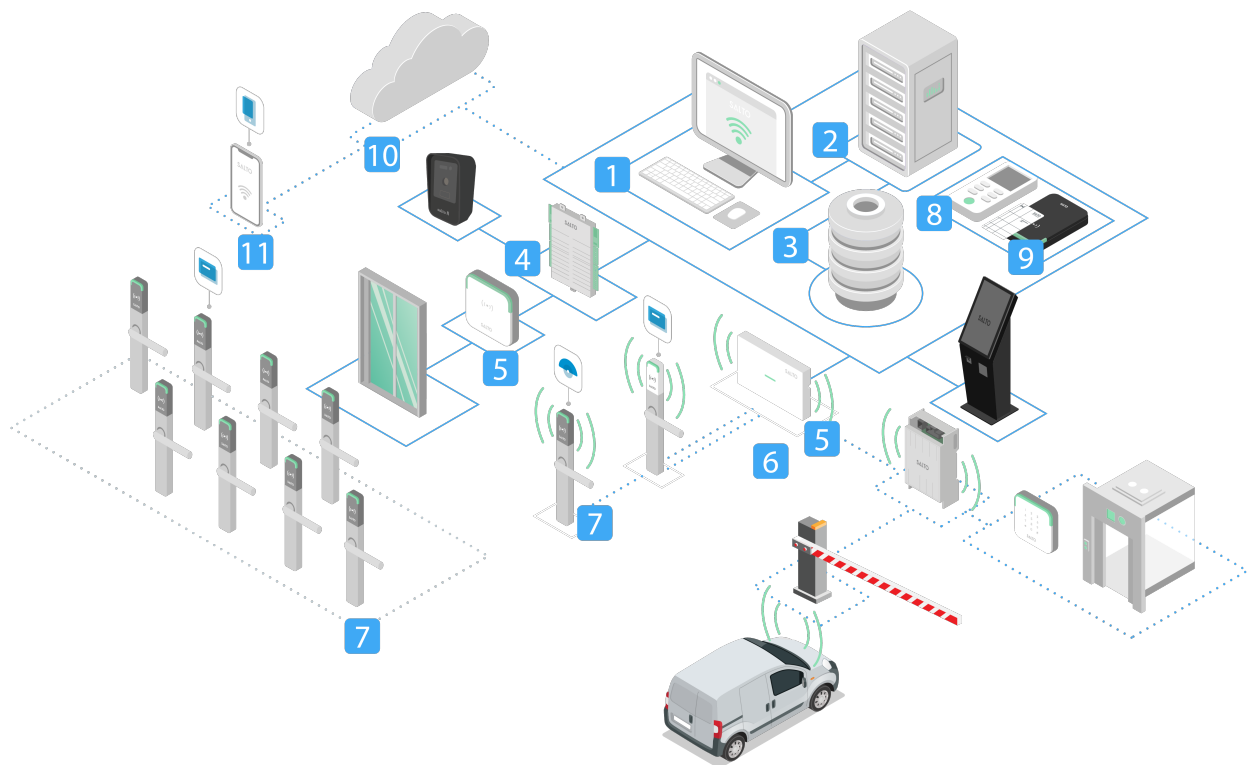


Säkerhetsarkitektur för plattformen

Diagrammet nedan är en översikt över ett Salto Space – Data-on-Card – lokalt teknikplattformssystem och dess enskilda komponenter.

Denna sida ger en översikt över säkerhetsstandarder och praxis som de relaterar till varje komponent i Salto Space.



1. SALTO SPACE FRONT-END OCH SPACE BACK-END

Salto Space är en HTTPS TLS webbapplikation och kommunikationen mellan Salto Service och användarwebbläsare är JSON-RPC.

Operatörer måste ange ett giltigt användarnamn och lösenord för att logga in i front-end-applikationen. Beroende på den valda konfigurationen valideras dessa autentiseringsuppgifter mot antingen Salto-databasen eller en katalogtjänst via LDAP.

Lösenord lagras med hjälp av starka kryptoalgoritmer i databasen.

2. SALTO SPACE BACK-END OCH SQL-DATABAS

Kommunikationen mellan databasen och Salto-tjänsten säkras med hjälp av ett TLS-protokoll.

3. SQL-DATABAS

Detta finns på en säker plats i kundens datacenter (databasen är hostad hos kunden). Logisk åtkomst till databasen hanteras genom autentisering med användarnamn och lösenord. Denna autentisering kan ske i SQL-läge eller Windows-läge, beroende på konfigurationen under databassättningsprocessen.

Känsliga uppgifter som användaruppgifter och kryptonycklar krypteras.

Åtkomst till databasen sker endast via Salto Space Service. Användare kan inte komma åt databasen direkt.

4. SALTO SPACE BACK-END OCH STYRENHET/GATEWAY

Kommunikationen mellan Salto-tjänsten och Salto-åtkomstkontrollenheterna eller gateways sker via Ethernet och denna kommunikation skyddas av ett säkert nätverksprotokoll baserat på UDP-datagram. Båda parter autentiseras ömsesidigt och använder starka krypteringsalgoritmer. De använda kryptonycklarna är krypterade och lagras säkert.

Det finns en autentiseringsprocess mellan Salto-tjänsten och Salto-åtkomstkontrollenheten eller gateways för att dela en gemensam sessionsnyckel, vilket skyddar kommunikationen.

5. STYRENHET OCH VÄGGLÄSARE SAMT GATEWAY OCH NOD

Trådbunden kommunikation mellan Salto* gateways och noder är baserad på RS485 fysisk kommunikation och skyddas med ett starkt säkerhetsprotokoll. Denna kommunikation använder starka krypteringsalgoritmer. Använda kryptonycklar krypteras och lagras säkert.

* Styrenhet, väggläsare och gateways och nod är.

6. NOD/INTERN NOD OCH DÖRRLÅS. DIREKT ELLER GENOM EN REPEATER

. Salto RFnet: I det IEEE 802.15.4-baserade RF-kommunikationsprotokollet som Salto använder autentiseras och krypteras alla strängar som innehåller applikationsdata genom ett säkert läge med starka krypteringsalgoritmer. De använda kryptonycklarna är krypterade och lagras säkert.

. BLUEnet: Denna kommunikation är baserad på BLE kommunikationsprotokoll, som använder en frekvenshoppmekanism för kommunikation med dörrar. Dataramar autentiseras och krypteras genom ett säkert läge med hjälp av starka krypteringsalgoritmer. Använda kryptonycklar krypteras och lagras på ett säkert sätt.

7. KORT- OCH VÄGGLÄSARE/ELEKTRONISKA LÅS

Säkerheten relaterad till hur kort läses och hur information skyddas beror på kortet som används, det vill säga själva kortets teknik: MIFARE DESFire EV2, HID iClass etc., så att krypteringsmekanismen baseras på kortets teknik: AES, DES, 3DES, Crypto1, etc.

Korten skyddas av Saltos säkerhetsnycklar. Dessa säkerhetsnycklar överförs till kort när applikationen skapas (utfärdas) av en SALTO-säker enhet: NCoder och/eller väggläsare.

Vidare erbjuder Salto olika typer av användarautentiseringsprocesser som kan kombineras

(dubbelfaktorautentisering) för att öka säkerheten för en installation: kort + PIN, kort + biometri eller PIN + biometri.

8. ÅTKOMSTPUNKTER OCH BÄRBAR PROGRAMMERINGSENHET

Säkerhetsnycklar krypteras och överförs till Saltos åtkomstpunkter av Salto Portable Programming Device (PPD). En PPD autentiseras av Salto-åtkomstpunkten genom starka krypteringsalgoritmer.

9. SALTO SPACE BACK-END OCH NCODER

Kommunikationen mellan Salto Space Service och en Salto NCoder skyddas av ett säkert krypteringsprotokoll.

10. JUSTIN MOBILE – DIGITALA NYCKLAR

Kommunikation till Salto JustIN Mobile-molnet från Salto ProAccess Space management access control software eller från JustIN Mobile App är säkrade med HTTPS-protokoll. API:s konfidentiella information lagras i hashformat i JustIN Mobile-molnet.

Den digitala nyckeln krypteras av NCoder och inkapslas i en token. Denna token kan endast öppnas av en Salto-åtkomstpunkt, vilket innebär att den digitala nyckeln är krypterad från början till slut, från NCoder till läsaren. En token lagras aldrig i JustIN Mobile-molnet. JustIN Mobile-molnet fungerar som en bro mellan baksidan och mobilappen.

Detsamma gäller om ett tredjepartsmoln används: NCoder skapar en token och endast läsaren av Salto-åtkomstpunkten kan öppna den. Detta innebär att, återigen, end-to-end-kryptering gäller för mobilnyckeln.

11. JUSTIN MOBILAPP OCH SMARTA LÅS

Krypteringsalgoritmer skyddar kommunikationen mellan Salto-åtkomstpunkten och mobilappen. Denna mekanism undviker en replay-attack och garanterar en tokens integritet.

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.