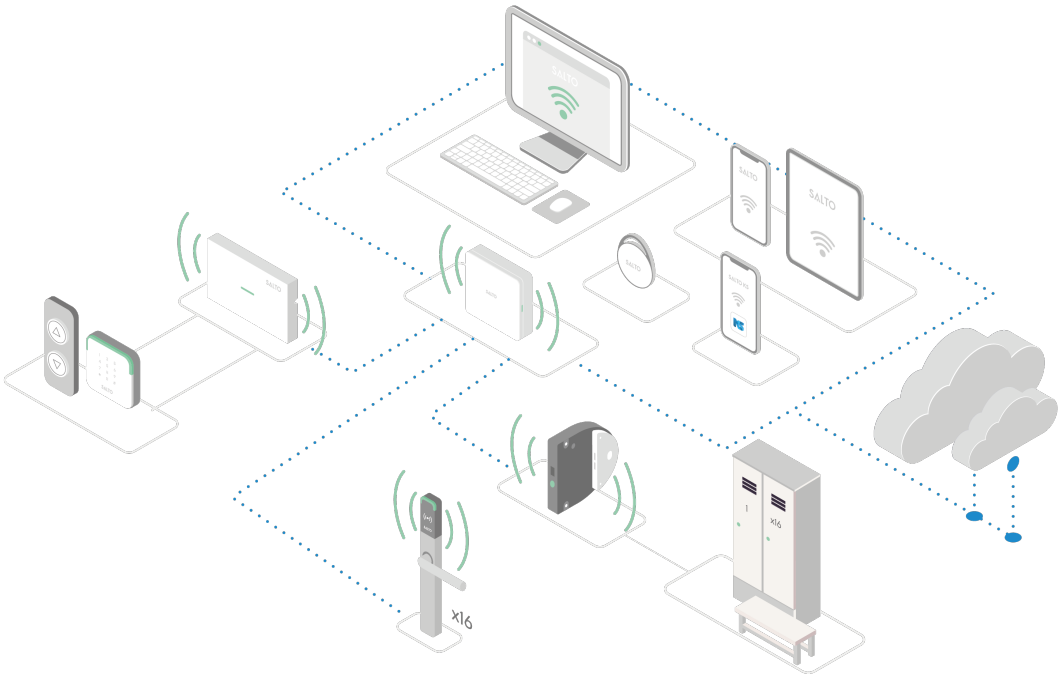
Architecture de sécurité de la plateforme

Le schéma ci-dessous donne un aperçu d'une plateforme technologique Salto KS et de ses composants individuels.

Ce document donne un aperçu des normes et pratiques de sécurité applicables à chaque composant de Salto KS.



1. CLÉ DIGITALE

Salto KS utilise une PKI (Public Key Infrastructure, architecture à clés publiques) pour transférer des clés. Notre infrastructure à clés publiques forme la base de tout ce qui est nécessaire pour gérer les clés digitales et leur cryptage, comme les politiques, le matériel, les logiciels et les procédures. Les téléphones portables contiennent une clé privée et communiquent une clé publique. Seule la clé privée peut déchiffrer la clé publique, c'est ce qu'on appelle le « cryptage asymétrique ».

Cela signifie que votre appareil mobile est le seul appareil capable de déchiffrer votre clé digitale, et que la clé digitale est toujours transmise sous forme cryptée lorsque la clé digitale est envoyée à la serrure. Nous effectuons régulièrement des tests de sécurité pour vérifier que l'ensemble du processus de clés digitales reste sécurisé, de la génération de la clé à son transfert à la serrure.

2. CODE PIN

Cette méthode d'entrée sans clé offre un haut niveau de sécurité et de commodité. Le code PIN fixe est généré via l'application KS et est unique pour chaque usager. Nous générons le code PIN en utilisant des algorithmes de hachage puissants. La valeur que nous choisissons d'utiliser pour le hachage génère une valeur presque unique, est l'une des fonctions de hachage les plus puissantes disponibles et n'a jamais été compromise.

Le code PIN est montré une seule fois à l'usager, après quoi il ne peut plus être récupéré par personne, pas même Salto KS. Si l'usager oublie son code PIN, un nouveau code devra être généré.

3. INFORMATIONS D'IDENTIFICATION DU TAG INTELLIGENT

Un Tag est un dispositif physique (clé électronique sans contact) basée sur la RFID (identification par radiofréquence). Notre tag ne contient aucune pile et présente un design robuste, gage de durabilité.

Le tag contient des informations stockées électroniquement qui sont sécurisées par une puce MIFARE® DESFire EV2, ce qui limite le risque de copie ou de piratage de transpondeurs. Nous effectuons régulièrement des tests de sécurité pour nous assurer que nos tags restent protégés contre les attaques courantes telles que la copie d'identifiants.

4. IQ

L'IQ est le hub central, c'est-à-dire le « cerveau » du système Salto KS. Il reçoit toutes les modifications et tous les paramètres de l'application Salto KS et s'assure que toutes les serrures sont mises à jour en quelques secondes. La distance maximale entre l'IQ et la serrure électronique intelligente est de 10 mètres.

Toutes les commandes à distance qui influencent les communications directes entre l'IQ et le matériel sont sécurisées avec un mot de passe à usage unique (OTP). Ces commandes auront le même cryptage de bout en bout que la fonction Clé Digitale.

5. COMMUNICATIONS ZIGBEE

ZigBee est utilisé principalement pour la communication bidirectionnelle entre un capteur et un système de commande. ZigBee est un protocole de communication à courte portée qui offre une connectivité jusqu'à 100 mètres, similaire au Bluetooth et au Wi-Fi.

En plus du ZigBee, un protocole de cryptage garantit la sécurité de toute communication entre l'IQ et d'autres matériels. Une fois qu'une nouvelle serrure s'est connectée à un IQ pour la première fois, il stockera un paramètre crypté qui empêchera les connexions à tout autre appareil que l'IQ appairé.

6. SERRURES INTELLIGENTES BLUETOOTH

Le Bluetooth à basse consommation permet d'obtenir une consommation d'énergie inférieure à celle du Bluetooth classique. Le BLE offre plusieurs fonctionnalités pour sécuriser la communication entre les appareils. Lorsque l'IQ initie la connexion avec la serrure, un processus d'appariement commence lorsque les deux dispositifs échangent les informations nécessaires pour établir la connexion cryptée. Une fois le processus d'appariement terminé, la serrure ne pourra pas établir de connexion avec un appareil autre que l'IQ appairé.

Chaque appareil BLE est identifié à l'aide d'une adresse d'appareil. Ces adresses sont similaires aux adresses MAC utilisées dans d'autres protocoles de communication. Étant donné que les serrures BLE utilisent des clés de cryptage pour le déverrouillage, elles sont hautement sécurisées.

7. IQ - CLOUD

L'IQ connecte les serrures radio-fréquence au cloud avec :

- Connectivité cellulaire globale (par USB)
- Wi-Fi
- Câble Ethernet (versions compatibles PoE disponibles)

La communication par défaut entre l'IQ et l'API KS Core est sécurisée par des protocoles de cryptage robustes. La communication entre l'IQ et le backend KS est authentifiée avec le certificat x509 (une norme spécifiant les formats pour les certificats à clé publique).

Toutes les données qui transitent dans ce tunnel TLS sont cryptées. Aucune donnée ne se déplace en dehors de ce tunnel. En l'absence de certification, il n'est pas possible de se faire passer pour l'IQ ou l'API KS Core. En d'autres termes, les attaques MITM (homme du milieu) deviennent improbables. Au cours de nos audits de sécurité externes, la sécurité de la communication est toujours évaluée pour nous assurer que nous restons à jour et utilisons toujours les normes de l'industrie

8. CLOUD > WEB, MOBILE, OUVERTURE À DISTANCE

L'application mobile et l'interface web Salto KS permettent de gérer l'accès aux emplacements de n'importe où. Tout le matériel est géré via une application/interface Web. Il peut s'agir d'une intégration personnalisée, où vous pouvez profiter de votre propre interface usager, ou d'une solution prête à l'emploi comme Salto KS. Nous utilisons les bonnes pratiques de l'industrie pour nous assurer que le processus de connexion à nos applications est sécurisé, y compris l'authentification multi-facteurs et des capacités de gestion de session.

Clause de non-responsabilité:

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.

Part of the content of this document may have been generated or assisted by artificial intelligence tools. This document may also include automatic or manual translations provided exclusively for informational purposes, which may contain errors or inaccuracies. Salto does not guarantee the accuracy, quality, or reliability of such content or translations, including those generated by AI.

The User is responsible for verifying the information contained in this document and, in case of doubt, must refer to the original English version, which shall prevail in the event of any discrepancy. Other language versions are provided for informational purposes only.

Although Salto makes reasonable efforts to review the content of its downloadable documents, they may contain errors or omissions. Salto assumes no liability arising from the User's use, interpretation, or decisions made based on the information contained in this document, which is used at the User's sole responsibility.

For more detailed information on the use of artificial intelligence, translations, and applicable limitations of liability, please refer to the "Terms of Use of our Website".

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.