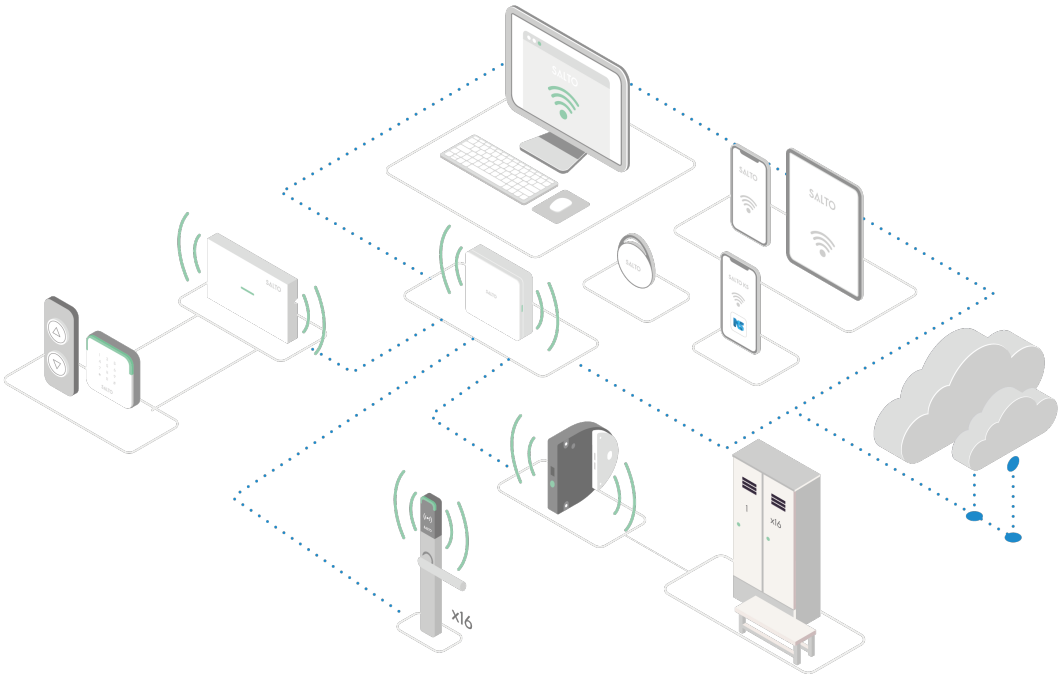
Platform security architecture

The diagram below is an overview of a Salto KS technology platform system and its individual components.

This document provides an overview of security standards and practice as they relate to each component of Salto KS.



1. DIGITAK KEY

Salto KS uses a PKI (Public Key Infrastructure) to transfer keys. Our public key infrastructure forms the foundation for everything that is needed to manage Digital Keys and their encryption such as policies, hardware, software and procedures. Mobile phones hold a private key and communicate a public key. The only one who can decrypt the public key is the one with the private key, this is called ‘Asymmetric Encryption’.

This means your mobile device is the only device that can decrypt your digital key, and the digital key is always transmitted in the encrypted form when the Digital Key is sent to the lock. We regularly perform security tests to ensure that the entire Digital Key process remains secure, from generation to transferring it to the lock.

2. PIN CODE

This keyless entry method provides a high level of security as well as convenience. The fixed pin code is generated through the KS app and it’s unique for every single user. We generate the PIN by using strong hashing algorithms. The value we choose to use for hashing generates an almost-unique value and is one of the strongest hash functions available and has never been compromised.

The PIN is displayed to the user once, after that it can no longer be retrieved by anyone, not even Salto KS. If the user forgets their PIN a new one will have to be generated.

3. SMART KEY TAG CREDENTIAL

A Tag is a physical device (contactless key fob) that works based on RFID (Radio-frequency identification). Our tag contains no batteries and features a sturdy and robust design to ensure you never have to worry about their physical durability.

The Tag contains electronically stored information which is secured with MIFARE® DESFire EV2 which makes copying or hacking transponders implausible. We perform regular security testing to ensure that our tags remain secured against common attacks such as credential copying.

4. IQ

The IQ is the central hub a.k.a. the 'brain' of your Salto KS system. It receives all changes and settings from the Salto KS application and ensures that all Locks are updated within seconds. The maximum distance from the IQ to the electronic smart lock is 10 metres.

All remote commands that are influencing direct communications between the IQ and Hardware are secured with an OTP (One Time Password). These commands will be adhering to the same end-to-end encryption as the Digital Key feature.

5. ZIGBEE COMMUNICATIONS

ZigBee is mainly used for two-way communication between a sensor and a control system. ZigBee is a short-range communication and offers connectivity up to 100 meters similar to Bluetooth and Wi-Fi.

Adopted on top of ZigBee is an encryption protocol that ensures any communication between the IQ and other hardware remains secure. After a new lock has connected to an IQ for the first time it will store an encrypted parameter which will prevent connections to any other device than the paired IQ.

6. BLUETOOTH SMART LOCKS

Bluetooth Low Energy is designed to cater to lower power consumption than regular Bluetooth. BLE offers several features for securing communication between devices. When the IQ initiates the connection with the lock a pairing process begins where the two devices exchange necessary information to build the encrypted connection. After the pairing process is completed, the lock will be prevented from forming a connection with any other device than the paired IQ.

Each BLE device is identified using a device address. These addresses are similar to the MAC addresses used in other communications protocols. Since BLE enabled locks use cryptographic keys to unlock they are highly secure.

7. IQ - CLOUD

The IQ connects the wireless Locks to the cloud with either:

- Global cellular connection (via USB)
- Wi-Fi
- Ethernet cable (PoE compatible versions available)

The default communication between the IQ and the KS Core API is secured and enforced with strong encryption protocols.

The communication between the IQ and KS backend is authenticated based on the x509 certificate (a standard that determines public key certificate arrangements).

All data travelling within this TLS tunnel is encrypted. In fact, there is no data travelling outside this tunnel. In the absence of certification, it is not possible to impersonate either the IQ or the KS Core API. In other words, it becomes improbable to perform MITM (man-in-the-middle) attacks. During our external security audits, the communication security is always evaluated to ensure we stay up to date and always use industry standards

8. CLOUD > WEB, MOBILE, REMOTE OPENING

The Salto KS mobile app and web interface allows you to manage access to your locations from anywhere. All the hardware is managed via an app/ web interface. This can either be a custom integration, where you can enjoy your own user interface, or a ready built solution like Salto KS. We use industry best practises to ensure the sign in process for our apps is secure, including multi-factor authentication and session management capabilities.