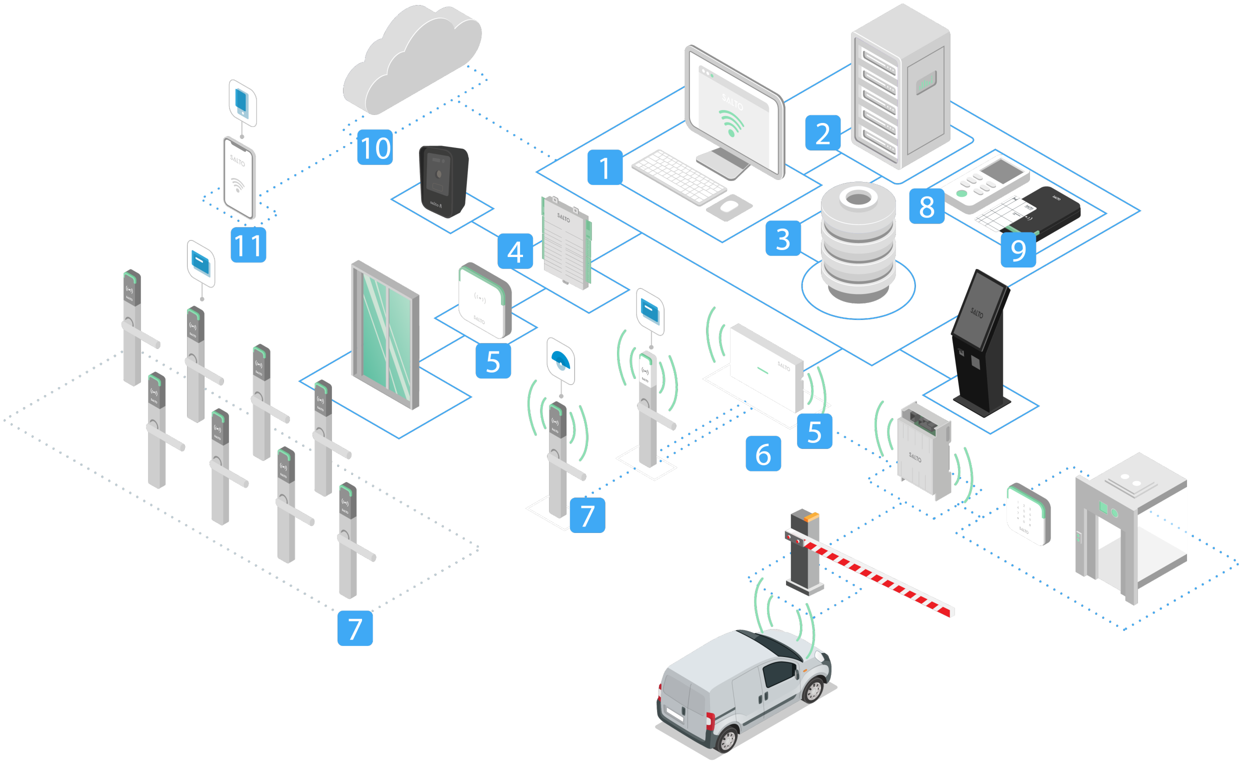
Platform security architecture

The diagram below is an overview of a Salto Space - Data-on-Card - on-premises technology platform system and its individual components.

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



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

Salto Space is a HTTPS TLS web application and the communications between Salto Service and user browsers are JSON-RPC.

Operators are required to provide a valid username and password in order to log in the front-end application. Depending on the selected configuration, these credentials are validated against either the Salto database or a directory service through LDAP.

Passwords are stored using strong crypto algorithms in the database.

2. SALTO SPACE BACK-END & SQL DATABASE

The communication between the database and the Salto Service is secured using a TLS protocol.

3. SQL DATABASE

This resides in a secure location in a client's data centre (the database is hosted on a customer's premises). Logical access to the database is managed through username and password authentication. This authentication could be in SQL mode or Windows mode, depending on the configuration during the database setup process.

Sensitive data such as user credentials and crypto keys are encrypted.

Access to the database only happens via Salto Space Service. Users cannot access the database directly.

4. SALTO SPACE BACK-END & CONTROL UNIT / GATEWAY

Communication between the Salto Service and the Salto access controller units or gateways is via Ethernet, and these communications are protected by a secure networking protocol based on UDP datagrams. Both parties are mutually authenticated and use strong encryption algorithms. Used crypto keys are encrypted and safely stored.

There is an authentication process between the Salto Service and the Salto access control unit or gateways to share a common session key, thus protecting communication.

5. CONTROL UNIT & WALL READER AND GATEWAY & NODE

Wired communication between the Salto* gateways and nodes is based on RS485 physical communication and is protected using a strong security protocol. This communication uses strong encryption algorithms. Used crypto keys are encrypted and safely stored.

* Control Unit, Wall Reader, and Gateways & Node is.

6. NODE / INTERNAL NODE & DOOR LOCK. DIRECT OR THROUGH A REPEATER

1. Salto RFnet: In the IEEE 802.15.4 based RF communication protocol which Salto uses, all strings containing application data are authenticated and encrypted through a secure mode, which uses strong encryption algorithms. Used crypto keys are encrypted and safely stored.

2. BLUEnet: This communication is based on BLE communication protocol, which uses a frequency hopping mechanism to communication with doors. Data frames are authenticated and encrypted through a secure mode, using strong encryption algorithms. Used crypto keys are encrypted and safely stored.

7. CARD & WALL READER/ ELECTRONIC LOCKS

The security related to how cards are read and how information is protected depends on the card used, which is to say, the technology of the card itself: MIFARE DESFire EV2, HID iClass, etc., such that the encryption mechanism is based on the technology of the card: AES, DES, 3DES, Crypto1, etc.

Cards are protected by Salto security keys. These security keys are transmitted to cards when the application is created (issued) by a SALTO secure device: NCoder and/or wall readers.

In addition, Salto offers different types of user authentication processes that can be combined (double-factor authentication) to increase the security of an installation: card + PIN, Card + Biometry, or PIN + Biometry.

8. ACCESS POINTS & PORTABLE PROGRAMMING DEVICE

Security keys are encrypted and transmitted to Salto access points by the Salto Portable Programming Device (PPD). A PPD is authenticated by the Salto access point through strong encryption algorithms.

9. SALTO SPACE BACK-END & NCODER

Communication between Salto Space Service and a Salto NCoder is protected by a secure encryption protocol.

10. JUSTIN MOBILE - DIGITAL KEYS

Communications to the Salto JustIN Mobile cloud from Salto ProAccess Space management access control software or from the JustIN Mobile App are secured with HTTPS protocol. API confidential information is stored in a hashed format in the JustIN Mobile cloud.

The digital Key is encrypted by the NCoder and encapsulated in a token. This token can only be opened by a Salto access point, which means that the digital key is encrypted end-to-end, from the NCoder to the reader. A token is never stored in the JustIN Mobile cloud. The JustIN Mobile cloud works as a bridge between the back end and the mobile App.

The same is true if a third-party cloud is used: the NCoder creates a token, and only the reader of the Salto access point can open it. This means that, again, end-to-end encryption applies to the mobile key.

11. JUSTIN MOBILE APP AND SMART LOCKS

Encryption algorithms protect communication between the Salto access point and mobile app. This mechanism avoids a replay attack and guarantees a token’s integrity.

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.