eleon S1
universal elevator gateway

a product of ELFIN Technology GmbH

eleon S1 - data and infrastructure security

The “eleon S1 - universal elevator gateway” gathers partially sensitive information and partially proprietary data from elevators. Hence, the underlying infrastructure complies with the necessary safety requirements to exclude unauthorized data access.

Embedded code / hardware security

On the eleon S1 hardware **secure boot** is enabled. Secure boot ensures that only our trusted and certified software can run on the device and prevents malware from hijacking the system during the boot process. We use **cryptographic keys** to validate the authenticity, source, and integrity of the code that is loaded.

The eleon S1 provides a local WiFi access point and network to configure the device during the onboarding process. To avoid unauthorized access it is secured with a password and **deactivated after 30 minutes automatically**. The password is printed on the eleon S1 so it is only visible for people who have physical access to the device itself.

The locally hosted configuration and maintenance pages are only accessible via local secure WiFi and are secured by different passwords. The password for the Onboarding website is printed on the package leaflet as part of the scope of delivery of every eleon S1 package. The password for the maintenance pages will be communicated to authorized customers only.

Firmware updates

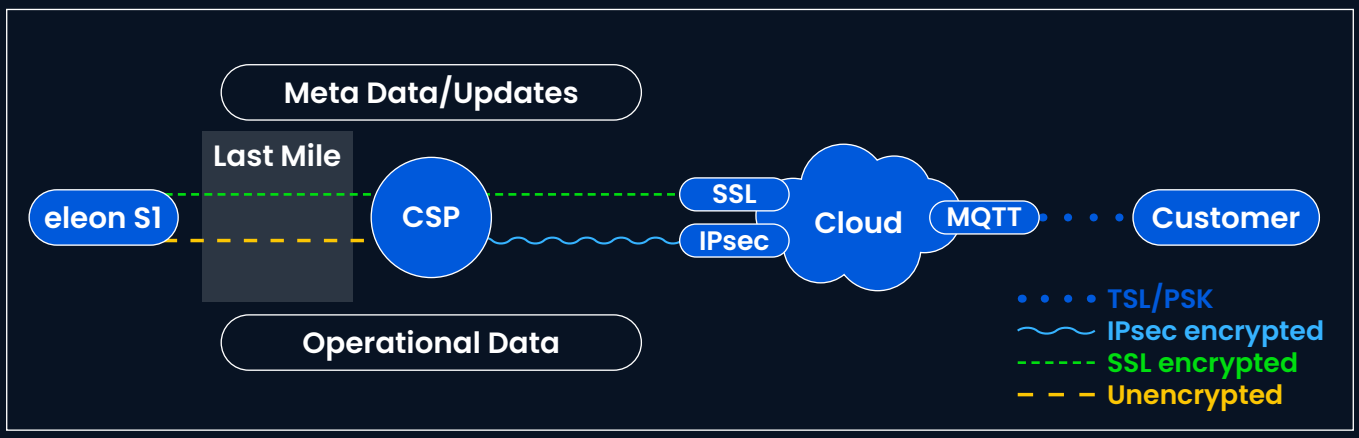
To ensure the continued security of our devices update capabilities are implemented into the software stack, which are transferred **SSL encrypted**.

Hosting

The cloud services are hosted with Hetzner in datacenters in Germany. The services are accessible via **firewall** restricted ports. Hetzner is ISO 27001 certified. You can download the latest certificates under: https://docs.hetzner.com/de/general/others/certificates/

Data transport

A crucial aspect of the data service is the end-to end-transport from the data source (elevator controller) to the storage (cloud) and from the storage to consumers (MQTT client).



Device › Cloud

The data sent from eleon S1 to the cloud is split into two categories:

- elevator meta data (installation and location related data) and
- elevator operational data

Elevator meta data which is used to identify specific elevators requires a higher security level. Therefore, it is transported via an **SSL encrypted** connection - even on the last mile between the device and the communication service provider (CSP).

Elevator operational data does not require an SSL encrypted connection to the CSP. From the CSP data is forwarded into the cloud via an **IPSec tunnel**. This procedure avoids the SSL overhead for each communicated data package, while maintaining security from CSP to the cloud server.

For elevator meta data and operational data a **proprietary, asynchronous, and binary** communication protocol is established to exclude third parties from understanding the contextual information of each data package.

Cloud › Customer

Gathered and evaluated data is provided exclusively to authorised consumers via **MQTT**. The mode of access is secured via **TLS/PSK**. This ensures an **encryption** during transport as well as an **authentication** that is used to restrict access of customers exclusively to the information of their elevator gateways.

eleon S1
universal elevator gateway

support@elfin.de
+49 221 6430816-3