure 5 – Configuration de différents ordinateurs avec plusieurs systèmes de verrouillage

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 se connecte au réseau via une eBox Apexx.

Ce concept est davantage développé dans le système montré à la figure 6, qui comprend plusieurs ordinateurs et systèmes de serrures répartis dans plusieurs bâtiments.

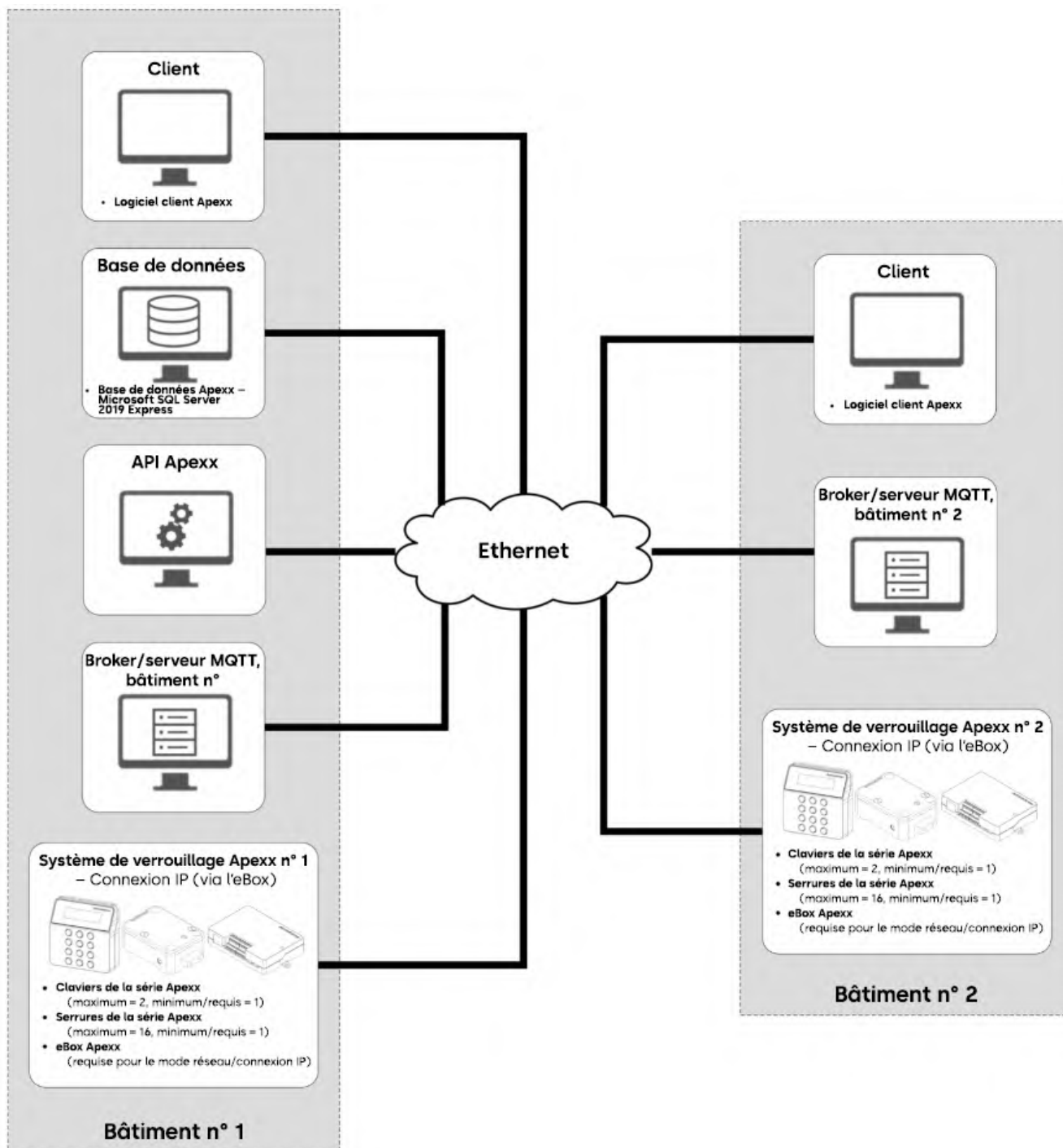


Figure 6 – Configuration de plusieurs ordinateurs/systèmes de verrouillage avec configuration multi-serveurs

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 Apexx sur l'ensemble du réseau.

Le dernier exemple de la figure 6 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 informatiques recommandées par Apexx

### Station de travail client Apexx

- Intel Core i7 – 4470 3,40 GHz avec 4 cœurs
- RAM 16 GO 1600 MHz DDR3 NON-ECC
- Disque dur de 500 GO
- Windows 10 Professionnel 64 bits
- Double moniteur AMD RADEON HD 8490 1 GO ou double moniteur AMD RADEON HD 8570 1 GO
- Ports USB 2.0
- Port Ethernet – Carte réseau 1 GO
- Clavier et souris
- Sauvegarde UPS

### Serveur broker Apexx

- Intel Xeon E5 – 2403, 1,80 GHz, 10 MB de cache
- RAM 16 GO 1333 MHz, RDIMM
- Disque dur de 500 GO
- Windows 2019 Server Standard 64 bits
- Carte graphique HD intégrée
- Port Ethernet – Carte réseau 1 GO
- Clavier et souris
- Sauvegarde UPS

### Serveur de base de données Apexx et API Apexx

- Intel Xeon E5 – 2420, 1,90 GHz, 15 MB de cache avec 6 cœurs
- RAM 32 GO 1333 MHz, RDIMM
- Disque dur 2 x 1TB 7.2K RPM SATA 3Gbps 3,5 po
- Configuration RAID 1
- Double alimentation hot-plug redondante
- Windows 2019 Server Standard 64 bits
- Carte graphique HD intégrée
- Port Ethernet – Carte réseau GO
- Clavier et souris
- Sauvegarde UPS

## Nos engagements en termes de durabilité

Nous nous engageons à favoriser un développement durable sur l'ensemble de notre chaîne de valeur conformément à nos responsabilités sociétales, environnementales et économiques à l'égard des générations actuelles et futures. La durabilité au niveau des produits est une approche importante et orientée vers l'avenir dans le domaine 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 (EPD), basées sur des évaluations holistiques du cycle de vie.

[www.dormakaba.com/sustainability](http://www.dormakaba.com/sustainability)



## Nos offres

### Solutions d'accès automatisées

Portes automatiques  
Solutions d'accès sécurisées



### Solutions de contrôle d'accès

Contrôle d'accès et gestion des temps  
Issues de secours et voies d'évacuation  
Contrôle d'accès électronique pour l'hébergement



### Solutions d'accès mécaniques

Ferme-portes  
Quincaillerie de porte  
Cylindres et clés mécaniques



### Services

Assistance technique  
Installation et mise en service  
Entretien et réparation



### Solutions pour les clés et les murs

Systèmes de clés  
Murs mobiles/coulissants



### Serrures de coffre-fort

Serrures électroniques de coffre-fort  
Serrures mécaniques de coffre-fort  
Tringlerie et accessoires



### Systèmes en verre

Systèmes de portes manuelles  
Ferrures en verre  
Murs coulissants horizontaux



Architecture du système Apexx, FR, 02/2024  
Sous réserve de modifications sans préavis

### dormakaba USA Inc.

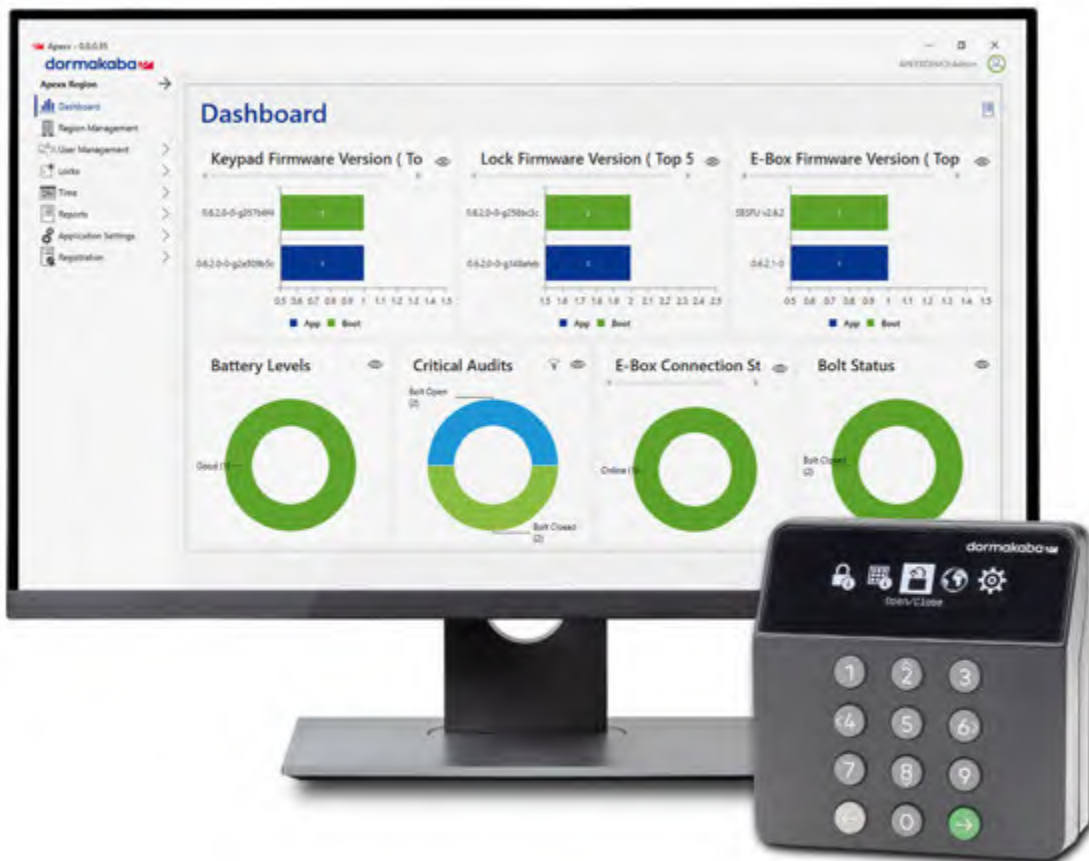
1525 Bull Lea Road, Suite 100  
Lexington, KY 40511  
[sales.safelocks.us@dormakaba.com](mailto:sales.safelocks.us@dormakaba.com)  
T +1 800 950 4744  
+1 888 950 4715 (support technique)  
[dormakaba.com](http://dormakaba.com)



AXESSOR APEXX IP  
GUIDES D'INSTALLATION  
ET D'UTILISATION

[dk.world/AxessorApexxIP](http://dk.world/AxessorApexxIP)

# Axessor Apexx Systemarchitektur



# Inhalt

- Apexx-Systemarchitektur. . . . . 2
- Apexx-API. . . . . 2
- Apexx-Client-Software. . . . . 2
- Apexx-Datenbank. . . . . 3
- MQTT-Broker/Server . . . . . 3
- SMTP. . . . . 3
- SSO. . . . . 3
- Benutzerkonfiguration . . . . . 3
- Lizenzen . . . . . 4
- Lokale und Remote-Firmware-Aktualisierungen . . . . . 4
- Datenübertragung . . . . . 5
- Sicherheits- und Datenverschlüsselung . . . . . 6
- Public Key-Infrastruktur (PKI) . . . . . 6
- Computer-Hardware-Konfigurationen. . . . . 7
- Besondere Hinweise zur Datenbank. . . . . 10
- Empfohlene Spezifikationen der Apexx-Computer. . . . . 10

# Apexx-Systemarchitektur

## Übersicht

Apexx-Schließanlagen können in 2 sichere Kommunikationsnetzwerke aufgeteilt werden: **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)
  - Fungiert als Brücke zwischen dem Schlosssystem und der API/Software

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

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

## 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 ist eine grafische Benutzeroberfläche (GUI), die es den Softwarebenutzern ermöglicht, die API zu verwenden, um Aktionen im 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.

## SMTP

Die Software der Apexx-Serie verwendet das Simple Mail Transport Protocol (SMTP), um Folgendes zu senden: Aktive Alarmer und geplante Berichte.

- 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.

## 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

Die Apexx-Systembenutzer lassen sich in zwei verschiedene Kategorien einteilen: **Tresorschlossbenutzer** und **Softwarebenutzer**.

**Tresorschlossbenutzer** sind Benutzer, die das Schlosssystem (bestehend aus den physischen Tastaturen, den Schlössern, der eBox usw.) 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.

Die drei Standardtypen der Tresorschlossbenutzer (Administrator, Manager und Benutzer) bilden eine Hierarchie aus Benutzern mit jeweils vordefinierten Rollen und Berechtigungen innerhalb der Schließanlage. 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.



**Softwarebenutzer** sind Benutzer, die die Software der Apexx-Serie ausführen und die Software-Tools verwenden, um Management- und Administratoraufgaben 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. Softwarebenutzer, die über eine Softwarebenutzer-Schreibberechtigung verfügen, können neue Softwarebenutzer hinzufügen und die Lese-/Schreibberechtigungen konfigurieren.

## Lizenzen

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

## Lokale und Remote-Firmware-Aktualisierungen

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

Die „Apexx Local“-Lizenz erlaubt nur lokale Firmware-Aktualisierungen, die durch den Aufbau einer temporären USB-Verbindung zwischen dem Computer, auf dem die Software der Apexx-Serie installiert ist, und der Tastatur Ihres Schlosssystems durchgeführt werden können.

Die „Apexx IP“-Lizenz erlaubt die Durchführung von **Remote-Firmware-Aktualisierungen**, die über eine Netzwerkverbindung über die eBox durchgeführt werden können. 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 die Schließanlage überträgt.
2. Die Firmware wird heruntergeladen und in der Schließanlage 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.

Weitere Informationen zum Prozess der Firmware-Aktualisierung finden Sie im **Axessor Apexx System User Guide** und im Hilfemenü der **Software der Apexx-Serie**.

# Datenübertragung

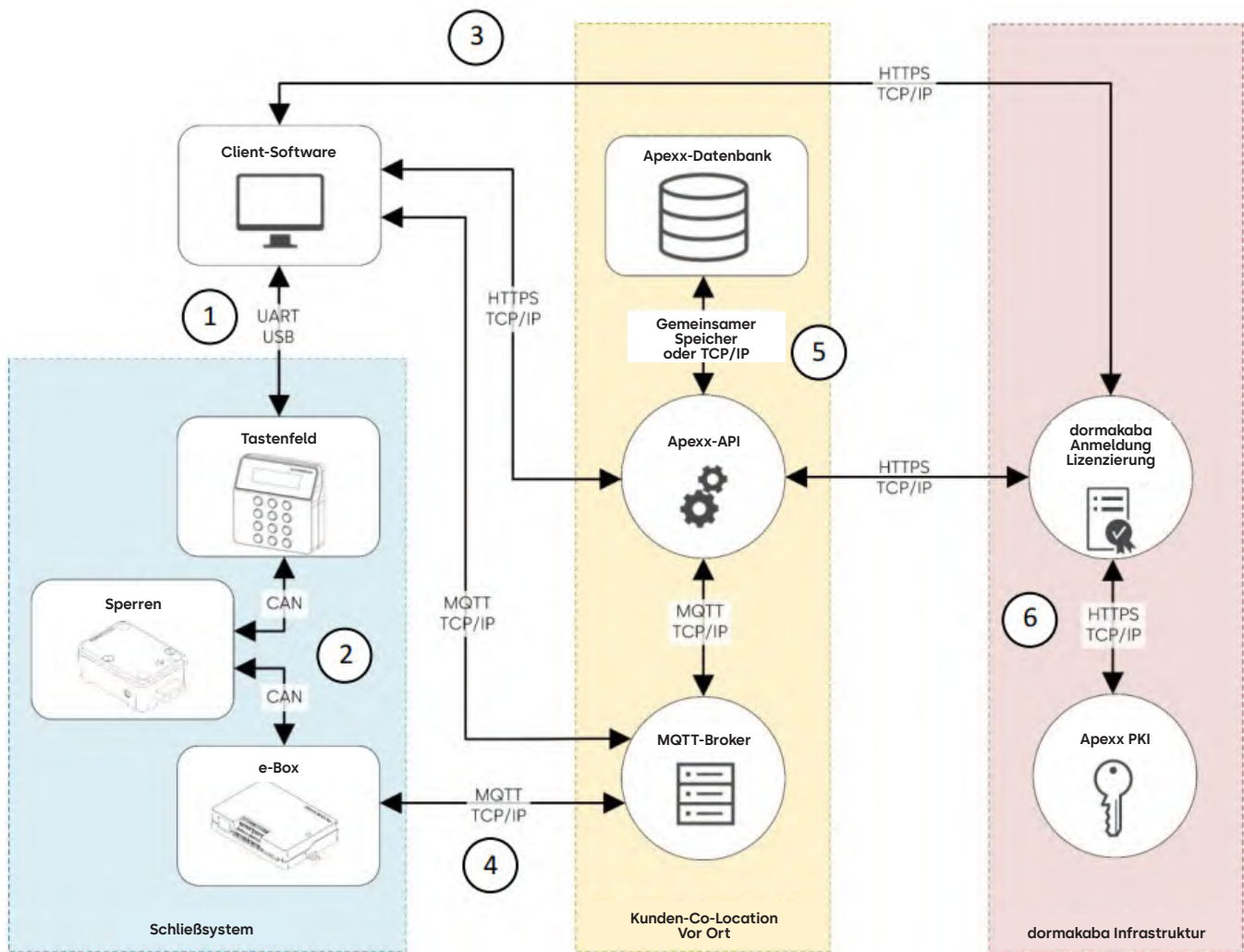


Abbildung 1: Apexx-Systemarchitektur – Systemkomponenten und Datenübertragung

	Kommunikations-protokolle	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	Abruf von Konfigurationen und von Prüfberichten im Netzwerkbetrieb

	Kommunikationsprotokolle	Datenfluss	Beschreibung/Zweck
5	Gemeinsamer Speicher oder TCP/IP	Bidirektionaler Pfad: <ul style="list-style-type: none"> <li>Apexx-API zu Apexx-Datenbank</li> </ul>	Persistente Datenspeicherung mit SQL-Server
6	HTTPS over TCP/IP	Bidirektionaler Pfad: <ul style="list-style-type: none"> <li>Client-Software zu Apexx-API</li> <li>Apexx-API zu dormakaba Registrierung/Lizenzierung</li> <li>dormakaba Registrierung/Lizenzierung zu Apexx-PKI</li> </ul>	Ausstellung von x.509-Zertifikaten

## Sicherheits- und Datenverschlüsselung

Das Apexx-System verwendet mehrere Verschlüsselungsmethoden, darunter AES256, PBKDF2 und TLS-Zertifikate, um die sichere Kommunikation und Speicherung von Daten zu gewährleisten.

## Public Key-Infrastruktur (PKI)

Das Apexx-System nutzt eine Public Key-Infrastruktur, um digitale Zertifikate zu erstellen, zu speichern und über eine Zertifizierungsstelle an Apexx-Geräte zu verteilen.

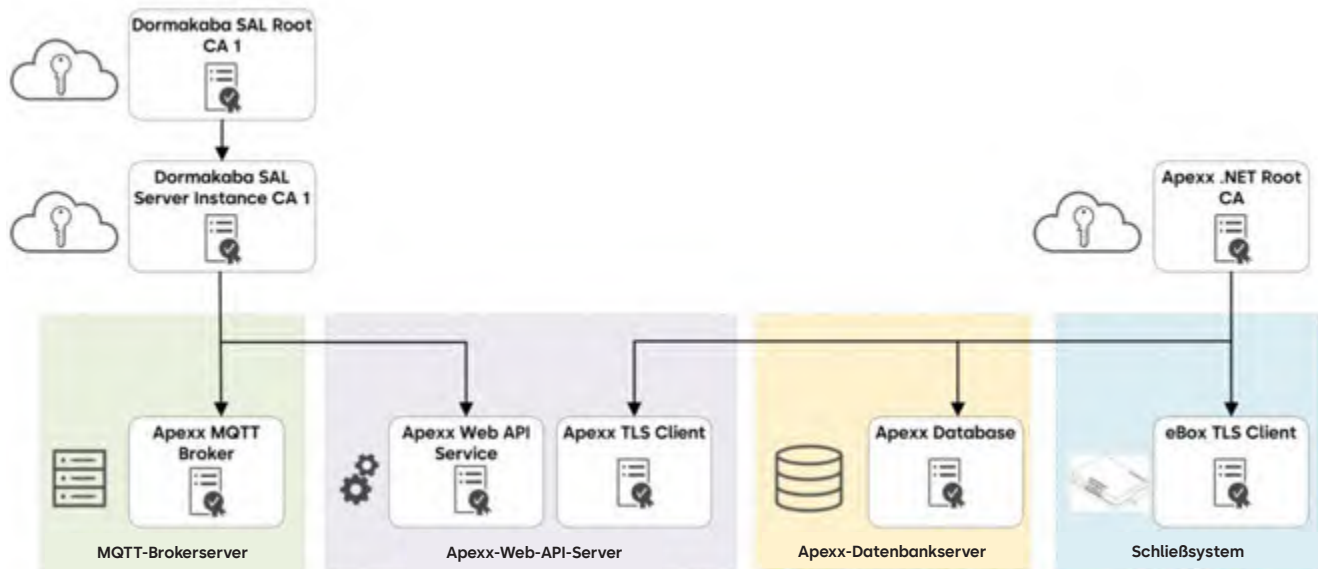


Abbildung 2: Public Key-Infrastruktur

Zertifikatstyp	Beschreibung
dormakaba SAL Root CA	<ul style="list-style-type: none"> <li>Dieses Zertifikat wird vor ihrer Auslieferung auf die Geräte geladen und wird per Firmware-Aktualisierung ersetzt.</li> </ul>
dormakaba SAL Server Instance CA	<ul style="list-style-type: none"> <li>Server, auf denen lokale Softwaredienste für Apexx ausgeführt werden, benötigen von der dormakaba SAL-PKI signierte Zertifikate, damit die Geräte ihnen vertrauen.</li> <li>Dieses Zertifikat muss auf allen Servern bereitgestellt werden, auf denen lokale Softwaredienste ausgeführt werden.</li> <li>Die lokale Software-PKI signiert Zertifikatsanforderungen für alle Clients des MQTT-Brokers.</li> <li>Diese Zertifikate werden sowohl für den Aufbau vertrauenswürdiger TLS-Verbindungen (Transport Layer Security) als auch für die Authentifizierung beim MQTT-Broker verwendet.</li> <li>Damit können auch die von SQL Server für TLS verwendeten Zertifikate signiert werden.</li> <li>Wenn alle Dienste auf einem einzigen Server gehostet werden, müssen nicht mehrere Zertifikate von der dormakaba SAL-PKI signiert werden.</li> <li>Auch die Datenbank kann dieses Zertifikat verwenden, wenn es auf demselben Server gehostet wird.</li> </ul>

Zertifikatstyp	Beschreibung
<b>Apexx MQTT-Broker</b>	<ul style="list-style-type: none"> <li>• Wird während der Softwareinstallation erstellt.</li> <li>• Wird für TLS-Verbindungen und die Authentifizierung verwendet.</li> </ul>
<b>Apexx Web-API-Dienst</b>	<ul style="list-style-type: none"> <li>• Wird während der Softwareinstallation erstellt.</li> <li>• Enthält den Namen des Servers (Computer, auf dem dieser Dienst installiert ist), die vertrauenswürdige Zertifizierungsstelle und den öffentlichen Verschlüsselungsschlüssel des Servers.</li> </ul>
<b>Apexx TLS-Client</b>	<ul style="list-style-type: none"> <li>• Wird für die Authentifizierung des Apexx-Clients verwendet.</li> <li>• Das Zertifikat ist dann ein verifizierter Benutzer, wenn der Aussteller mit der installierten Apexx .NET Root CA auf dem Broker-Server übereinstimmt.</li> </ul>
<b>Apexx-Datenbank</b>	<ul style="list-style-type: none"> <li>• SQL Server unter Windows ist die einzige unterstützte Datenbank-Engine.</li> <li>• In der Instanz/Datenbank sind die folgenden Einstellungen aktiviert: <ul style="list-style-type: none"> <li>• Windows-Authentifizierung</li> </ul> </li> <li>• Die rollenbasierte Zugriffssteuerung (RBAC) wird zusammen mit der Windows-Authentifizierung zur Steuerung der Berechtigungen verwendet.</li> </ul>
<b>eBox TLS-Client</b>	<ul style="list-style-type: none"> <li>• Wird für die Authentifizierung der eBox verwendet.</li> <li>• Das Zertifikat ist dann ein verifizierter Benutzer, wenn der Aussteller mit der installierten Apexx .NET Root CA auf dem Broker-Server übereinstimmt.</li> </ul>
<b>Apexx .NET Root CA</b>	<ul style="list-style-type: none"> <li>• Wird während der Softwareinstallation erstellt.</li> <li>• Jeder Computer, auf dem die Software ausgeführt wird (Client, Server, Datenbank usw.), benötigt für die Zwecke der Sicherheit/Identifizierung eine Kopie dieses Zertifikats.</li> </ul>

## Computer-Hardware-Konfigurationen

Der Computer-Hardware/API/Software-Teil des Apexx-Systems kann in Abhängigkeit von der Komplexität Ihres Systems (Anzahl der Apexx-Schließanlagen, 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 der Preisliste zu Axessor Apexx.

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

Abbildung 3 zeigt eine Basiskonfiguration mit nur einem Computer und einer Apexx-Schließanlage. In dieser Konfiguration werden alle API/Software-Elemente auf einem einzigen Computer gehostet, wobei eine USB-Verbindung verwendet wird, um vorübergehend eine Verbindung zur Apexx-Schließanlage für die Programmierung/Systemkonfiguration herzustellen.

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

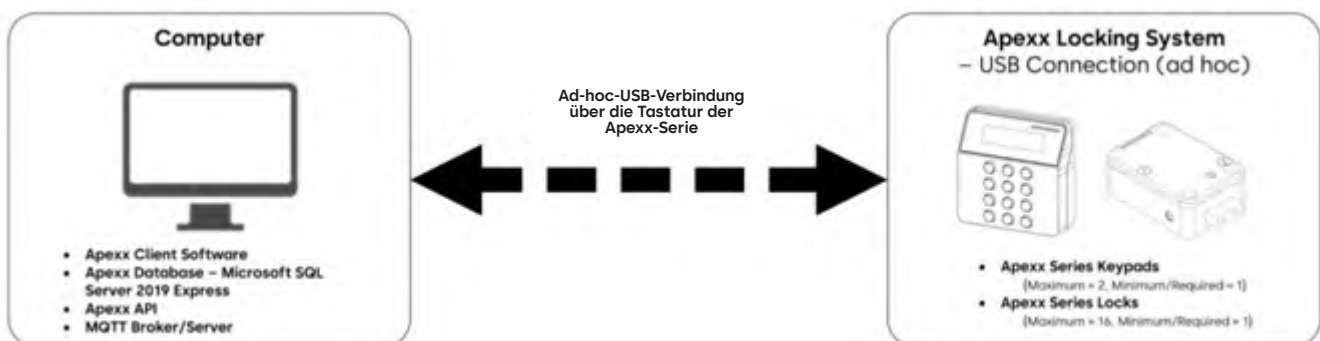


Abbildung 3: Konfiguration mit einem Computer – Ad-hoc-USB-Verbindung

Abbildung 4 zeigt eine weitere einfache Konfiguration mit nur einem Computer und einer Apex-Schließanlage. Diesmal wird aber die Apex eBox verwendet, um eine Netzwerk/IP-Verbindung für eine kontinuierliche/direkte Kommunikation zwischen dem Computer und der Schließanlage herzustellen.

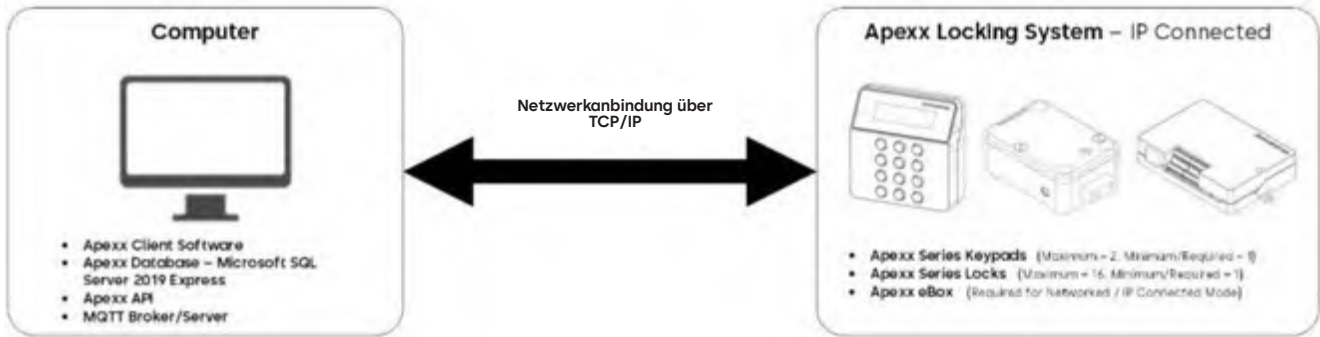


Abbildung 4: Konfiguration mit einem Computer – Netzwerk über eBox (TCP/IP)

Diese Konfiguration ist 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).

Für größere Standorte mit größeren Gebäuden und/oder mehreren Schließanlagen bietet die in Abbildung 5 gezeigte Konfiguration mit mehreren Computern zusätzliche Flexibilität.

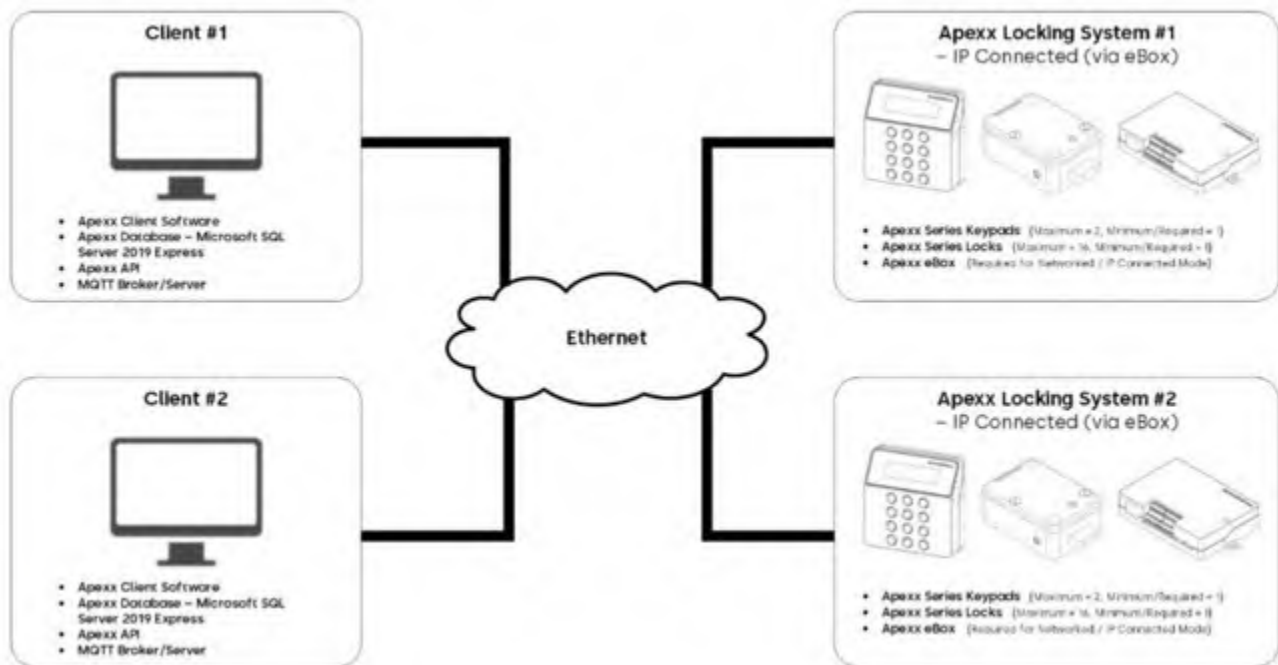


Abbildung 5: Konfiguration mit mehreren Computern und mehreren Schließanlagen

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 Schließsysteme bietet. Beachten Sie, dass jede Schließanlage über eine Apex eBox mit dem Netzwerk verbunden ist.

Dieses Konzept wird in dem in Abbildung 6 gezeigten System mit mehreren Computern und Schlosssystemen, die über mehrere Gebäude verteilt sind, noch erweitert.



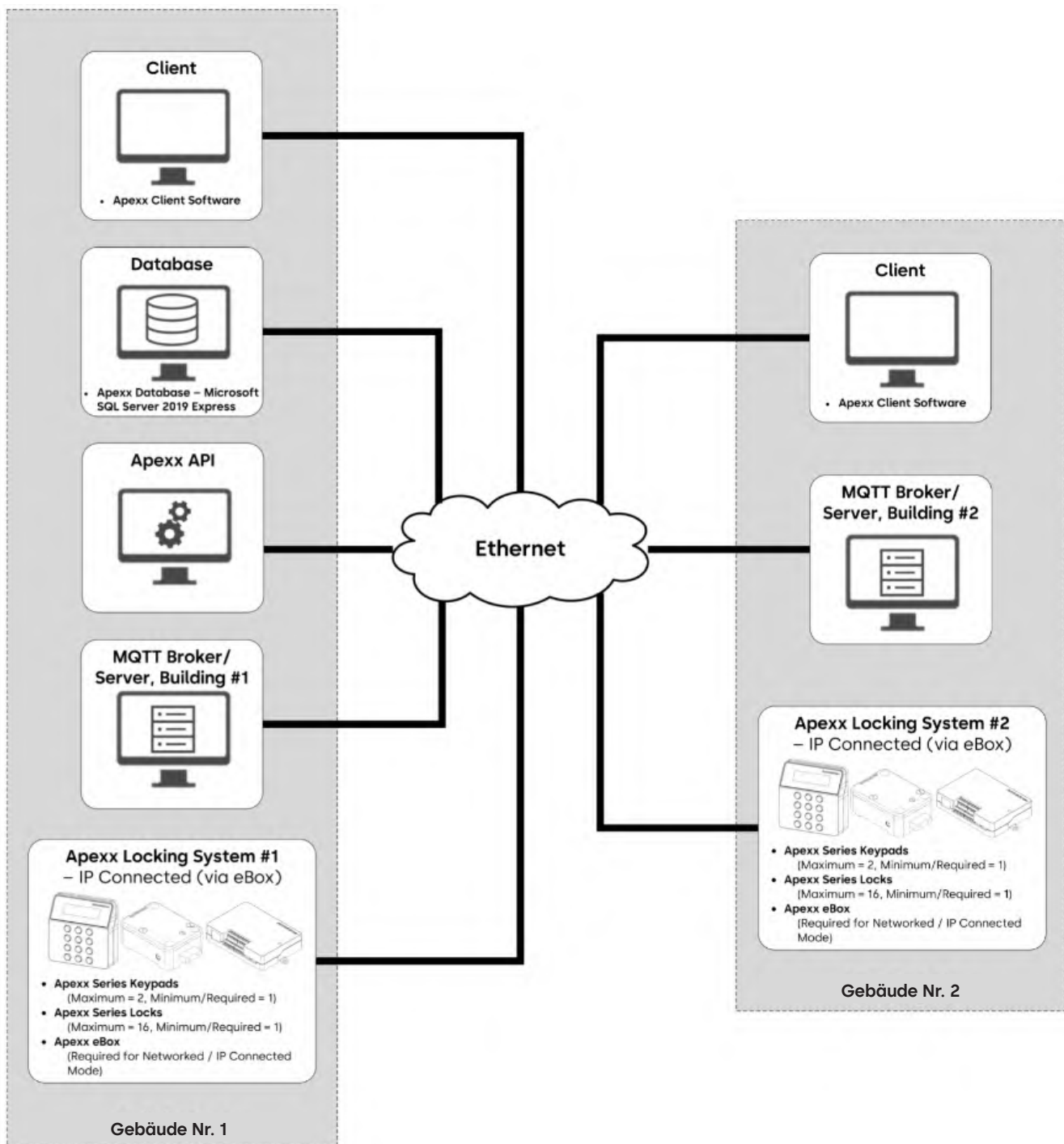


Abbildung 6: Konfiguration mit mehreren Computern/Schließanlagen und mehreren Servern

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 Apex-API bzw. die Apex-Datenbank hosten. Diese beiden Computer können so konfiguriert werden, dass sie als API und Datenbank für die Schließanlagen in Gebäude 1, Gebäude 2 und/oder jedes andere Apex-System 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 Spezifikationen der Apexx-Computer

### Apexx-Client-Workstation

- Intel Core i7 – 4470 3,40 GHz mit 4 Kernen
- 16 GB RAM 1600 MHz DDR3 NON-ECC
- 500 GB Festplatte
- Windows 10 Professional 64-Bit
- AMD RADEON HD 8490 1 GB Dual Monitor oder AMD RADEON HD8570 1 GB Dual Monitor
- USB 2.0-Ports
- Ethernet-Port – 1-Gb-Netzwerkkarte
- Tastatur und Maus
- USV-Ausweichstromversorgung

### Apexx-Broker-Server

- Intel Xeon E5 – 2403, 1,80 GHz, 10 MB Cache
- 16 GB RAM 1333 MHz, RDIMM
- 500 GB Festplatte
- Windows 2019 Server Standard 64-Bit
- Integrierte HD-Grafikkarte
- Ethernet-Port – 1-Gb-Netzwerkkarte
- Tastatur und Maus
- USV-Ausweichstromversorgung

### Apexx-Datenbank-Server und Apexx-API

- Intel Xeon E5 – 2420, 1,90 GHz, 15 MB Cache mit 6 Kernen
- 32 GB RAM 1333 MHz, RDIMM
- 2 x 1 TB 7,2 K RPM SATA 3 Gb/s 3,5-Zoll-Festplatte
- RAID 1-Konfiguration
- Duales, redundantes Hot-Plug-Netzteil
- Windows 2019 Server Standard 64-Bit
- Integrierte HD-Grafikkarte
- Ethernet-Port – Gb-Netzwerkkarte
- Tastatur und Maus
- USV-Ausweichstromversorgung



## Unser Nachhaltigkeitsversprechen

Im Einklang mit unserer wirtschaftlichen, ökologischen und sozialen Verantwortung sind wir bestrebt, für die gegenwärtigen und zukünftigen Generationen eine nachhaltige Entwicklung in unserer gesamten Wertschöpfungskette zu fördern. Nachhaltigkeit auf Produktebene ist ein wichtiger und zukunftsorientierter Ansatz im Bauwesen. Um Kunden quantifizierte Daten über die Umweltauswirkungen eines Produktes entlang dessen gesamten Lebenszyklus bereitzustellen, bietet dormakaba Umweltproduktdeklarationen (Environmental Product Declaration, EPD) an, die auf ganzheitlichen Ökobilanzen basieren.

[www.dormakaba.com/sustainability](http://www.dormakaba.com/sustainability)



## Unser Angebot

### Automatische Türsysteme

Automatisierter Zutritt  
Sicherheit



### Lösungen für die Zutrittskontrolle

Elektronischer Zugriff und Daten  
Systeme für Flucht- und  
Rettungswege  
Hotelzutrittssysteme



### Türtechnik

Türschließer  
Architekturlösungen  
Mechanische Schließsysteme



### Serviceleistungen

Technischer Kundendienst  
Installation und Inbetriebnahme  
Wartung und Reparatur



### Key & Wall Solutions

Schlüsselsysteme  
Mobile Wände/Schiebewände



### Tresorschlösser

Elektronische Tresorschlösser  
Mechanische Tresorschlösser  
Riegelwerke und Zubehör



### Glassysteme

Manuelle Türsysteme  
Glasbeschläge  
Horizontale Schiebewände



Apexx-Systemarchitektur, DE, 02/2024  
Änderungen vorbehalten

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

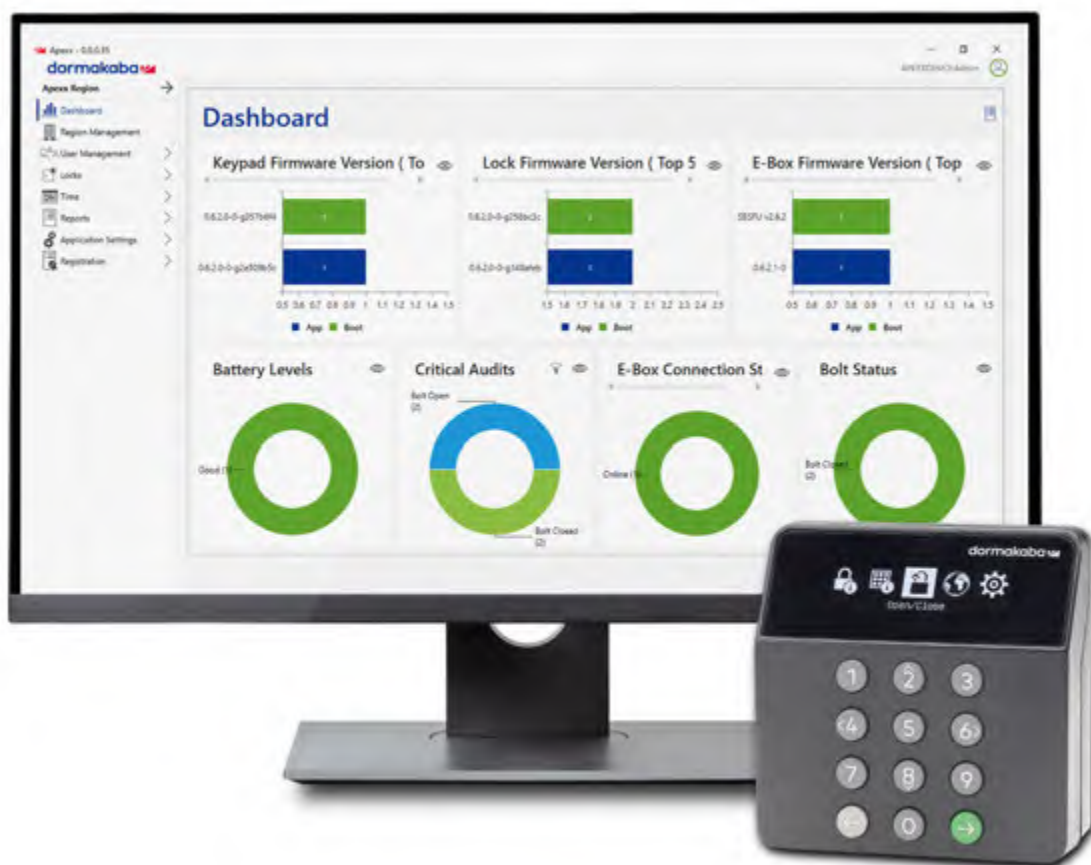
**dormakaba USA Inc.**  
1525 Bull Lea Road, Suite 100  
Lexington, KY 40511  
sales.safelocks.us@dormakaba.com  
T +1 800 950 4744  
**dormakaba.com**



AXESSOR APEXX IP  
INSTALLATION AND  
OPERATION GUIDES

[dk.world/AxessorApexxIP](http://dk.world/AxessorApexxIP)

# Architettura del sistema Axessor Apexx



# Indice

- Architettura del sistema Apexx ..... 2
- API Apexx..... 2
- Apexx Client Software..... 2
- Database Apexx..... 2
- Broker/server MQTT ..... 3
- SMTP..... 3
- SSO..... 3
- Configurazione utente..... 3
- Licenze..... 4
- Aggiornamenti del firmware locali vs. remoti..... 4
- Transito di dati ..... 5
- Sicurezza e crittografia dei dati ..... 6
- Infrastruttura a chiave pubblica (PKI)..... 6
- Configurazioni hardware del computer..... 7
- Considerazioni sul database..... 10
- Specifiche del computer consigliate da Apexx ..... 10

# Architettura del sistema Apexx

## Panoramica

I sistemi di chiusura Apexx possono essere suddivisi in 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
- **Apexx eBox** (necessario per la modalità connessa in rete/IP)
  - Funziona da ponte tra il sistema di chiusura e API/software

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

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

## 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 è un'interfaccia grafica utente (GUI) che consente agli utenti del software di utilizzare l'API per eseguire azioni nel sistema (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.

## SMTP

Il software della serie Apexx utilizza il Simple Mail Transport Protocol (SMTP) per inviare quanto segue: Avvisi attivi e rapporti programmati.

- 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.

## 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

Gli utenti del sistema 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 (costituito da tastierini fisici, serrature, eBox, ecc.) 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.

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.

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/chiudere 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). 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.

## 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 il listino prezzi Axessor Apexx IP.

### Aggiornamenti del firmware locali vs. remoti

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

La licenza "Apexx Local" consente solo aggiornamenti locali del firmware, che possono essere effettuati stabilendo una connessione USB provvisoria tra il computer su cui si trova il software della serie Apexx e il tastierino del sistema di chiusura.

La licenza "Apexx IP" consente di eseguire **aggiornamenti remoti del firmware**, che possono avvenire tramite una connessione di rete via 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.

Per ulteriori informazioni sul processo di aggiornamento del firmware, consultare la "**Guida dell'utente del sistema Axessor Apexx**" e il menu di aiuto del **software della serie Apexx**.

# Transito di dati

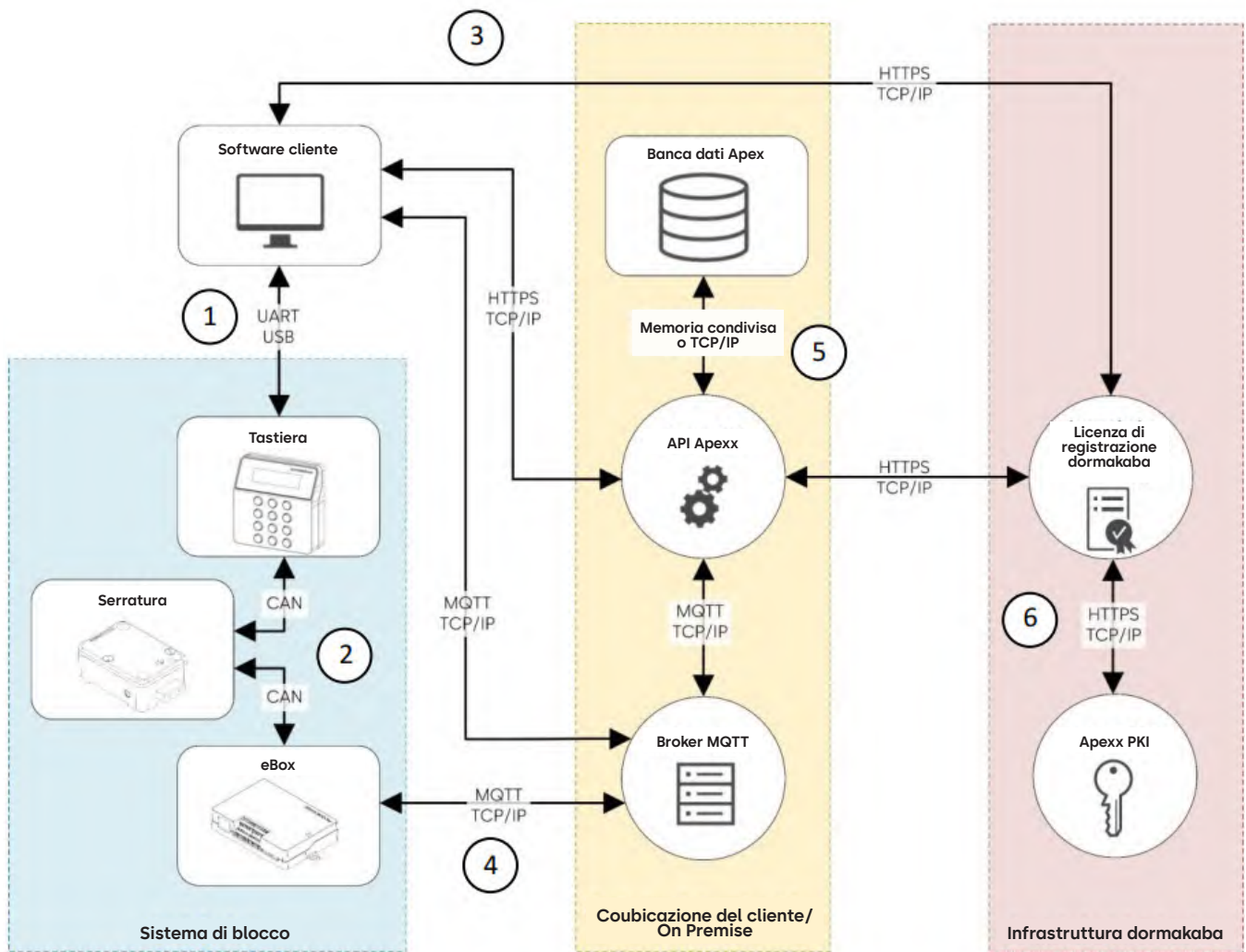


Figura 1 - Architettura del sistema Apex - Componenti del sistema e transito dei dati

	Protocolli di comunicazione	Flusso di dati	Descrizione/scopo
1	UART su USB	Percorso bidirezionale: <ul style="list-style-type: none"> <li>Client Software a tastierino</li> </ul>	Configurazione diretta e recupero degli audit
2	CAN	Percorso bidirezionale: <ul style="list-style-type: none"> <li>Tastierino a serratura</li> <li>Serratura ad eBox</li> </ul>	Comunicazione da dispositivo a dispositivo
3	HTTPS su TCP/IP	Percorso bidirezionale: <ul style="list-style-type: none"> <li>Software client per la registrazione/licenza di dormakaba</li> </ul>	Licenza e registrazione online
4	MQTT su TCP/IP	Percorso bidirezionale: <ul style="list-style-type: none"> <li>Software client per broker MQTT</li> </ul> Percorso bidirezionale: <ul style="list-style-type: none"> <li>Broker da eBox a MQTT</li> </ul>	Configurazione in rete e recupero degli audit
5	Memoria condivisa o TCP/IP	Percorso bidirezionale: <ul style="list-style-type: none"> <li>Da Apexx API al database Apexx</li> </ul>	Archiviazione duratura dei dati con SQL Server



	Protocolli di comunicazione	Flusso di dati	Descrizione/scopo
6	HTTPS su TCP/IP	Percorso bidirezionale: <ul style="list-style-type: none"> <li>Client Software ad Apexx API</li> <li>Apexx API a Registrazione/Licenza dormakaba</li> <li>Registrazione/Licenza dormakaba ad Apexx PKI</li> </ul>	Emissione di certificati x.509

## Sicurezza e crittografia dei dati

Il sistema Apexx utilizza diversi metodi di crittografia, tra cui AES256, PBKDF2 e certificati TLS, per garantire la sicurezza della comunicazione e dell'archiviazione dei dati.

## Infrastruttura a chiave pubblica (PKI)

Il sistema Apexx utilizza un'infrastruttura a chiave pubblica per creare, memorizzare e distribuire certificati digitali ai dispositivi Apexx tramite un'autorità di certificazione.

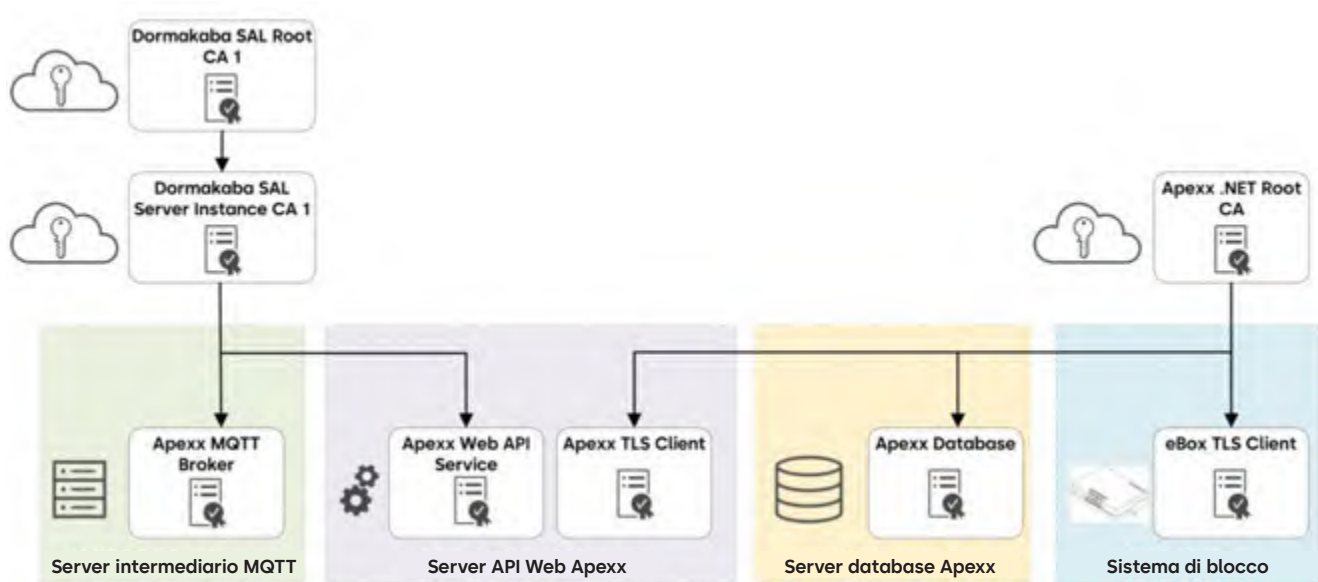


Figura 2 - Infrastruttura a chiave pubblica

Tipo di certificato	Descrizione
dormakaba SAL Root CA	<ul style="list-style-type: none"> <li>Questo certificato viene preinstallato in fabbrica sui dispositivi e sostituito tramite aggiornamento del firmware.</li> </ul>
dormakaba SAL Server Instance CA	<ul style="list-style-type: none"> <li>I server che eseguono servizi software locali per Apexx necessitano di certificati firmati da dormakaba SAL PKI affinché i dispositivi possano considerarli affidabili.</li> <li>Questo certificato deve essere distribuito a tutti i server che eseguono servizi software locali.</li> <li>La PKI software locale firma le richieste di certificato per tutti i client del broker MQTT.</li> <li>Questi certificati sono utilizzati sia per stabilire connessioni Transport Layer Security (TLS) a fiducia reciproca, sia per l'autenticazione con il broker MQTT.</li> <li>Può anche firmare i certificati utilizzati da SQL Server per TLS.</li> <li>Se tutti i servizi sono ospitati su un singolo server, non è necessario che più certificati siano firmati da dormakaba SAL PKI.</li> <li>Anche il database può utilizzare tale certificato se ospitato sullo stesso server.</li> </ul>

Tipo di certificato	Descrizione
Broker Apexx MQTT	<ul style="list-style-type: none"> <li>• Creato durante l'installazione del software.</li> <li>• Utilizzato per le connessioni TLS e l'autenticazione.</li> </ul>
Servizio API Web di Apexx	<ul style="list-style-type: none"> <li>• Creato durante l'installazione del software.</li> <li>• 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.</li> </ul>
Apexx TLS Client	<ul style="list-style-type: none"> <li>• Utilizzato per l'autenticazione del client Apexx.</li> <li>• Il certificato è un utente verificato se l'emittente corrisponde alla Apexx .NET Root CA installata sul server del broker.</li> </ul>
Database Apexx	<ul style="list-style-type: none"> <li>• SQL Server su Windows è l'unico motore di database supportato.</li> <li>• Le seguenti impostazioni sono abilitate sull'istanza/database: <ul style="list-style-type: none"> <li>• Autenticazione di Windows</li> </ul> </li> <li>• Il controllo degli accessi basato sui ruoli (RBAC) viene utilizzato all'interno, insieme all'autenticazione di Windows, per controllare le autorizzazioni.</li> </ul>
eBox TLS Client	<ul style="list-style-type: none"> <li>• Utilizzato per l'autenticazione dell'eBox.</li> <li>• Il certificato è un utente verificato se l'emittente corrisponde alla Apexx .NET Root CA installata sul server del broker.</li> </ul>
Apexx .NET Root CA	<ul style="list-style-type: none"> <li>• Creato durante l'installazione del software.</li> <li>• Ogni computer che esegue il software (client, server, database, ecc.) richiede una copia di questo certificato per motivi di sicurezza/identificazione.</li> </ul>

## 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.

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

La figura 3 illustra una configurazione di base che prevede un solo computer e un sistema di chiusura Apexx. 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 Apexx a fini di programmazione/configurazione del sistema.

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 Apexx eBox.

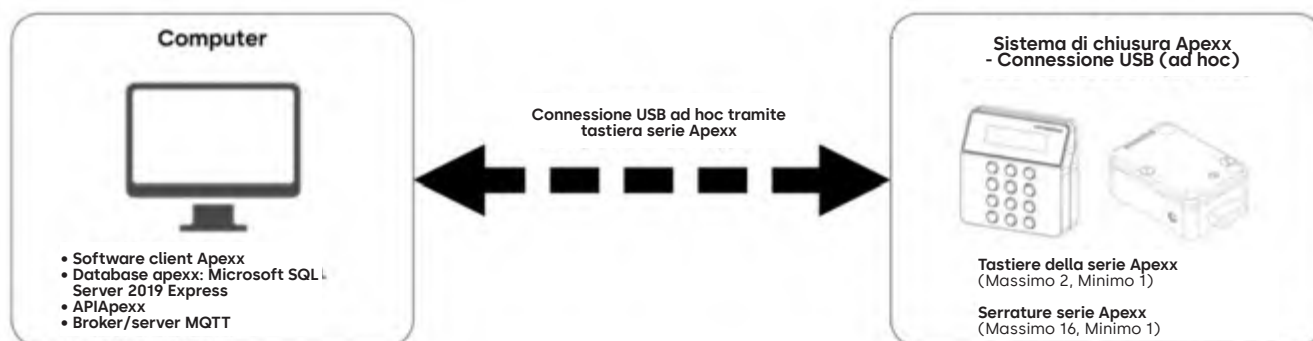


Figura 3 - Configurazione di un singolo computer - connessione USB ad hoc

La figura 4 mostra un'altra semplice configurazione con un solo computer e un sistema di chiusura Apexx, ma questa volta l'eBox Apexx viene utilizzato per fornire una connessione di rete/IP per una comunicazione continua/live tra il computer e il sistema di chiusura.

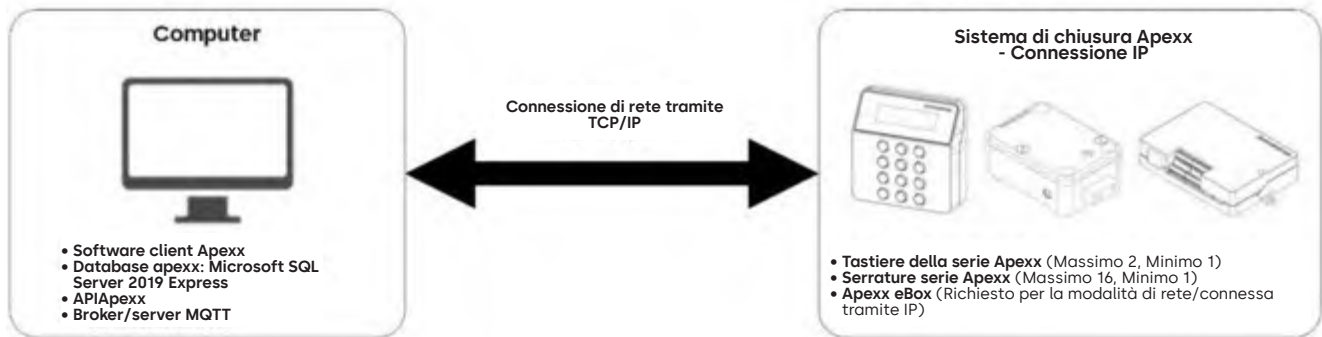


Figura 4 - Configurazione di un singolo computer - Rete tramite eBox (TCP/IP)

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).

Per i siti più grandi che coinvolgono edifici di dimensioni maggiori e/o sistemi di chiusura multipli, la configurazione a più computer mostrata nella figura 5 offre una maggiore flessibilità.

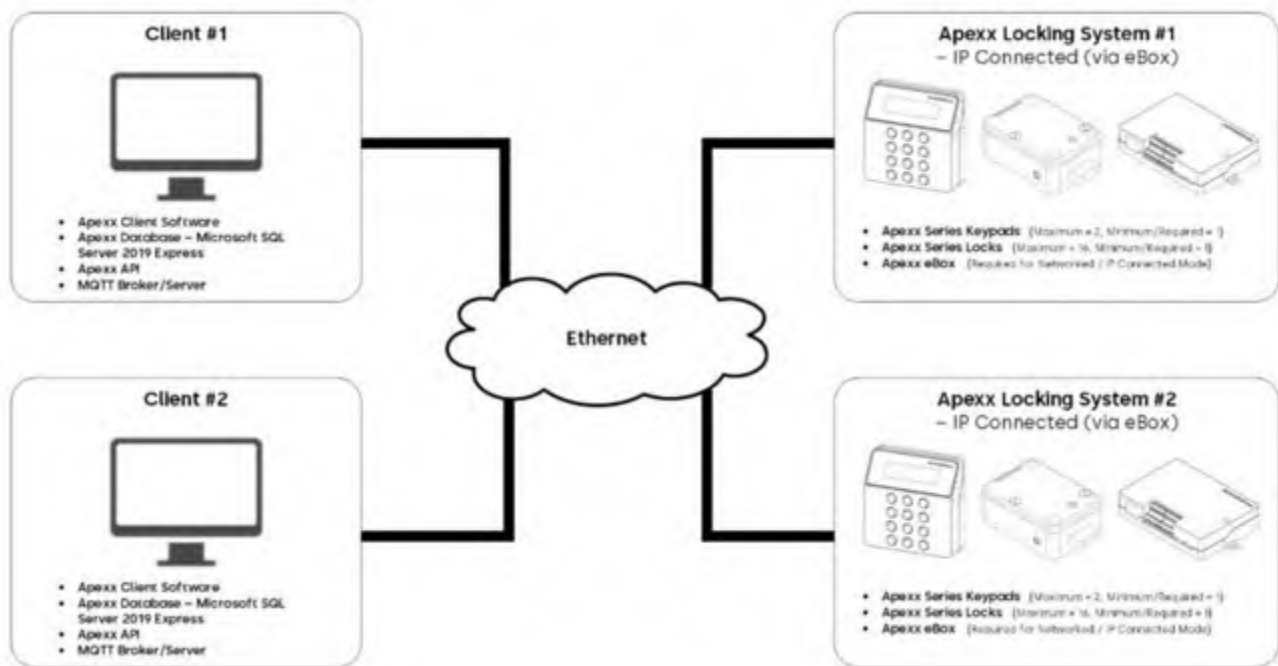


Figura 5 - Configurazione di più computer con sistemi di chiusura multipli

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 si collega alla rete tramite una eBox Apexx.

Questo concetto viene ulteriormente ampliato nel sistema illustrato nella figura 6, che comprende più computer e sistemi di chiusura distribuiti in più edifici.

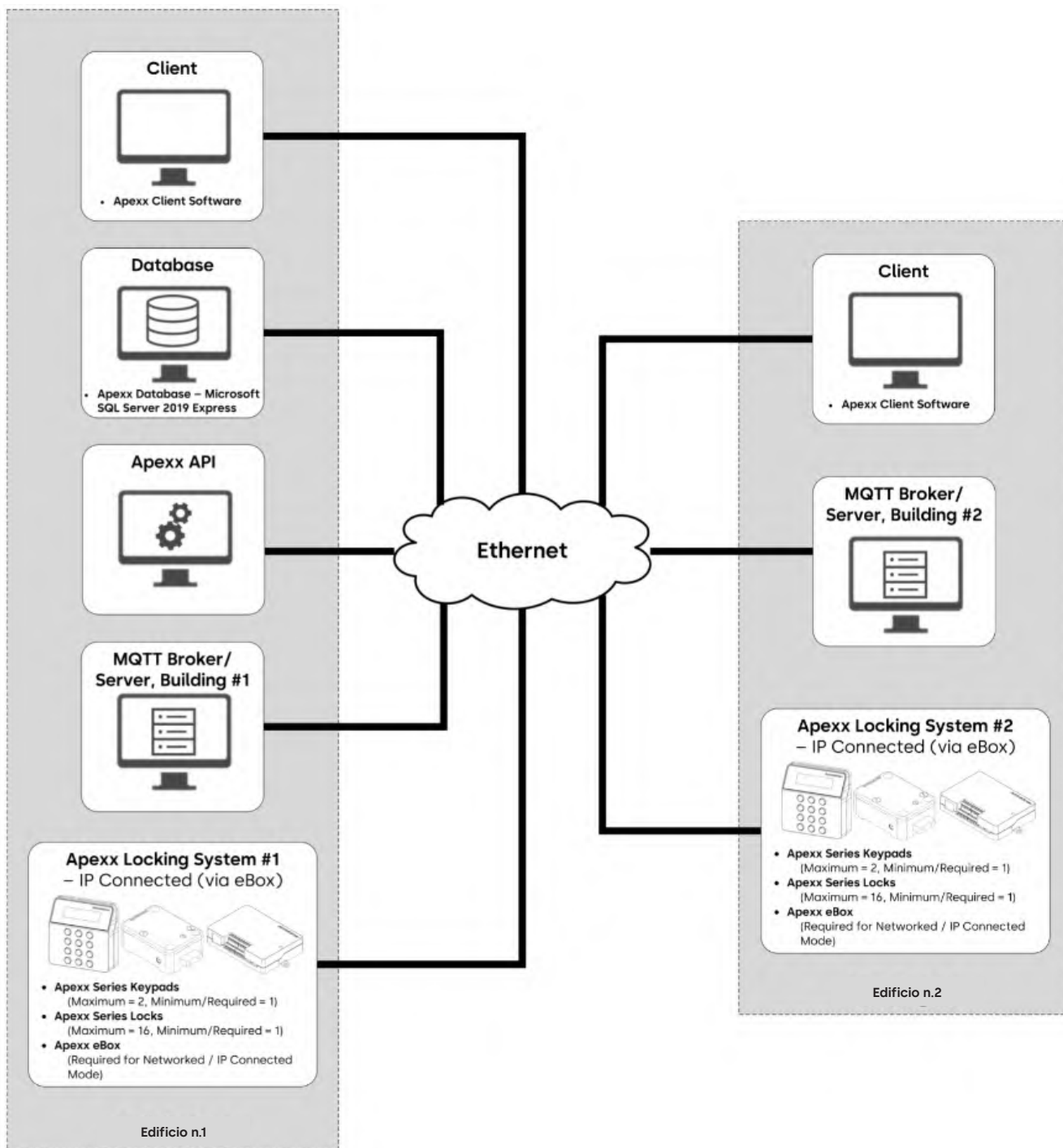


Figura 6 - Configurazione del sistema di chiusura e computer multipli con impostazione multi-server

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 ospitano 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 Apexx 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 del computer consigliate da Apexx

### Stazione di lavoro Client Apexx

- Intel Core i7 - 4470 3,40 GHz con 4 core
- 16 GB di RAM 1600 MHz DDR3 NON-ECC
- Disco rigido da 500 GB
- Windows 10 Professional 64 bit
- AMD RADEON HD 8490 1 GB Doppio Monitor o AMD RADEON HD8570 1 GB Doppio Monitor
- Porte USB 2.0
- Porta Ethernet - Scheda di rete da 1 GB
- Tastiera e mouse
- Backup UPS

### Server Broker Apexx

- Intel Xeon E5 - 2403, 1,80 GHz, 10 MB Cache
- 16 GB di RAM 1333 MHz, RDIMM
- Disco rigido da 500 GB
- Windows 2019 Server Standard 64 bit
- Scheda grafica HD integrata
- Porta Ethernet - Scheda di rete da 1 GB
- Tastiera e mouse
- Backup UPS

### Server di database Apexx e API Apexx

- Intel Xeon E5 - 2420, 1,90 GHz, 15 MB Cache con 6 core
- 32 GB di RAM 1333 MHz, RDIMM
- 2x unità disco da 1 TB 7,2K RPM SATA 3 GBps da 3,5 pollici
- Configurazione RAID 1
- Alimentazione doppia, hot plug, ridondante
- Windows 2019 Server Standard 64 bit
- Scheda grafica HD integrata
- Porta Ethernet - Scheda di rete GB
- Tastiera e mouse
- Backup UPS

## Il nostro impegno per la sostenibilità

Ci impegniamo a favorire uno sviluppo sostenibile lungo tutta la catena del valore nel rispetto delle nostre responsabilità economiche, ambientali e sociali verso le generazioni presenti e future. Nel settore dell'edilizia la sostenibilità a livello di prodotto è un approccio importante in un'ottica orientata al futuro. Per fornire informazioni quantitative sull'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.

[www.dormakaba.com/sustainability](http://www.dormakaba.com/sustainability)



## La nostra offerta

### Soluzioni di automazione degli accessi

Automazione degli ingressi  
Sicurezza degli ingressi



### Soluzioni per il controllo degli accessi

Controllo accessi e raccolta dati  
Sistemi di fuga e soccorso  
Sistemi per alloggi



### Soluzioni hardware e componentistica per accessi

Chiudiporta  
Hardware e componentistica architettonica  
Sistemi di chiusura meccanici



### Servizi

Assistenza tecnica  
Installazione e messa in funzione  
Manutenzione e riparazione



### Soluzioni chiavi e pareti

Sistemi di chiavi  
Pareti mobili/scorrevoli



### Serrature per cassaforti

Serrature elettroniche per cassaforti  
Serrature meccaniche per cassaforti  
Catenacci e accessori



### Sistemi in vetro

Sistemi di porte manuali  
Guarnizioni in vetro  
Pareti scorrevoli orizzontali



Architettura del sistema Apexx, IT, 02/2024  
Soggetto a modifiche senza preavviso

### dormakaba USA Inc.

1525 Bull Lea Road, Suite 100  
Lexington, KY 40511

[sales.safelocks.us@dormakaba.com](mailto:sales.safelocks.us@dormakaba.com)

T +1 800 950 4744

+1 888 950 4715 (assistenza tecnica)

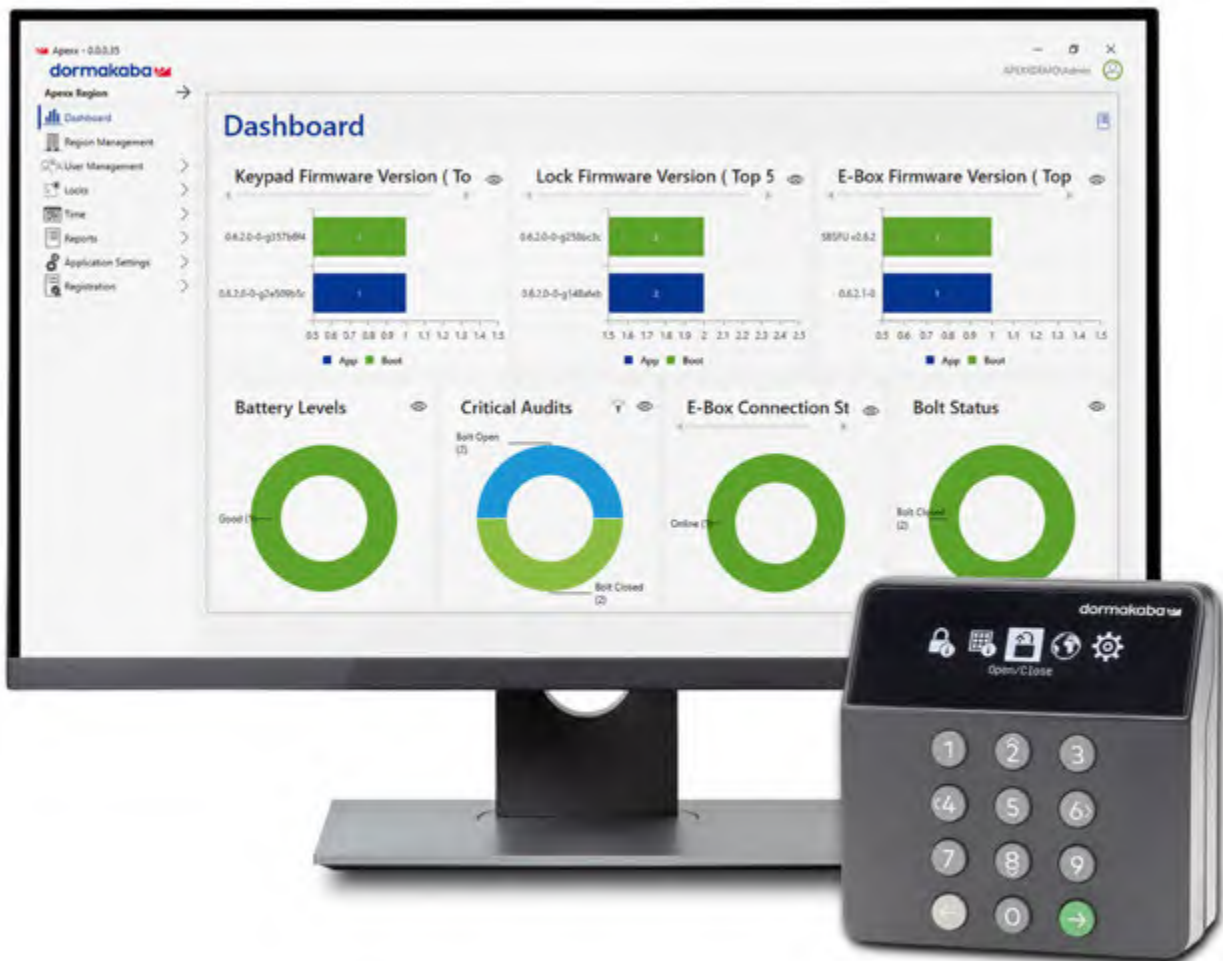
[dormakaba.com](http://dormakaba.com)



AXESSOR APEXX IP  
INSTALLATION AND  
OPERATION GUIDES

[dk.world/AxessorApexxIP](http://dk.world/AxessorApexxIP)

# Arquitetura do sistema do Axessor Apexx





# Índice

Arquitetura do sistema Apexx – Visão geral. ....	3
API Apexx. ....	3
Software do cliente Apexx . ....	3
Banco de dados Apexx . ....	3
MQTT Broker/Servidor . ....	3
SMTP. ....	4
SSO. ....	4
Configuração do usuário. ....	4
Licenças. ....	4
Atualizações de firmware locais e remotas . ....	4
Trânsito de dados. ....	5
Segurança e criptografia de dados . ....	6
Infraestrutura de chave pública (PKI) . ....	6
Configurações de hardware do computador. ....	7
Considerações sobre o banco de dados . ....	10
Especificações de computador recomendadas pela Apexx . ....	10

# Arquitetura do sistema Apexx

## Visão geral

Os sistemas de bloqueio Apexx podem ser divididos em duas redes de comunicação seguras: **barramento CAN do sistema de fechadura** e **rede de software/API**

O **barramento CAN do sistema de fechadura** é compatível com os seguintes componentes:

- **Teclados da série Apexx** (máximo = 2, mínimo/necessário = 1)
  - Usados como uma interface de usuário para acessar e configurar o sistema de bloqueio
- **Fechaduras da série Apexx** (máximo = 16, mínimo/necessário = 1)
  - Fechadura eletromecânica física que controla o acesso do usuário ao cofre
- **Apexx eBox** (necessário para o modo conectado em rede/IP)
  - Funciona como uma ponte entre o sistema de fechadura e a API/o software

A **API/o software** é composto por quatro componentes principais:

- Software de cliente Apexx
- Banco de dados Apexx – Microsoft SQL Server 2019 Express
- API Apexx
- MQTT Broker/servidor

## API Apexx

A Interface de Programação de Aplicativos, ou API, atua como editor e assinante na arquitetura MQTT.

## Software de cliente Apexx

O software cliente Apexx é uma interface gráfica do usuário (GUI) que permite que os usuários do software usem a API para executar ações no sistema (alterar as configurações do sistema, armazenar/recuperar dados etc.).

O Cliente Apexx oferece suporte a vários usuários, mas não a vários usuários simultâneos em um único cliente. Apenas uma pessoa pode estar conectada a uma única instância de cliente em um determinado momento.

## Banco de dados Apexx

O banco de dados Apexx funciona como o principal local de armazenamento de dados no sistema Apexx. O banco de dados Apexx usa o sistema de gerenciamento de banco de dados relacional proprietário da Microsoft, o Microsoft SQL Server 2019 Express, como um meio de armazenar e recuperar dados do sistema.

## MQTT Broker/servidor

O Message Queuing Telemetry Transport, ou MQTT, é um protocolo de mensagens que utiliza um modelo de publicação e assinatura para facilitar a comunicação entre dispositivos. O MQTT Broker/servidor atua como um hub de mensagens centralizado e utiliza o protocolo MQTT para gerenciar a comunicação entre dispositivos.

## SMTP

O software da série Apexx utiliza o protocolo SMTP (Simple Mail Transport Protocol) para enviar o seguinte: Alertas ativos e relatórios agendados.

- Os alertas ativos são enviados aos destinatários com base na ocorrência de um ou mais eventos de auditoria selecionados pelo usuário do software.
- Os relatórios programados podem ser enviados por e-mail aos destinatários com base em uma programação definida pelo usuário, também usando SMTP.

## SSO

O software da série Apexx utiliza o logon único, garantindo que um usuário do software possa usar suas credenciais para fazer login na API usando um único conjunto de credenciais.

## Configuração do usuário

Os usuários do sistema Apexx se enquadram em duas categorias distintas: **Usuários de fechaduras para cofre** e **usuários de software**.

**Os usuários de fechaduras para cofre** utilizarão o sistema de travamento (que consiste em teclados físicos, fechaduras, eBox etc.) e terão credenciais e funções exclusivas com permissões que determinam o acesso ao sistema de travamento.

Os usuários de fechaduras para cofre usam IDs de usuário e PINs numéricos para acessar o sistema de travamento com o teclado da série Apexx.

Os três tipos de usuário padrão de fechaduras para cofre (Administrador, Gerente e Usuário) constituem uma hierarquia de usuários com funções e privilégios predefinidos no sistema de travamento. Além desses tipos de usuários, é possível criar funções de usuário adicionais da fechadura para cofre usando as ferramentas administrativas do software da série Apexx com permissões definidas por um usuário do software.

**Usuários de software** são usuários que executam o software da série Apexx e usam as ferramentas de software para realizar tarefas administrativas e de gerenciamento. Diferentemente dos usuários de fechaduras para cofres, os usuários de software não acessam diretamente o sistema de bloqueio físico (abrir/fechar portas de cofres), mas executam tarefas administrativas/gerenciais por meio do software (adicionar usuários de fechadura para cofre, redefinir senhas de usuários de fechaduras).

Os usuários do software usam credenciais para obter acesso ao software da série Apexx usando logon único (SSO). Os usuários de software com permissão de "gravação" podem adicionar novos usuários de software e configurar as permissões de leitura/gravação.

## Licenças

O software da série Apexx tem vários tipos de licença disponíveis, em que cada um deles desbloqueia diferentes funções e recursos do software. Consulte o Catálogo de preços do Axessor Apexx IP para obter mais informações.

## Atualizações de firmware locais ou remotas

O processo de atualização do firmware do dispositivo é diferente dependendo da licença comprada.

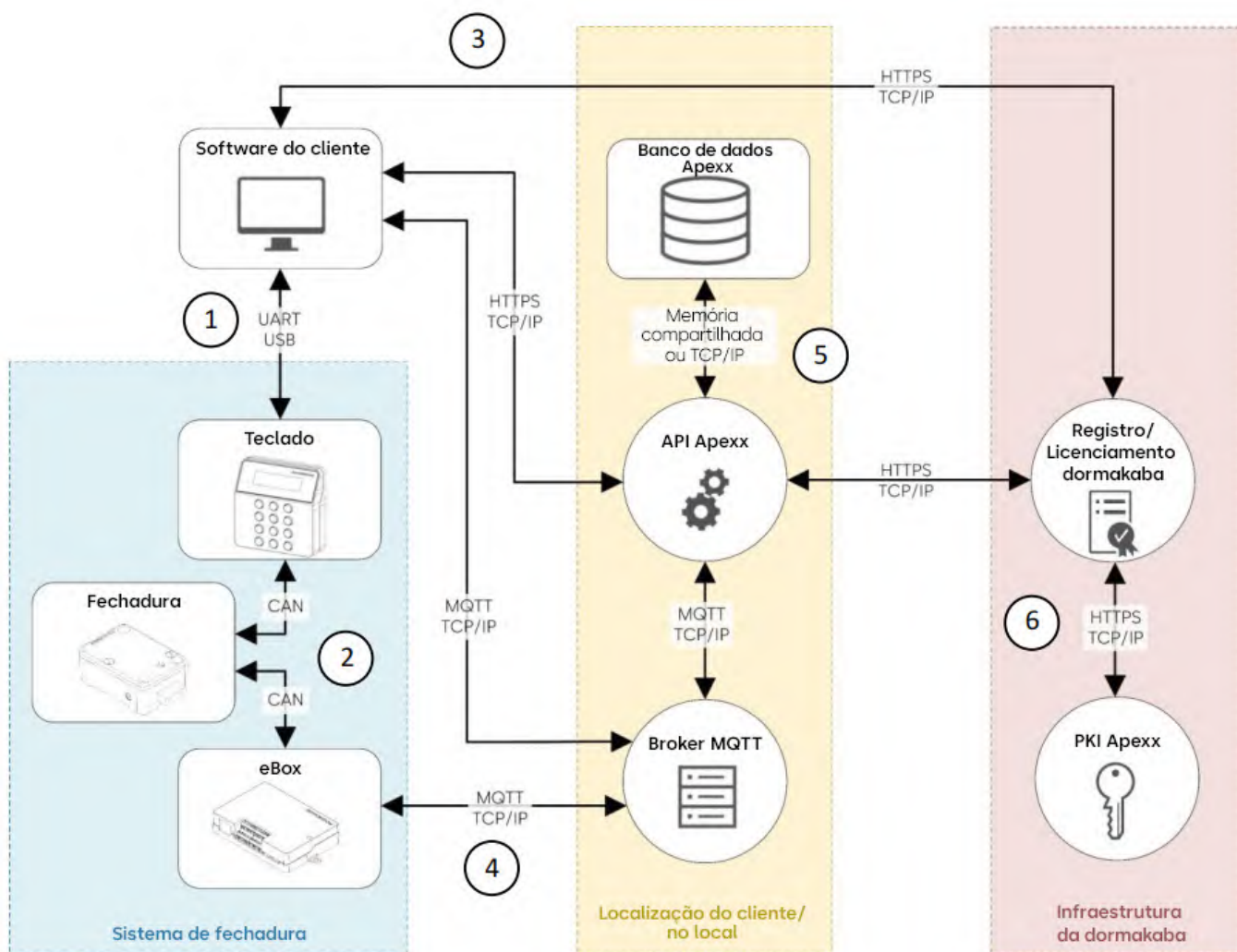
A licença "Apexx Local" permite apenas atualizações locais de firmware, o que pode ser feito estabelecendo uma conexão USB temporária entre o computador que hospeda o software da série Apexx e o teclado do seu sistema de bloqueio.

A licença "Apexx IP" permite que você realize **atualizações remotas de firmware**, que podem ser feitas por meio de uma conexão de rede via eBox. Esse é um processo de três etapas:

1. Um usuário de software inicia o processo de atualização remota do firmware, enviando o firmware da API/do software para o sistema de travamento pela eBox.
2. O firmware é baixado e armazenado no sistema de travamento. Será exibida uma mensagem no visor do teclado que informa aos usuários da fechadura para cofre que há uma atualização de firmware pendente.
3. Um usuário de fechadura para cofre insere credenciais válidas (ID de usuário e PIN) no teclado e, em seguida, inicia a atualização do firmware.

Para obter mais informações sobre o processo de atualização do firmware, consulte o **Guia do usuário do sistema Acessor Apexx** e o menu de ajuda do **software da série Apexx**.

## Trânsito de dados



## Trânsito de dados

	Protocolos de comunicação	Fluxo de dados	Descrição/Objetivo
1	UART por USB	Caminho bidirecional: <ul style="list-style-type: none"> <li>Software cliente para teclado</li> </ul>	Configuração direta e recuperação de auditoria
2	CAN	Caminho bidirecional: <ul style="list-style-type: none"> <li>Teclado da fechadura</li> <li>Fechadura para eBox</li> </ul>	Comunicação entre dispositivos
3	HTTPS por TCP/IP	Caminho bidirecional: <ul style="list-style-type: none"> <li>Software cliente para registro/licenciamento da dormakaba</li> </ul>	Licenciamento e registro on-line
4	MQTT por TCP/IP	Caminho bidirecional: <ul style="list-style-type: none"> <li>Software cliente para o MQTT Broker</li> </ul> Caminho bidirecional: <ul style="list-style-type: none"> <li>eBox para MQTT Broker</li> </ul>	Configuração em rede e recuperação de auditoria
5	Memória compartilhada ou TCP/IP	Caminho bidirecional: <ul style="list-style-type: none"> <li>API Apexx para banco de dados Apexx</li> </ul>	Armazenamento persistente de dados com o SQL Server
6	HTTPS por TCP/IP	Caminho bidirecional: <ul style="list-style-type: none"> <li>Software cliente para API Apexx</li> <li>API Apexx para registro/licenciamento da dormakaba</li> <li>Registro/Licenciamento da dormakaba para a PKI Apexx</li> </ul>	Emissão de certificados x.509

## Segurança e criptografia de dados

O sistema Apexx emprega vários métodos de criptografia, incluindo AES256, PBKDF2 e certificados TLS, para garantir a comunicação e o armazenamento seguros dos dados.

## Infraestrutura de chave pública (PKI)

O sistema Apexx utiliza uma infraestrutura de chave pública para criar, armazenar e distribuir certificados digitais para dispositivos Apexx por meio de uma autoridade de certificação.

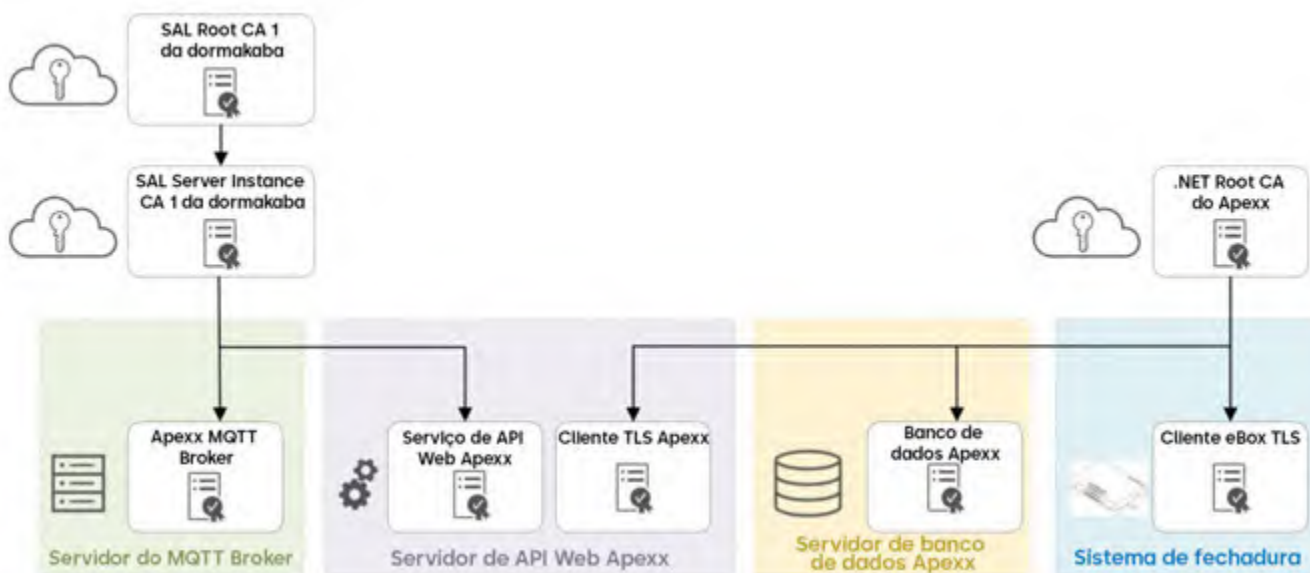


Figura 2 – Infraestrutura de chave pública

## Infraestrutura de chave pública (PKI)

Tipo de certificado	Descrição
SAL Root CA da dormakaba	<ul style="list-style-type: none"><li>• Esse certificado é pré-carregado nos dispositivos na fábrica e substituído por meio da atualização do firmware</li></ul>
SAL Server Instance CA da dormakaba	<ul style="list-style-type: none"><li>• Os servidores que executam serviços de software locais para o Apexx precisam de certificados assinados pela PKI do SAL da dormakaba para que os dispositivos confiem neles.</li><li>• Esse certificado deve ser implantado em todos os servidores que executam serviços de software locais.</li><li>• A PKI do software local assina solicitações de certificado para todos os clientes do MQTT Broker.</li><li>• Esses certificados são usados para estabelecer conexões TLS (Transport Layer Security) de confiança mútua e autenticar com o MQTT Broker.</li><li>• Eles também podem assinar os certificados usados pelo SQL Server para TLS.</li><li>• Se todos os serviços estiverem hospedados em um único servidor, não será necessário que vários certificados sejam assinados pela PKI do SAL da dormakaba.</li><li>• Até mesmo o banco de dados pode usar esse certificado se estiver hospedado no mesmo servidor.</li></ul>
Apexx MQTT Broker	<ul style="list-style-type: none"><li>• Criado durante a instalação do software</li><li>• Usado para conexões TLS e autenticação</li></ul>
Serviço de API Web Apexx	<ul style="list-style-type: none"><li>• Criado durante a instalação do software</li><li>• Contém o nome do servidor (computador em que o serviço está instalado), a autoridade de certificação confiável e a chave de criptografia pública do servidor</li></ul>
Cliente TLS Apexx	<ul style="list-style-type: none"><li>• Usado para autenticação do cliente Apexx</li><li>• O certificado é um usuário verificado se o emissor corresponder a .NET Root CA do Apexx instalada no servidor do broker</li></ul>
Banco de dados Apexx	<ul style="list-style-type: none"><li>• SQL Server no Windows é o único mecanismo de banco de dados compatível</li><li>• As configurações a seguir estão ativadas na instância/no banco de dados:<ul style="list-style-type: none"><li>• Autenticação do Windows</li></ul></li><li>• O RBAC (controle de acesso baseado em função) é usado juntamente com a autenticação do Windows para controlar as permissões</li></ul>
Cliente eBox TLS	<ul style="list-style-type: none"><li>• Usado para autenticação da eBox</li><li>• O certificado é um usuário verificado se o emissor corresponder a .NET Root CA do Apexx instalada no servidor do broker</li></ul>
.NET Root CA do Apexx	<ul style="list-style-type: none"><li>• Criado durante a instalação do software</li><li>• Qualquer computador que esteja executando o software (cliente, servidor, banco de dados etc.) precisa de uma cópia desse certificado para fins de segurança/identificação</li></ul>

## Configurações de hardware de computador

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

**Observação:** Se desejar, qualquer um dos componentes de software (cliente, banco de dados, API ou MQTT) pode ser hospedado em uma máquina virtual.

A Figura 3 ilustra uma configuração básica que envolve um único computador e um sistema de travamento Apexx. Nessa configuração, todos os elementos de API/software são hospedados em um único computador e a conexão USB é usada para se conectar temporariamente ao sistema de travamento Apexx para fins de programação/configuração do sistema.



Esse tipo de configuração funciona bem em locais pequenos, onde o computador e todos os componentes do sistema de travamento (teclados e fechaduras) estão no mesmo local físico. Mas essa opção não tem a versatilidade e a conveniência oferecidas pelas configurações em rede que utilizam o Apexx eBox.



Figura 3 – Configuração de um único computador (conexão USB ad hoc)

A Figura 4 mostra outra configuração simples que envolve apenas um computador e um sistema de bloqueio Apexx, mas, desta vez, o Apexx eBox é usado para fornecer uma conexão de rede/IP para comunicação contínua/em tempo real entre o computador e o sistema de travamento.



Figura 4 – Configuração de um único computador (rede via eBox [TCP/IP])

Essa configuração também é útil para configurações menores em que todos os equipamentos estão no mesmo local físico, mas a eBox permite que o administrador do sistema aproveite todos os recursos fornecidos por uma conexão IP ativa (auditorias em tempo real, monitoramento ativo do sistema, atualizações remotas de firmware e outros recursos adicionais de hardware/software). Para locais maiores, que envolvem edifícios maiores e/ou vários sistemas de travamento, a configuração de vários computadores mostrada na Figura 5 oferece maior flexibilidade.

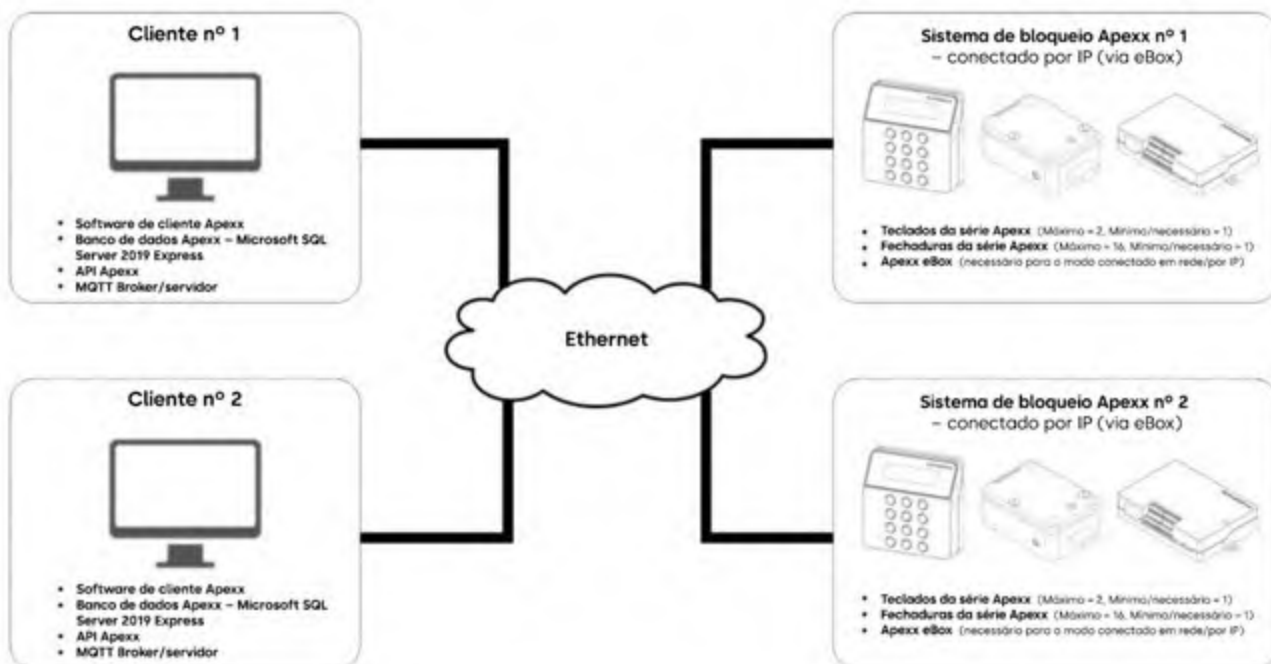


Figura 5 – Configuração de vários computadores e sistemas de travamento



Nessa configuração, qualquer um ou todos os componentes de software podem ser instalados em um ou mais computadores (ou máquinas virtuais), o que permite maior conveniência e flexibilidade na execução e na configuração de seus sistemas de travamento. Observe que cada sistema de travamento se conecta à rede pela Apexx eBox.

Esse conceito é expandido ainda mais no sistema mostrado na Figura 6, que inclui vários computadores e sistemas de travamento que abrangem vários edifícios.

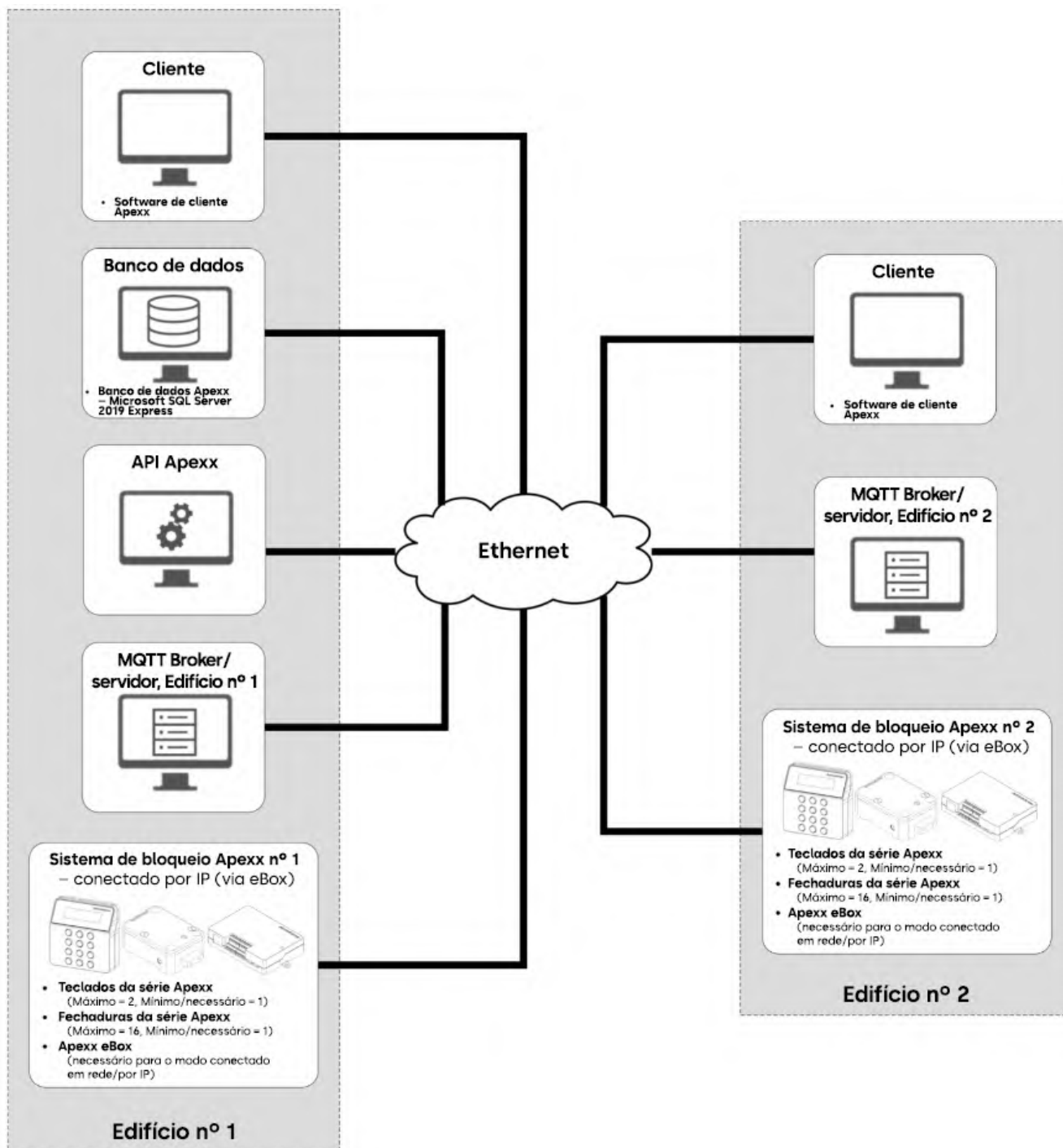


Figura 6 – Configuração de vários computadores/sistemas de travamento com configuração de vários servidores

Uma grande diferença entre essa configuração e as outras é que ela inclui vários computadores que hospedam diferentes componentes de software. Observe como dois dos computadores no Edifício nº 1 hospedam a API e o banco de dados Apexx, respectivamente. Esses dois computadores podem ser configurados para serem usados como API e banco de dados nos sistemas de travamento no Edifício nº 1, no Edifício nº 2 e/ou em qualquer outro sistema Apexx em toda a rede.

O exemplo final na Figura 6 ilustra que diversas configurações diferentes podem ser aplicadas, dependendo de suas necessidades organizacionais e da configuração da infraestrutura de TI.

## Considerações sobre o banco de dados

O software da série Apexx inclui o Microsoft SQL Server 2019 Express como seu mecanismo de banco de dados interno dedicado

	Microsoft SQL Server 2019 Express (64 bits)
Limite do banco de dados	10 GB
Número de CPUs	1 processador físico
RAM	1 GB
Sistemas operacionais compatíveis	Windows 10, Windows Server 2016, Windows Server 2019

## Especificações de computador recomendadas pelo Apexx

### Estação de trabalho do cliente Apexx

- Intel Core i7 – 4470 3,40 GHz com 4 núcleos
- 16 GB de RAM 1600 MHz DDR3 NÃO ECC
- Disco rígido de 500 GB
- Windows 10 Professional 64 bits
- Monitor duplo AMD RADEON HD 8490 de 1 GB ou monitor duplo AMD RADEON HD8570 de 1 GB
- Portas USB 2.0
- Porta Ethernet – placa de rede de 1 Gb
- Teclado e mouse
- Backup de UPS

### Servidor do Apexx Broker

- Intel Xeon E5 – 2403, 1,80 GHz, 10 MB de cache
- 16 GB de RAM 1333 MHz, RDIMM
- Disco rígido de 500 GB
- Windows 2019 Server Standard 64 bits
- Placa gráfica HD integrada
- Porta Ethernet – placa de rede de 1 Gb
- Teclado e mouse
- Backup de UPS

### Servidor de banco de dados e API Apexx

- Intel Xeon E5 – 2420, 1,90 GHz, cache de 15 MB com 6 núcleos
- 32 GB de RAM 1333 MHz, RDIMM
- 2 x disco rígido de 1 TB 7,2 K RPM SATA 3 Gbps 3,5 pol.
- Configuração de RAID 1
- Fonte de alimentação dupla, hot-plug e redundante
- Windows 2019 Server Standard 64 bits
- Placa gráfica HD integrada
- Porta Ethernet – placa de rede Gb
- Teclado e mouse
- Backup de UPS

## Nosso compromisso com a sustentabilidade

Somos comprometidos com a promoção do desenvolvimento sustentável em toda a cadeia de valor, de acordo com nossas responsabilidades econômicas, ambientais e sociais para com as gerações atuais e futuras. A sustentabilidade no nível de produto é uma abordagem importante e orientada para o futuro no campo da construção. Para fornecer divulgações expressas do impacto ambiental de um produto em todo o seu ciclo de vida, a dormakaba fornece Declarações ambientais de produto (EPD), com base em avaliações holísticas do ciclo de vida.

[www.dormakaba.com/sustainability](http://www.dormakaba.com/sustainability)



## Nossa oferta

### Soluções de automação de acesso

Automação de entrada  
Segurança de entrada



### Soluções de controle de acesso

Dados e acesso eletrônicos  
Sistemas de fuga e resgate  
Sistemas de hospedagem



### Soluções de hardware de acesso

Fechaduras de portas  
Hardware de arquitetura  
Sistemas de chaves mecânicas



### Serviços

Suporte técnico  
Instalação e comissionamento  
Manutenção e reparo



### Soluções para chaves e paredes

Sistemas de chaves  
Paredes móveis/deslizantes



### Fechaduras para cofres

Fechaduras eletrônicas para cofres  
Fechaduras mecânicas para cofres  
Mecanismo de fechamento e acessórios



### Sistemas de vidro

Sistemas de portas manuais  
Acessórios de vidro  
Paredes deslizantes horizontais



Arquitetura do sistema Apexx, PTBR, 02/2024  
Sujeito a alterações sem aviso prévio

### dormakaba USA Inc.

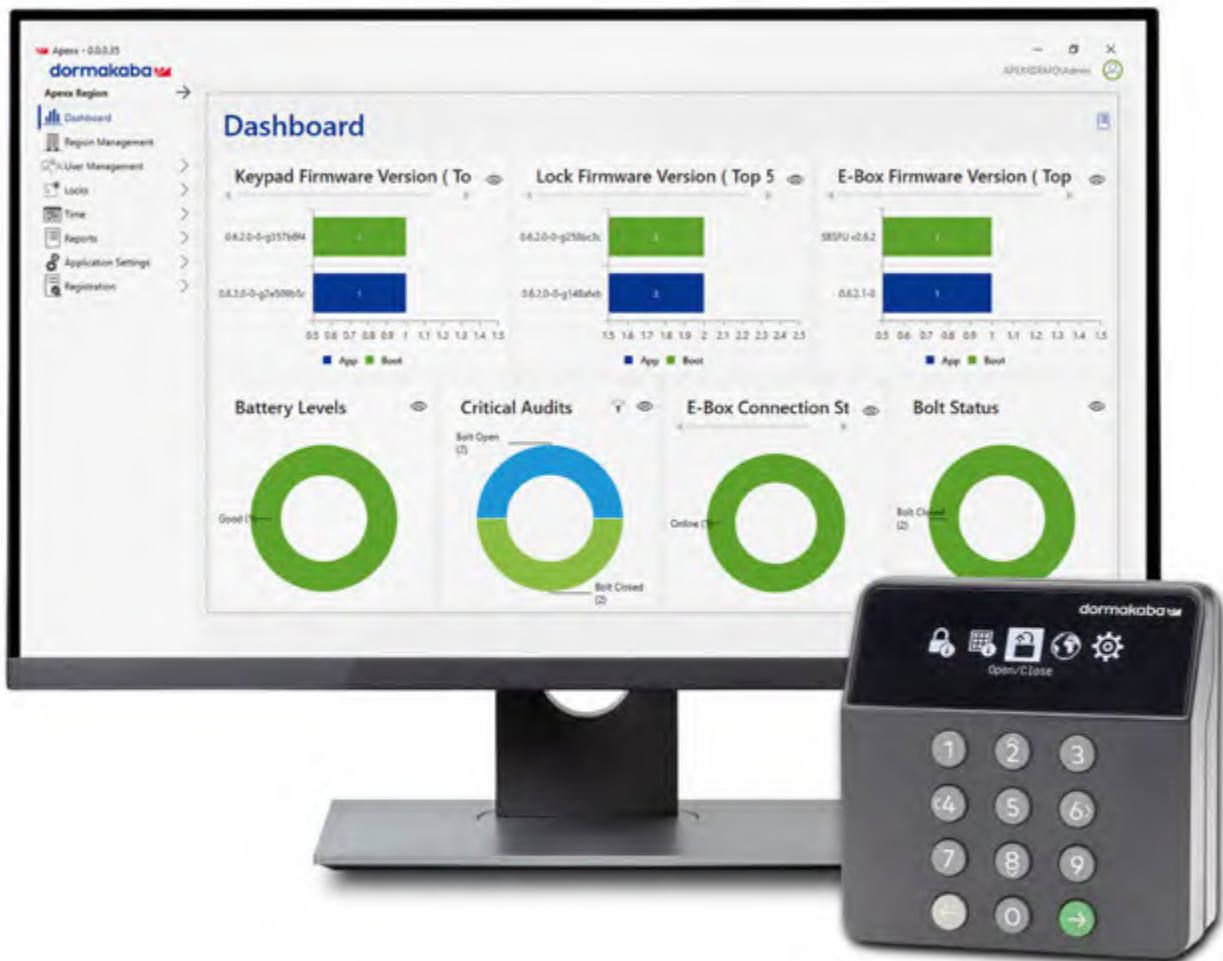
1525 Bull Lea Road, Suite 100  
Lexington, KY 40511  
[sales.safelocks.us@dormakaba.com](mailto:sales.safelocks.us@dormakaba.com)  
T +1 800 950 4744  
+1 888 950 4715 (suporte técnico)  
[dormakaba.com](http://dormakaba.com)



AXESSOR APEXX IP  
INSTALAÇÃO E  
GUIAS DE OPERAÇÃO

[dk.world/AxessorApexxIP](http://dk.world/AxessorApexxIP)

# Architektura systemu Axessor Apexx



# Spis treści

Architektura systemu Apexx - przegląd. ....	3
Apexx API. ....	3
Oprogramowanie klienckie Apexx . ....	3
Baza danych Apexx . ....	3
Broker/serwer MQTT. ....	3
SMTP. ....	4
SSO. ....	4
Konfiguracja użytkownika . ....	4
Licencje . ....	4
Lokalne i zdalne aktualizacje oprogramowania układowego . ....	4
Transmisja danych . ....	5
Bezpieczeństwo i szyfrowanie danych . ....	6
Infrastruktura klucza publicznego (PKI). ....	6
Konfiguracje sprzętu komputerowego. ....	7
Rozważania dotyczące bazy danych. ....	10
Dane techniczne komputera zalecane przez Apexx . ....	10

# Architektura systemu Apexx

## Przegląd

Systemy blokujące Apexx można podzielić na 2 bezpieczne sieci komunikacyjne: **Magistrala Can systemu blokującego** i **sieć API/oprogramowania**.

**Magistrala CAN systemu blokującego** 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 pomost między systemem zamka a interfejsem API/oprogramowaniem

**API/Software** składa się z 4 głównych komponentów:

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

## Apexx API

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

## Oprogramowanie klienckie Apexx

Oprogramowanie klienckie Apexx to graficzny interfejs użytkownika (GUI), który umożliwia użytkownikom oprogramowania korzystanie z interfejsu API do wykonywania czynności w systemie (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.

## SMTP

Oprogramowanie serii Apexx wykorzystuje protokół SMTP (Simple Mail Transport Protocol) do wysyłania następujących wiadomości: Aktywne alerty i Zaplanowane raporty.

- 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.

## 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

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

**Użytkownicy zamków sejfowych** to użytkownicy, którzy będą korzystać z systemu zamków (składającego się z fizycznych klawiatur, zamków, eBox itp.) i 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.

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.

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

## Licencje

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

## Lokalne i zdalne aktualizacje oprogramowania układowego

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

Licencja "Apexx Local" pozwala tylko na lokalne aktualizacje oprogramowania układowego, które można wykonać poprzez ustanowienie tymczasowego połączenia USB między komputerem z oprogramowaniem serii Apexx a klawiaturą systemu zamka.

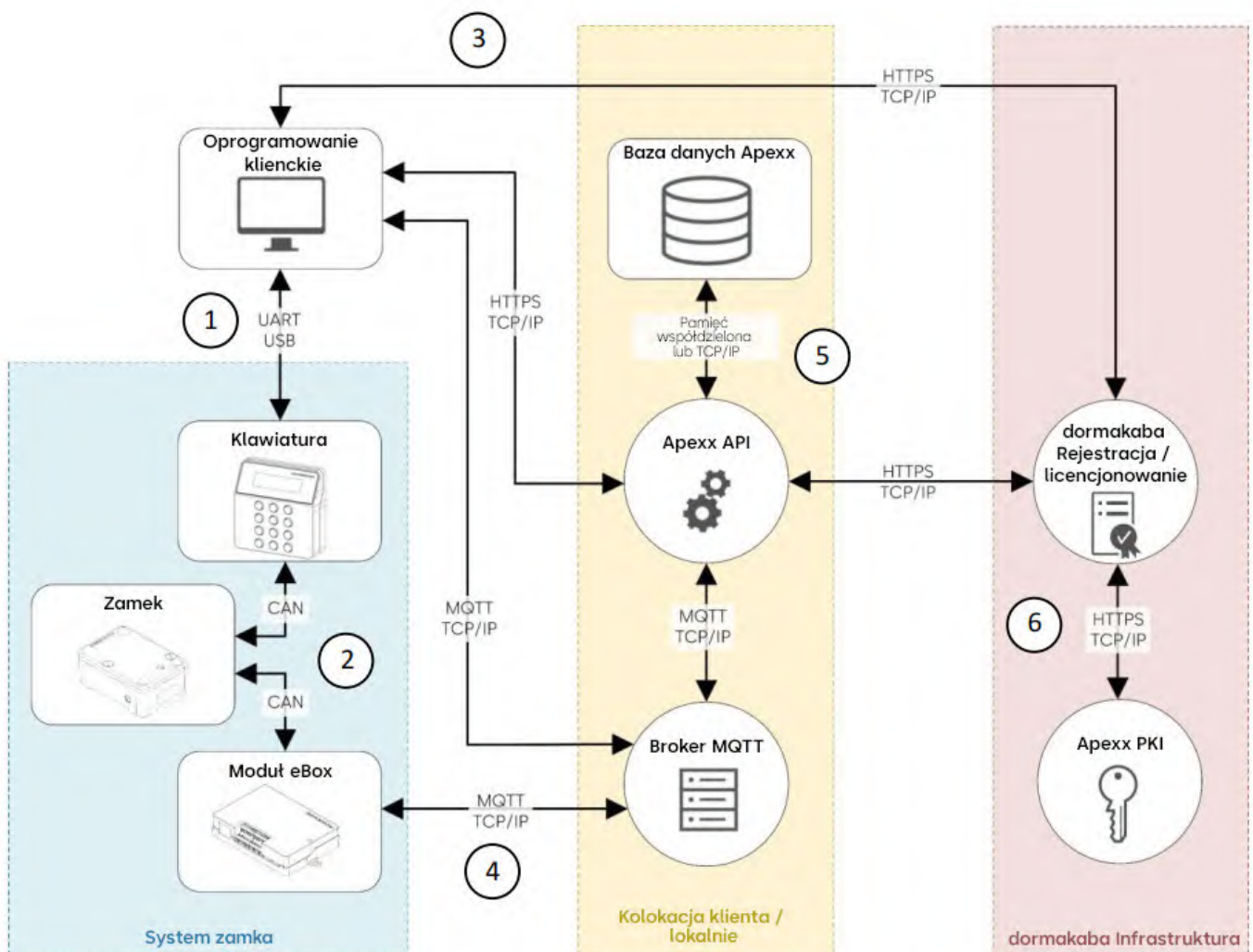


Licencja "Apexx IP" pozwala na wykonywanie **zdalnych aktualizacji oprogramowania układowego**, które mogą być wykonywane przez połączenie sieciowe za pośrednictwem eBox. Jest to proces składający się z trzech etapów:

1. Użytkownik oprogramowania inicjuje proces zdalnej aktualizacji oprogramowania układowego, przysyłając 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.

Więcej informacji na temat procesu aktualizacji oprogramowania układowego można znaleźć w **Podręczniku użytkownika systemu Axessor Apexx** oraz w menu pomocy **oprogramowania serii Apexx**.

## Transmisja danych



## Transmisja danych

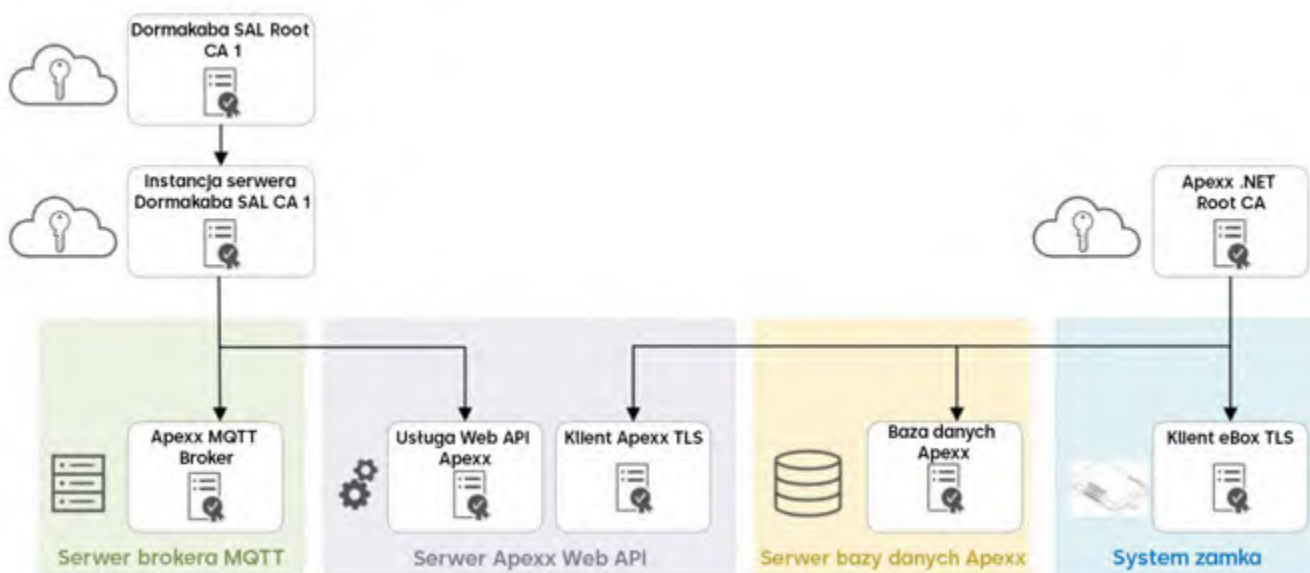
	Komunikacja Protokoły	Przepływ danych	Opis / cel
1	UART przez USB	Ścieżka dwukierunkowa: <ul style="list-style-type: none"> <li>Oprogramowanie klienckie do klawiatury</li> </ul>	Bezpośrednia konfiguracja i pobieranie audytów
2	CAN	Ścieżka dwukierunkowa: <ul style="list-style-type: none"> <li>Klawiatura do zamka</li> <li>Blokada do eBox</li> </ul>	Komunikacja między urządzeniami
3	HTTPS przez TCP/IP	Ścieżka dwukierunkowa: <ul style="list-style-type: none"> <li>Oprogramowanie klienckie do rejestracji/licencjonowania dormakaba</li> </ul>	Licencjonowanie i rejestracja online
4	MQTT przez TCP/IP	Ścieżka dwukierunkowa: <ul style="list-style-type: none"> <li>Oprogramowanie klienckie dla brokera MQTT</li> </ul> Ścieżka dwukierunkowa: <ul style="list-style-type: none"> <li>eBox do brokera MQTT</li> </ul>	Konfiguracja sieciowa i wyszukiwanie audytów
5	Pamięć współdzielona lub TCP/IP	Ścieżka dwukierunkowa: <ul style="list-style-type: none"> <li>Apexx API do bazy danych Apexx</li> </ul>	Trwałe przechowywanie danych za pomocą SQL Server
6	HTTPS przez TCP/IP	Ścieżka dwukierunkowa: <ul style="list-style-type: none"> <li>Oprogramowanie klienckie do Apexx API</li> <li>Apexx API do dormakaba Rejestracja/Licencjonowanie</li> <li>dormakaba Rejestracja/licencjonowanie w Apexx PKI</li> </ul>	Wydawanie certyfikatów x.509

## Bezpieczeństwo i szyfrowanie danych

System Apexx wykorzystuje wiele metod szyfrowania, w tym AES256, PBKDF2 i certyfikaty TLS, aby zapewnić bezpieczną komunikację i przechowywanie danych.

## Infrastruktura klucza publicznego (PKI)

System Apexx wykorzystuje infrastrukturę klucza publicznego do tworzenia, przechowywania i dystrybucji certyfikatów cyfrowych do urządzeń Apexx za pośrednictwem instytucji certyfikującej.



Rysunek 2 – Infrastruktura klucza publicznego

## Infrastruktura klucza publicznego (PKI)

Typ certyfikatu	Opis
dormakaba SAL Root CA	<ul style="list-style-type: none"><li>Certyfikat ten jest fabrycznie wgrany do urządzeń i wymieniany poprzez aktualizację oprogramowania układowego</li></ul>
Instancja serwera dormakaba SAL CA	<ul style="list-style-type: none"><li>Serwery uruchamiające lokalne usługi oprogramowania dla Apexx wymagają certyfikatów podpisanych przez dormakaba SAL PKI, aby urządzenia mogły im zaufać</li><li>Certyfikat ten musi zostać wdrożony na wszystkich serwerach z uruchomionymi lokalnymi usługami oprogramowania</li><li>Lokalne oprogramowanie PKI podpisuje żądania certyfikatów dla wszystkich klientów brokera MQTT</li><li>Certyfikaty te są używane zarówno do ustanawiania połączeń wzajemnego zaufania Transport Layer Security (TLS), jak i uwierzytelniania z brokerem MQTT</li><li>Może również podpisywać certyfikaty używane przez SQL Server dla TLS</li><li>Jeśli wszystkie usługi są hostowane na jednym serwerze, nie jest wymagane podpisywanie wielu certyfikatów przez Dormakaba SAL PKI</li><li>Nawet baza danych może korzystać z tego certyfikatu, jeśli jest hostowana na tym samym serwerze</li></ul>
Apexx MQTT Broker	<ul style="list-style-type: none"><li>Utworzony podczas instalacji oprogramowania</li><li>Używany do połączeń TLS i uwierzytelniania</li></ul>
Usługa Web API Apexx	<ul style="list-style-type: none"><li>Utworzona podczas instalacji oprogramowania</li><li>Zawiera nazwę serwera (komputer, na którym zainstalowana jest ta usługa), zaufaną instytucję certyfikującą i publiczny klucz szyfrowania serwera</li></ul>
Klient Apexx TLS	<ul style="list-style-type: none"><li>Służy do uwierzytelniania klienta Apexx</li><li>Certyfikat jest zweryfikowanym użytkownikiem, jeśli wystawca jest zgodny z Apexx .NET Root CA zainstalowanym na serwerze brokera</li></ul>
Baza danych Apexx	<ul style="list-style-type: none"><li>SQL Server w systemie Windows jest jedynym obsługiwany silnikiem bazy danych</li><li>Następujące ustawienia są włączone w instancji/bazie danych:<ul style="list-style-type: none"><li>Uwierzytelnianie systemu Windows</li></ul></li><li>Kontrola dostępu oparta na rolach (RBAC) jest używana wraz z uwierzytelnianiem systemu Windows do kontrolowania uprawnień</li></ul>
Klient eBox TLS	<ul style="list-style-type: none"><li>Służy do uwierzytelniania eBox</li><li>Certyfikat jest zweryfikowanym użytkownikiem, jeśli wystawca jest zgodny z Apexx .NET Root CA zainstalowanym na serwerze brokera</li></ul>
Apexx .NET Root CA	<ul style="list-style-type: none"><li>Utworzona podczas instalacji oprogramowania</li><li>Każdy komputer z uruchomionym oprogramowaniem (klient, serwer, baza danych itp.) wymaga kopii tego certyfikatu do celów bezpieczeństwa/identyfikacji</li></ul>

## 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 cenniku Axessor Apexx.

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

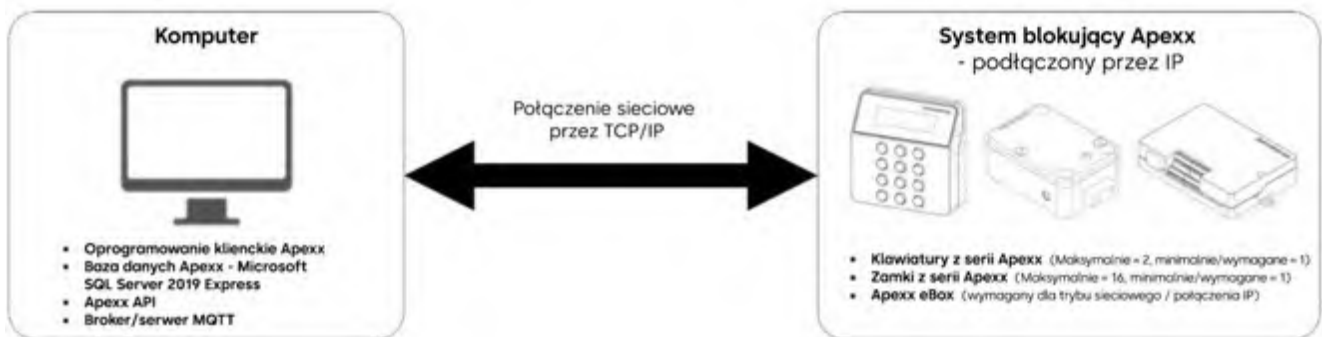
Rysunek 3 ilustruje podstawową konfigurację obejmującą tylko jeden komputer i jeden system blokujący Apexx. W tej konfiguracji wszystkie elementy API / oprogramowania są hostowane na jednym komputerze z połączeniem USB używanym do tymczasowego połączenia z systemem blokującym Apexx w celu programowania / konfiguracji systemu.

Ten rodzaj konfiguracji 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 konfigurację sieciową wykorzystującą Apexx eBox.



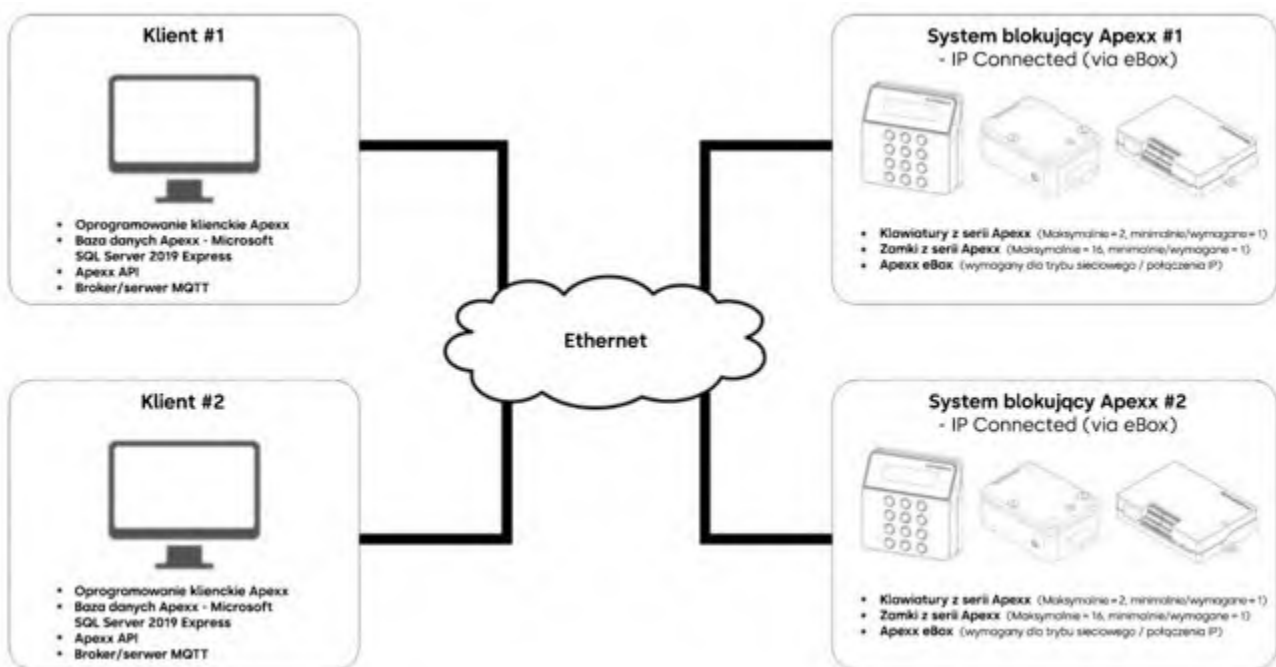
Rysunek 3 – Konfiguracja pojedynczego komputera - połączenie USB ad hoc

Rysunek 4 przedstawia kolejną prostą konfigurację obejmującą tylko jeden komputer i jeden system zamykania Apexx, ale tym razem Apexx eBox służy do zapewnienia połączenia sieciowego / IP w celu ciągłej / bieżącej komunikacji między komputerem a systemem zamykania.



Rysunek 4 – Konfiguracja pojedynczego komputera - sieć przez eBox (TCP/IP)

Ta konfiguracja jest również przydatna w przypadku mniejszych konfiguracji, 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). W przypadku większych obiektów obejmujących duże budynki i/lub wiele systemów blokujących, konfiguracja z wieloma komputerami pokazana na rysunku 5 zapewnia dodatkową elastyczność.

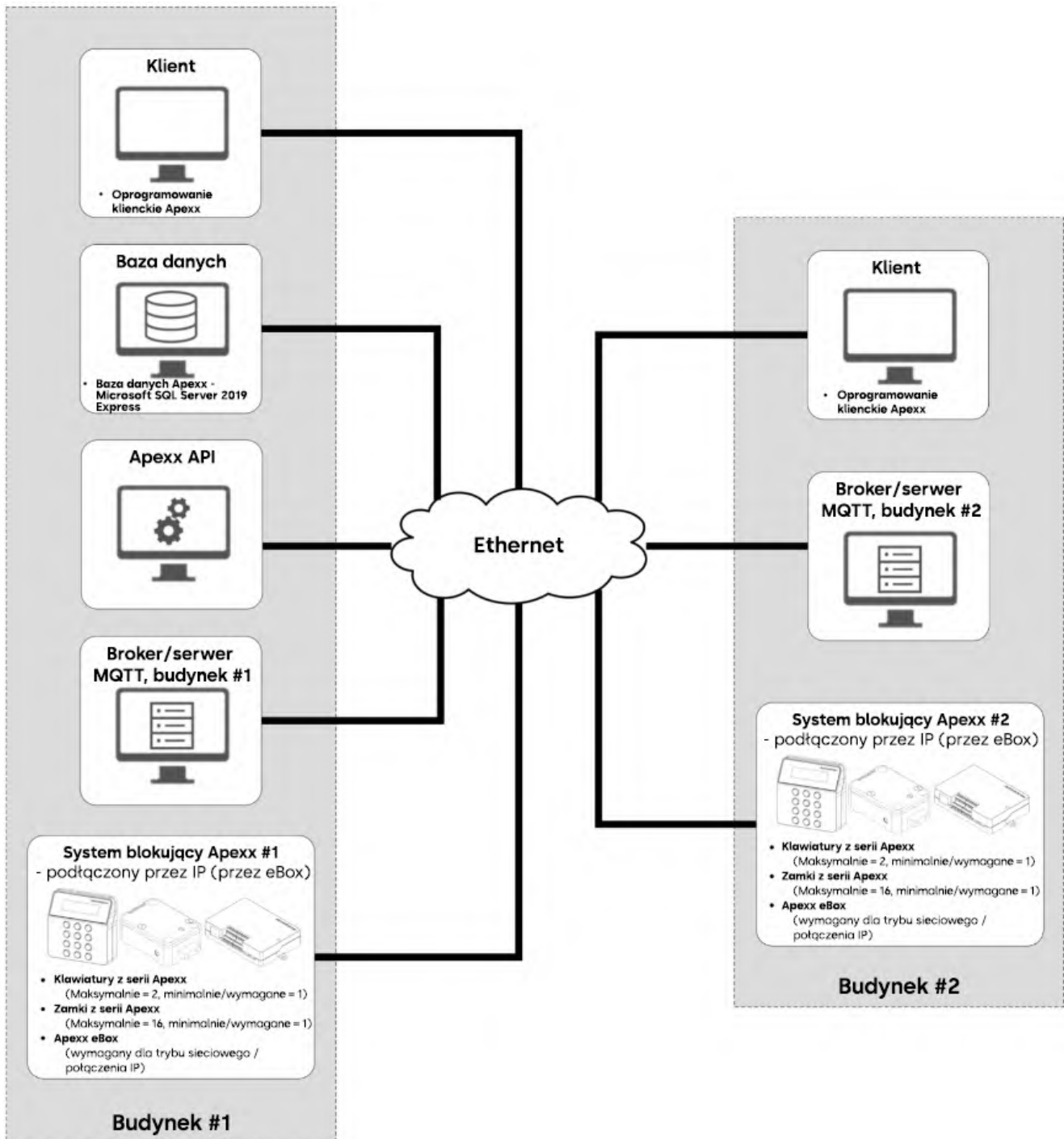


Rysunek 5 – Konfiguracja z wieloma komputerami i wieloma systemami blokującymi



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 łączy się z siecią za pośrednictwem Apexx eBox.

Koncepcja ta jest dalej rozwijana w systemie pokazanym na rysunku 6, który obejmuje wiele komputerów i systemów zamków rozmieszczonych w wielu budynkach.



Rysunek 6 – Konfiguracja wielu komputerów/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 Budynek #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 Apexx w całej sieci.

Ostatni przykład na rysunku 6 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

## Zalecane specyfikacje komputera Apexx

### Stacja robocza klienta Apexx

- Intel Core i7 – 4470 3,40 GHz z 4 rdzeniami
- 16 GB RAM 1600 MHz DDR3 NON-ECC
- Dysk twardy 500 GB
- Windows 10 Professional 64 bit
- AMD RADEON HD 8490 1 GB Dual Monitor lub AMD RADEON HD8570 1 GB Dual Monitor
- Porty USB 2.0
- Port Ethernet - karta sieciowa 1 Gb
- Klawiatura i mysz
- Kopia zapasowa UPS

### Apexx Broker Server

- Intel Xeon E5 – 2403, 1,80 GHz, 10 MB pamięci podręcznej
- 16 GB pamięci RAM 1333 MHz, RDIMM
- Dysk twardy 500 GB
- Windows 2019 Server Standard 64 bit
- Zintegrowana karta graficzna HD
- Port Ethernet – karta sieciowa 1 Gb
- Klawiatura i mysz
- Kopia zapasowa UPS

### Serwer bazy danych Apexx i interfejs API Apexx

- Intel Xeon E5 – 2420, 1,90 GHz, 15 MB pamięci podręcznej z 6 rdzeniami
- 32 GB pamięci RAM 1333 MHz, RDIMM
- 3,5-calowy dysk twardy 2 x 1 TB 7,2 tys. obr./min SATA 3 Gb/s
- Konfiguracja RAID 1
- Podwójny, redundantny zasilacz Hot-Plug
- Windows 2019 Server Standard 64 bit
- Zintegrowana karta graficzna HD
- Port Ethernet – karta sieciowa Gb
- Klawiatura i mysz
- Kopia zapasowa UPS

## Nasze zaangażowanie w zrównoważony rozwój

Jesteśmy zaangażowani we wspieranie 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. W celu ilościowego ujawnienia wpływu produktu na środowisko w całym jego cyklu życia, dormakaba dostarcza Deklaracje Środowiskowe Produktu (EPD), oparte na holistycznej ocenie cyklu życia.

[www.dormakaba.com/sustainability](http://www.dormakaba.com/sustainability)



## Nasza oferta

### Dostęp do rozwiązań automatyzacyjnych

Automatyka wejść  
Ochrona wejścia



### Rozwiązania kontroli dostępu

Elektroniczny dostęp i dane  
Systemy ewakuacji i ratownictwa  
Systemy zakwaterowania



### Dostęp do rozwiązań sprzętowych

Samozamykacze  
Sprzęt architektoniczny  
Mechaniczne systemy kluczy



### Usługi

Wsparcie techniczne  
Instalacja i uruchomienie  
Konserwacja i naprawa



### Rozwiązania dla kluczy i ścian

Kluczowe systemy  
Ściany ruchome/przesuwne



### Zamki sejfowe

Elektroniczne zamki sejfowe  
Mechaniczne zamki sejfowe  
Śruby i akcesoria



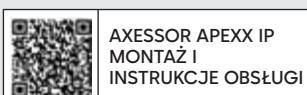
### Systemy szklane

Ręczne systemy drzwiowe  
Okucia do szkła  
Poziome ściany przesuwne



Architektura systemu Apexx, PL, 02/2024  
Zastrzega się możliwość wprowadzania zmian bez powiadomienia

**dormakaba USA Inc.**  
1525 Bull Lea Road, Suite 100  
Lexington, KY 40511  
[sales.safelocks.us@dormakaba.com](mailto:sales.safelocks.us@dormakaba.com)  
T +1 800 950 4744  
+1 888 950 4715 (pomoc techniczna)  
**dormakaba.com**



AXESSOR APEXX IP  
MONTAŻ I  
INSTRUKCJE OBSŁUGI

[dk.world/AxessorApexxIP](https://dk.world/AxessorApexxIP)