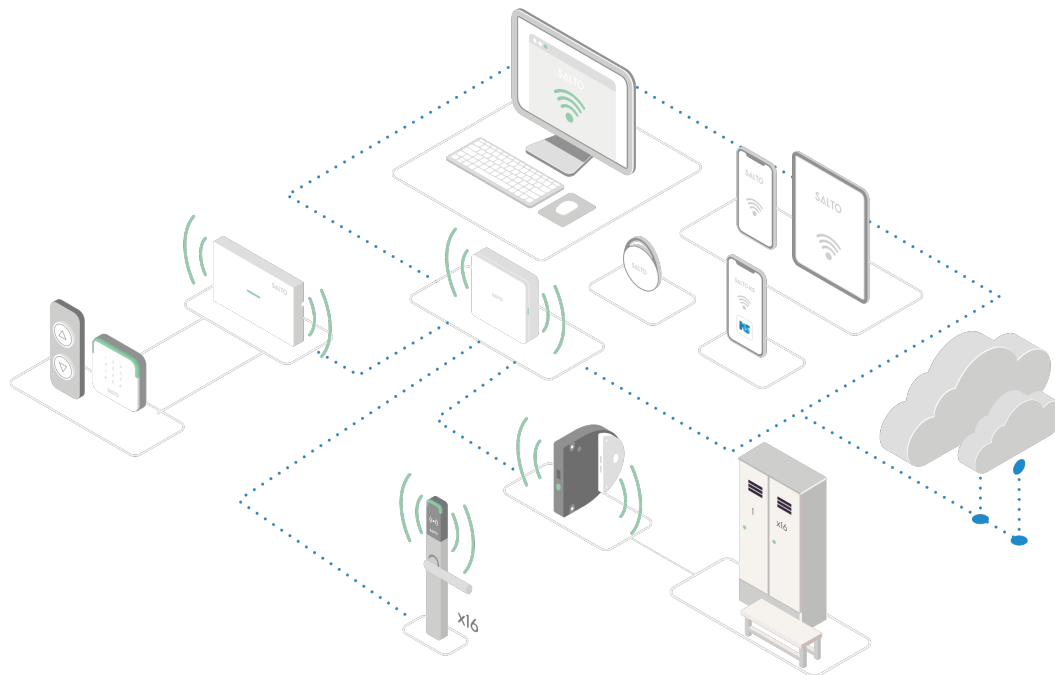


Plattform-Sicherheitsarchitektur

Das folgende Diagramm gibt einen Überblick über den Systemaufbau und die einzelnen Komponenten in einer Salto KS Anlage.

Diese Seite schafft Übersicht über die Sicherheitsstandards und -praktiken in Bezug auf jede Komponente von Salto KS.



1. DIGITALE SCHLÜSSEL

Salto KS verwendet eine PKI (Public Key Infrastructure) zur Übertragung von Schlüsseln. Unsere Public Key Infrastructure bildet die Grundlage für alles, was zur Verwaltung digitaler Schlüssel und deren Verschlüsselung benötigt wird, wie z. B. Sicherheitsrichtlinien, Hardware, Software und Prozesse. Mobilgeräte speichern einen privaten Schlüssel und kommunizieren einen öffentlichen Schlüssel. Der Einzige, der den öffentlichen Schlüssel entschlüsseln kann, ist derjenige, der über den privaten Schlüssel verfügt. Dies wird als „asymmetrische Verschlüsselung“ bezeichnet.

Das bedeutet, dass Ihr Mobilgerät das einzige Gerät ist, das Ihren digitalen Schlüssel dechiffrieren kann, wobei der digitale Schlüssel immer in codierter Form übertragen wird, wenn er an das Schließgerät gesendet wird. Wir führen regelmäßig Sicherheitstests durch, um sicherzustellen, dass der gesamte Prozess des digitalen Schlüssels umfassend geschützt bleibt, von der Generierung bis zur Übertragung an das Schließgerät.

2. PIN-CODE

Diese schlüssellose Zutrittsmethode bietet ein hohes Maß an Sicherheit und Komfort. Der feste PIN-Code wird über die KS-App generiert und ist für jeden Benutzer einzigartig. Wir generieren die PIN mithilfe starker Hashing-

Algorithmen. Der Wert, den wir für das Hashing verwenden, erzeugt einen eindeutigen Wert und ist eine der stärksten und bisher nie kompromittierten Hash-Funktionen.

Die PIN wird dem Benutzer einmalig angezeigt und kann danach von niemandem mehr abgerufen werden, auch nicht vom Salto KS System. Wenn der Benutzer seine PIN vergisst, muss eine neue generiert werden.

3. SMARTE AUSWEISMEDIEN / SMART TAGS

Ein Smart Tag ist ein physisches Medium (kontaktloser Schlüsselanhänger), das auf RFID (Radiofrequenz-Identifikation) basiert. Unsere Tags enthalten keine Batterien und verfügen über ein stabiles und robustes Design, damit die physische Haltbarkeit gewährleistet ist.

Der Tag enthält digital gespeicherte Daten, die mittels MIFARE® DESFire EV2 geschützt sind, wodurch das Kopieren oder Hacken von Transpondern sehr unwahrscheinlich ist. Wir führen regelmäßige Sicherheitstests durch, um dafür zu sorgen, dass unsere Tags gegen übliche Angriffe (wie etwa das Kopieren von Zutrittsausweisen) geschützt bleiben.

4. IQ

Der IQ fungiert als zentraler Hub, auch bekannt als das „Gehirn“ des Salto KS Systems. Er übernimmt alle Aktualisierungen und Konfigurationen von der Salto KS-Anwendung und stellt sicher, dass alle elektronischen Schließgeräte innerhalb von Sekunden aktualisiert werden. Die maximale Entfernung zwischen dem IQ und der Türhardware beträgt 10 Meter.

Alle Steuerbefehle, die die direkte Kommunikation zwischen IQ und Hardware beeinflussen, sind mit einem OTP (One Time Password) abgesichert. Diese Steuerung erfolgt mit derselben End-to-End-Verschlüsselung wie bei der Digital-Key-Funktion.

5. ZIGBEE-VERNETZUNG

ZigBee wird hauptsächlich für die Zwei-Wege-Kommunikation zwischen einem Sensor und einem Steuerungssystem verwendet. ZigBee ermöglicht eine Kommunikation über kurze Distanzen und bietet eine Reichweite von bis zu 100 Metern, ähnlich wie Bluetooth und WLAN.

Auf ZigBee wurde ein Verschlüsselungsprotokoll aufgesetzt, das die Sicherheit der Kommunikation zwischen dem IQ und anderer Hardware garantiert. Nachdem ein neues Schließgerät zum ersten Mal mit einem IQ verbunden wurde, speichert es einen verschlüsselten Parameter, der Verbindungen zu anderen Geräten als dem mit ihm gekoppelten IQ verhindert.

6. BLUETOOTH-GERÄTE

Bluetooth Low Energy ist so konzipiert, dass es einen geringeren Stromverbrauch als reguläres Bluetooth aufweist. BLE bietet diverse Funktionen zur Sicherung der Kommunikation zwischen Endgeräten. Wenn der IQ die Verbindung mit dem Schließgerät herstellt, beginnt ein Kopplungsprozess, bei dem die beiden Geräte die erforderlichen Informationen austauschen, um die verschlüsselte Verbindung aufzubauen. Nach Abschluss des Kopplungsprozesses wird sichergestellt, dass das Schließgerät keine Verbindung zu einem anderen Gerät als dem

gekoppelten IQ herstellen kann.

Jedes BLE-Gerät wird anhand einer Geräteadresse identifiziert. Diese Adressen ähneln den in anderen Kommunikationsprotokollen verwendeten MAC-Adressen. Da BLE-fähige Schließgeräte zum Decodieren von Verschlüsselungscodes verwenden, bieten sie ein hohes Maß an Sicherheit.

7. IQ – CLOUD

Der IQ verbindet die kabellose Türhardware mit der Cloud, entweder über:

- › Mobilfunkverbindung (via USB)
- › WLAN
- › Ethernet-Verkabelung (PoE-kompatible Versionen verfügbar)

Die standardmäßige Kommunikation zwischen der IQ und der KS Core API erfolgt gesichert über starke Verschlüsselungsprotokolle. Die Kommunikation zwischen dem IQ und dem KS Backend wird auf der Grundlage des x509-Zertifikats authentifiziert (ein Standard, der die Anforderungen an Public-Key-Zertifikate festlegt).

Alle Daten, die innerhalb dieses TLS-Tunnels übertragen werden, sind verschlüsselt. Außerhalb dieses Tunnels werden keine Daten übertragen. Ohne Zertifizierung ist es nicht möglich, sich als IQ oder KS Core API auszugeben. Mit anderen Worten: Es ist unwahrscheinlich, dass MITM-Angriffe (Man-in-the-Middle) durchgeführt werden können. Bei unseren externen Sicherheitsprüfungen wird die Kommunikationssicherheit kontinuierlich evaluiert, um sicherzustellen, dass wir auf dem neuesten Stand bleiben und stets branchenübliche Standards befolgen.

8. CLOUD – INTERNET, MOBILE, FERNÖFFNUNG

Mit der mobilen App sowie der Web-Oberfläche von Salto KS können Sie den Zutritt zu Ihren Standorten von überall aus verwalten. Die gesamte Hardware wird über eine App/Web-Oberfläche verwaltet. Dies kann entweder über eine benutzerdefinierte Integration erfolgen, bei der Sie Ihre eigene Benutzeroberfläche nutzen können, oder über eine fertige Lösung wie Salto KS. Wir verwenden branchenübliche Best Practices, um sicherzustellen, dass der Anmeldevorgang bei unseren Apps bestens abgesichert ist, einschließlich Multi-Faktor-Authentifizierung und Session-Management-Funktionen.

Disclaimer:

This is a downloadable version of the website content that we make available to you for informative purposes for an easier consultation and filling. However, SALTO assumes no responsibility for any errors or typos that the downloadable version may contain.

As SALTO reserves the right to modify this content from time to time, please check on the Legal section of our website to find the latest version of the legal documents and their updates.