Select a Language

- **EN** - IT Security Guide
- **ES** - Guía de seguridad informática
- **DE** - IT-Sicherheitsleit-faden
- **IT** - Guida alla sicurezza informatica

dormakaba

Axessor Apexx
IT Security Guide

System Description

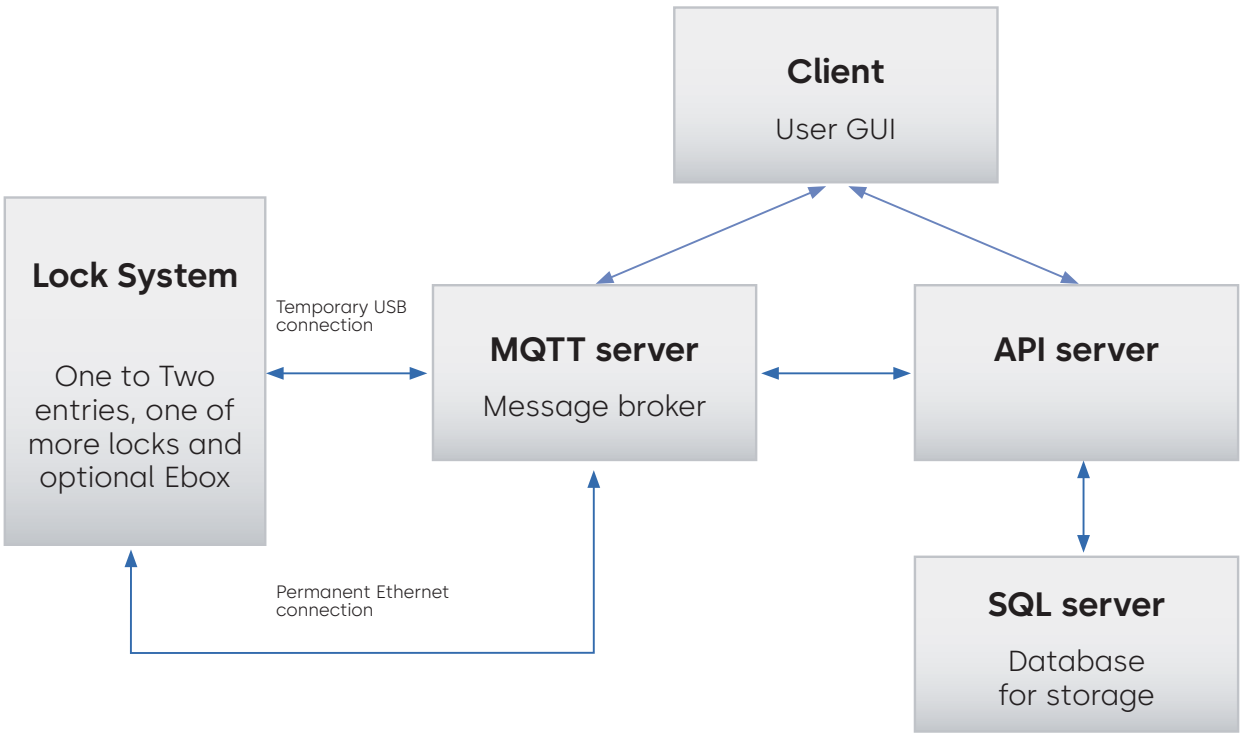
February 2024- EN

Axessor Apexx

System Descriptions

The Apexx solution consist of one or two Entries, one or more locks, up to one E-box and one instance of Apexx SW solution (Local Software). This document will focus on solutions containing E-box.

The general architecture of the solution is:



There are two possible connections between the lock system and the local SW. One is direct connection over USB to the entry. This connection must be enabled by an authorized user in the menu selection of the lock. The second connection is from the E-box over Ethernet to the local SW.

Local SW notes:

- All parts of the SW (MQTT, client and API) are designed as a Windows 10 applications. To be able to use them in cloud environment, one must be able to manage the communication channels between them.
- The communication channels are established during installation – These rely on DNS (or static IP addresses). Once the installation is completed, certificates will be established for the purpose of security. These certificates need to be properly managed to prevent any attack paths.

- The client supports multiple users but doesn't support multiuser simultaneously on single client. Only one person can be logged into a single client instance at any given moment.
- The communication to-and from the locking system is MQTT over SSL, so the standard ports need to be reachable.
- SW requires Windows certificates subsystem and an SQL19 database to run.

Pairing of local SW with E-box

The local SW and E-box need to be paired before a connection can be established.
When a brand-new e-box needs to be installed:

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

Disaster recovery:

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

Recover path will then be to re-install the API, MQTT and client either with fresh copy from dormakaba, or local backup. All data is at rest in the SQL database. API, MQTT and client don't store any data, only connection setting.

Key takeaways:

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

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

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 IT Security Guide, 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
T +1 800 950 4744
+1 888 950 4715 (tech support)
dormakaba.com

AXESSOR APEXX IP INSTALLATION AND OPERATION GUIDES

dk.world/AxessorApexxIP

dormakaba

Axessor Apexx
Guía de seguridad informática

Descripción del sistema

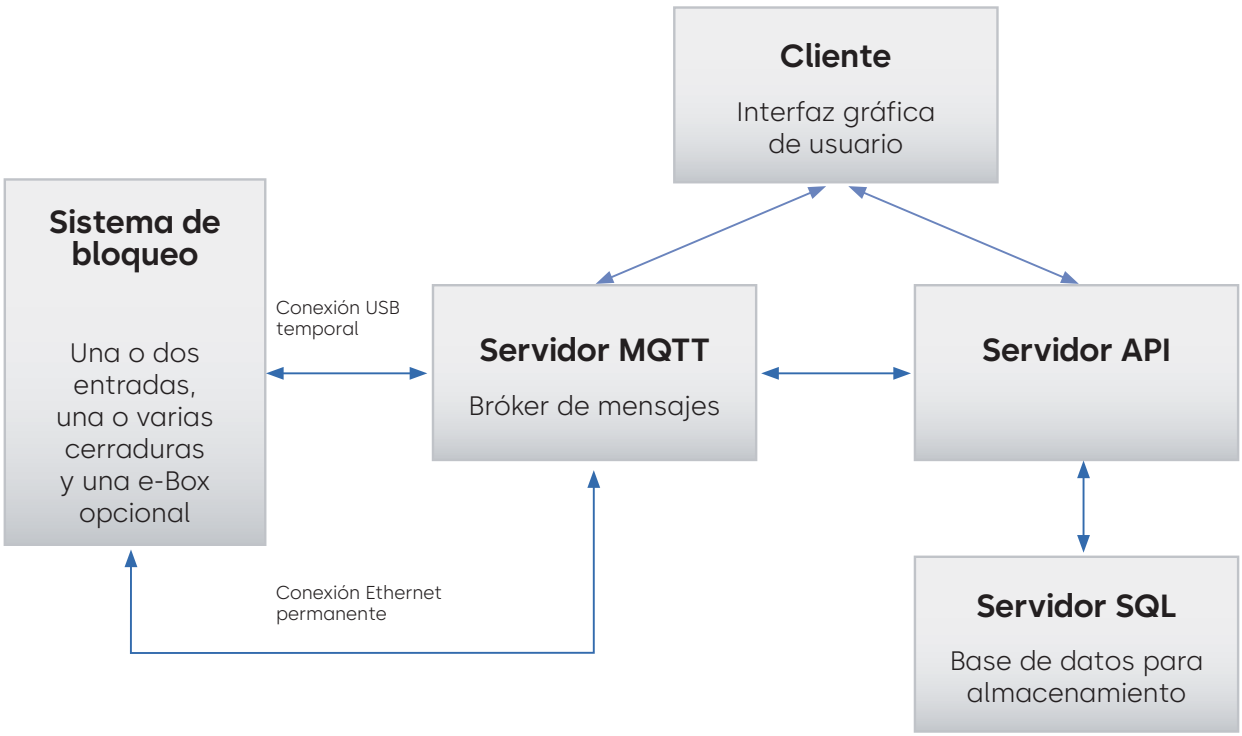
Febrero de 2024 - ES

Axessor Apexx

Descripción del sistema

La solución Apexx consiste en una o dos entradas, una o más cerraduras, hasta una e-Box y una instancia de la solución de software Apexx (software local). Este documento se centrará en las soluciones que contienen e-Box.

Arquitectura general de la solución



Hay dos posibilidades de conexión entre el sistema de bloqueo y el software local. Una es la conexión directa a la entrada por USB. Esta conexión debe ser habilitada por un usuario autorizado en el menú de selección de la cerradura. La segunda conexión va de la e-Box al software local a través de Ethernet.

Notas sobre el software local:

- Todos los elementos del software (MQTT, cliente y API) han sido diseñados como aplicaciones Windows 10. Para poder utilizarlos en un entorno de nube, hay que saber cómo gestionar los canales de comunicación entre ellos.
- Los canales de comunicación se establecen durante la instalación: se basan en DNS (o direcciones IP estáticas). Una vez finalizada la instalación, se establecerán certificados a efectos de seguridad. Estos certificados deben gestionarse adecuadamente para evitar cualquier vía de ataque.

- 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.
- La comunicación hacia y desde el sistema de bloqueo es MQTT sobre SSL, por lo que los puertos estándar deben estar accesibles.
- El software requiere el subsistema de certificados de Windows y una base de datos SQL19 para su uso.

Emparejamiento del software local con la e-Box

Para poder conectarse, primero hay que emparejar el software local y la e-Box. Si hay que instalar una e-Box nueva:

1) Instale físicamente la e-Box en el bus CAN.
2) Un usuario autorizado tiene que iniciar sesión en la entrada y habilitar la e-Box en el bus CAN (ningún dispositivo no autorizado puede monitorear el bus CAN).
3) Tras la habilitación de la e-Box, esta podrá obtener las claves de cifrado del bus CAN (AES-256 con claves específicas del sistema).
4) Una vez que la e-Box está en el bus CAN, hay que conectarla al software local. La e-Box verificará si se ha creado la configuración para el software local (a través del menú de configuración de la entrada). Si la configuración existe, se utilizará. De lo contrario, la e-Box utilizará DHCP para obtener la dirección IP.
5) Cuando haya una configuración Ethernet válida, la e-Box intentará conectarse al servidor MQTT en el software local (ya sea a través de comunicación IP directa basada en la configuración, o difusión en la red local en caso de DHCP). Esto se hace a través del TLS.
6) Si el software local detecta una nueva e-Box, esta debe autorizarse en el software antes de iniciar sesión utilizando el código de validación. Una vez que la e-Box esté autorizada en el software, el software emitirá un PIN de verificación que tendrá que ser validado en la entrada del sistema (verificación del software en la e-Box, y de la e-Box en el software).
7) Una vez verificado el sistema, se establecerá un canal seguro. Para ello, se utilizan certificados firmados de fábrica que han sido preinstalados (infraestructura PKI). Cualquier comunicación posterior se cifrará mediante TLS.

Recuperación en caso de catástrofe:

El software local se conecta a la base de datos SQL19 para el almacenamiento de datos (SQL19 Express de Microsoft - Referencia: https://www.microsoft.com/en-ca/sql-server/sql-server-2019-pricing).
La configuración de la base de datos debe introducirse en el software local en forma de archivo de configuración. El cifrado/protección y la recuperación de datos seguirán entonces la ruta de la base de datos SQL19. La base de datos debe ser gestionada por el departamento de TI local.

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

Principales conclusiones:

1) Los servidores con software local son los únicos que necesitan tener una dirección IP asignada, la e-Box no.

2) La comunicación entre la e-Box y el software local (tráfico a través de intranet/Internet) se cifra mediante TLS.

3) Incluya el servidor SQL en su plan de recuperación en caso de catástrofes. Esta base de datos es crucial para el funcionamiento del sistema.

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

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

Guía de seguridad informática de Apexx, ES, 02/2024
Sujeto a cambios sin previo aviso

dormakaba USA Inc.
1525 Bull Lea Road, Suite 100
Lexington, KY 40511
sales.safelocks.us@dormakaba.com
Tel: +1 800 950 4744
+1 888 950 4715 (Servicio técnico)
dormakaba.com

AXESSOR APEXX IP INSTALLATION AND OPERATION GUIDES

dk.world/AxessorApexxIP

dormakaba

Axessor Apexx IT-Sicherheitsleit-faden

Systembeschreibung

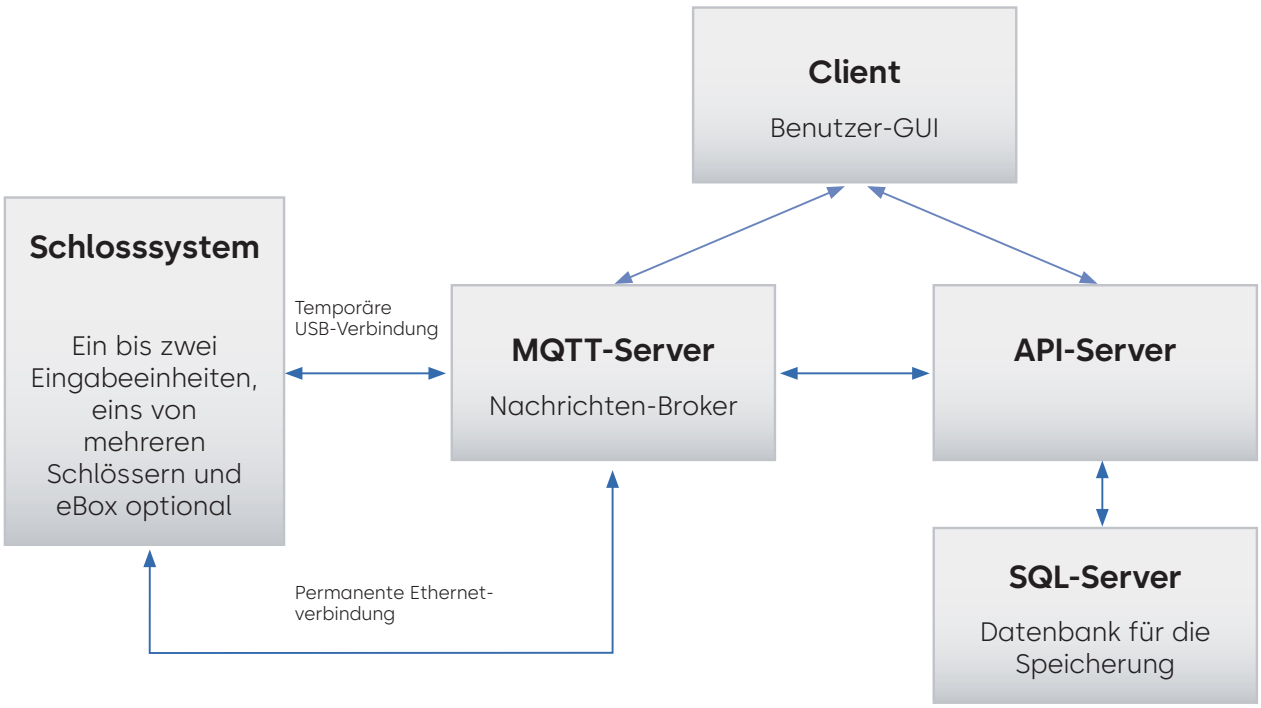
Februar 2024 – DE

Axessor Apexx

Systembeschreibungen

Die Apexx-Lösung besteht aus einer oder zwei Eingabeeinheiten, einem oder mehreren Schlössern, bis zu einer eBox und einer Instanz der Apexx-SW-Lösung (lokale Software). Dieses Dokument konzentriert sich auf Lösungen, die eine eBox enthalten.

Die allgemeine Architektur der Lösung sieht so aus:



Es gibt zwei mögliche Verbindungen zwischen dem Schlosssystem und der lokalen SW. Eine davon ist die direkte Verbindung über USB zur Eingabeeinheit. Diese Verbindung muss von einem berechtigten Benutzer in der Menüauswahl des Schlosses aktiviert werden. Die zweite Verbindung verläuft von der eBox über Ethernet zur lokalen SW.

Hinweise zur lokalen SW:

- Alle Teile der SW (MQTT, Client und API) sind als Windows 10-Anwendungen konzipiert. Um sie in einer Cloudumgebung nutzen zu können, muss man in der Lage sein, die Kommunikationskanäle zwischen ihnen zu verwalten.
- Die Kommunikationskanäle werden während der Installation eingerichtet. Diese basieren auf DNS (oder statischen IP-Adressen). Sobald die Installation abgeschlossen ist, werden aus Sicherheitsgründen Zertifikate eingerichtet. Diese Zertifikate müssen ordnungsgemäß verwaltet werden, um Angriffswege zu verhindern.

- Der Client unterstützt mehrere Benutzer, aber nicht gleichzeitig auf einem einzigen Client. Es kann zu jeder Zeit immer nur eine Person bei einer einzigen Client-Instanz angemeldet sein.
- Da die Kommunikation zur und von der Schließanlage über MQTT over SSL erfolgt, müssen die Standardports erreichbar sein.
- Die SW erfordert die Ausführung eines Windows-Zertifikatssubsystems und einer SQL19-Datenbank.

Kopplung der lokalen SW mit der eBox

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

1) Die eBox ist am CAN-Bus angeschlossen.
2) Ein berechtigter Benutzer muss sich bei der Eingabeeinheit anmelden und die eBox am CAN-Bus aktivieren (den CAN-Bus können keine nicht autorisierten Geräte überwachen).
3) Nach der Autorisierung der eBox kann die eBox die Verschlüsselungsschlüssel für den CAN-Bus abrufen (AES-256 mit systemspezifischen Schlüsseln).
4) Sobald die eBox am CAN-Bus angeschlossen ist, muss eine Verbindung zur lokalen SW hergestellt werden. Die eBox prüft, ob eine Einstellung für die lokale SW erstellt wurde (über das „Settings"-Menü der Eingabeeinheit). Wenn eine Einstellung vorhanden ist, wird sie verwendet. Andernfalls geht die eBox davon aus, dass DHCP zum Abrufen einer IP-Adresse verwendet wird.
5) Sobald eine gültige Etherneteinstellung vorhanden ist, versucht die eBox, sich mit dem MQTT-Server in der lokalen SW zu verbinden (entweder durch direkte IP-Kommunikation basierend auf den Einstellungen oder durch Broadcast im lokalen Netzwerk im Falle von DHCP). Dies erfolgt über TLS.
6) Wenn die lokale SW eine neue eBox erkennt, dann muss diese in der SW vor der erfolgreichen Anmeldung mit dem Anforderungscode autorisiert werden. Sobald die eBox in der SW autorisiert ist, erstellt die SW eine Verifizierungs-PIN, die in der Eingabeeinheit des Systems validiert werden muss (Verifizierung der SW gegenüber der eBox und der eBox gegenüber der SW).
7) Nachdem das System verifiziert wurde, wird ein sicherer Kanal eingerichtet. Dies erfolgt über vorinstallierte, werkseitig signierte Zertifikate (PKI-Infrastruktur). Jede weitere Kommunikation wird mit TLS verschlüsselt.

Notfallwiederherstellung:

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

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

Quintessenz:

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

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 Declarations, EPD) an, die auf ganzheitlichen Ökobilanzen basieren.

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 IT-Sicherheitsleitfaden, 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, USA
sales.safelocks.us@dormakaba.com
T +1 800 950 4744
dormakaba.com

AXESSOR APEXX IP INSTALLATION AND OPERATION GUIDES

dk.world/AxessorApexxIP

dormakaba

Axessor Apexx

Guida alla sicurezza informatica

Descrizione del sistema

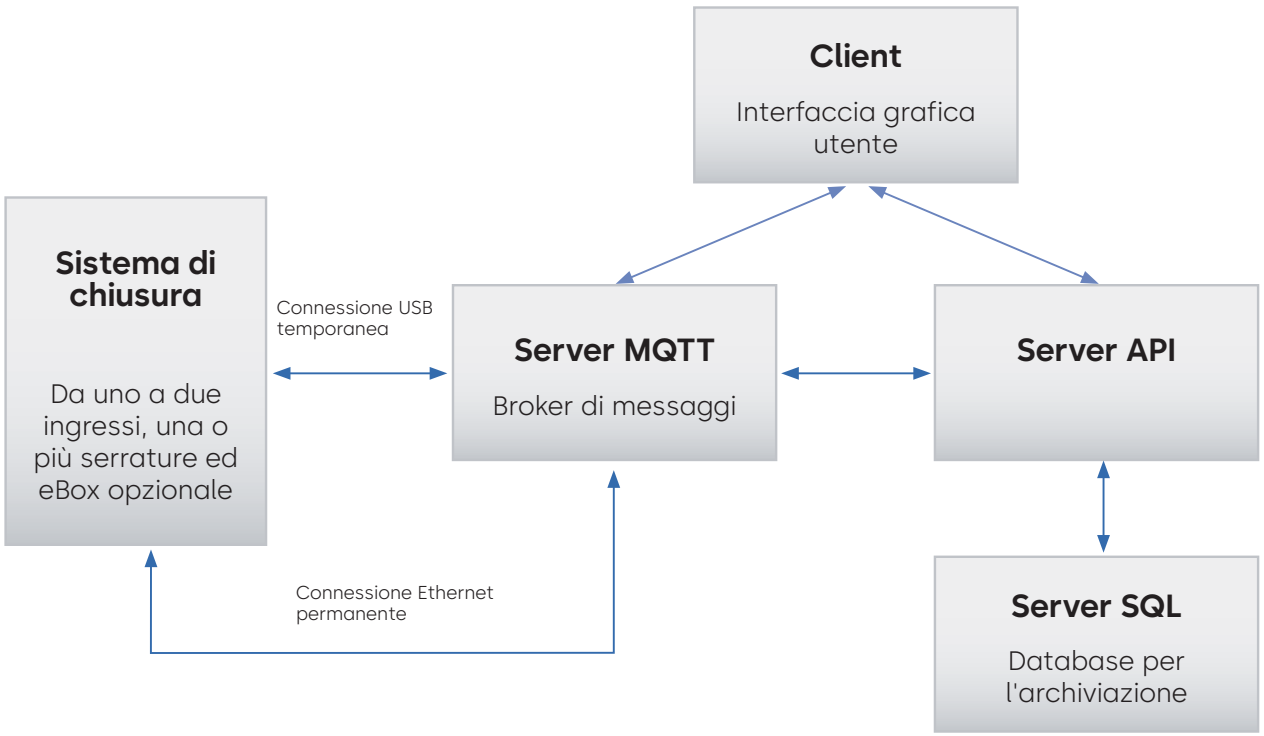
Febbraio 2024 - IT

Axessor Apexx

Descrizioni del sistema

La soluzione Apexx è composta da uno o due ingressi, una o più serrature, fino a una eBox e un'istanza della soluzione Apexx SW (Local Software). Questo documento si concentra sulle soluzioni con eBox.

L'architettura generale della soluzione è la seguente:



Esistono due possibili collegamenti tra il sistema di chiusura e il SW locale. Uno è il collegamento diretto via USB all'ingresso. Questa connessione deve essere abilitata da un utente autorizzato nel menu di selezione della serratura. La seconda connessione è dalla eBox via Ethernet al SW locale.

Note sul SW locale:

- Tutte le parti del SW (MQTT, client e API) sono progettate come applicazioni Windows 10. Per poterle utilizzare in un ambiente cloud, bisogna essere in grado di gestire i canali di comunicazione tra di essi.
- I canali di comunicazione vengono stabiliti durante l'installazione: si basano su DNS (o indirizzi IP statici). Una volta completata l'installazione, verranno creati dei certificati a scopo di sicurezza. Questi certificati devono essere gestiti in modo appropriato per evitare qualsiasi attacco.

- Il client supporta più utenti, ma non supporta la multiutenza simultanea su un singolo client. Una sola persona può accedere a una singola istanza del client in un dato momento.
- La comunicazione da e verso il sistema di chiusura avviene tramite MQTT su SSL, pertanto le porte standard devono essere raggiungibili.
- Per funzionare, il SW richiede il sottosistema dei certificati di Windows e un database SQL19.

Accoppiamento del SW locale con l'eBox

Il SW locale e la eBox devono essere accoppiati prima di poter stabilire una connessione. In caso di installazione di una nuova eBox:

1) La eBox è fisicamente installata sul CAN bus.
2) Un utente autorizzato deve accedere all'ingresso e abilitare la eBox sul CAN bus (nessun dispositivo non autorizzato può ascoltare il CAN bus).
3) Dopo l'autorizzazione della eBox, la eBox sarà in grado di ottenere le chiavi di crittografia del CAN bus (AES-256 con chiavi specifiche del sistema).
4) Una volta che la eBox è sul CAN bus, è necessario effettuare il collegamento con il SW locale. L'eBox verificherà se è stata creata un'impostazione per il SW locale (attraverso il menu impostazioni dell'ingresso). Se esiste un'impostazione, verrà utilizzata. Altrimenti, la eBox assumerà il protocollo DHCP per ottenere l'indirizzo IP.
5) Se le impostazioni Ethernet sono valide, l'eBox tenterà di connettersi al server MQTT nel SW locale (tramite comunicazione IP diretta in base alle impostazioni, oppure tramite broadcast sulla rete locale in caso di DHCP). Questo avviene tramite TLS.
6) Se il SW locale rileva una nuova eBox, è necessario autorizzarla nel SW prima di effettuare il login con il codice di riscatto. Una volta che la eBox è stata autorizzata dal SW, quest'ultimo produrrà un PIN di verifica che dovrà essere convalidato all'ingresso del sistema (verifica del SW alla eBox e della eBox al SW).
7) Dopo la verifica del sistema, viene stabilito un canale sicuro. A tal fine si utilizzano certificati firmati in fabbrica preinstallati (infrastruttura PKI). Tutte le comunicazioni successive sono crittografate con TLS.

Ripristino in caso di catastrofe:

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

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

Punti salienti:

1) Solo i server con SW locale devono essere indirizzabili via IP, non l'eBox.
2) La comunicazione tra la eBox e il SW locale (traffico su intranet/Internet) è criptata con TLS.
3) Includere il server SQL nel piano di disaster recovery. Questo database è fondamentale per il funzionamento del sistema.

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

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 di sicurezza

Serrature elettroniche per casseforti
Serrature meccaniche per casseforti
Catenacci e accessori

Sistemi in vetro

Sistemi di porte manuali
Guarnizioni in vetro
Pareti scorrevoli orizzontali

Guida alla sicurezza informatica di 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
T +1 800 950 4744
+1 888 950 4715 (assistenza tecnica)
dormakaba.com

AXESSOR APEXX IP INSTALLATION AND OPERATION GUIDES

dk.world/AxessorApexxIP