FAQ - Security concerns EntryTower

Is there a risk that unauthorized persons could open or damage the EntryTower?

The robust aluminium tower offers a high level of protection against external influences from the ground up. In addition, the lockable plug-in door prevents unauthorized persons from gaining access to the interior.

Is the EntryTower adequately protected against weather conditions?

Yes, all components of the EntryTower are designed for outdoor use and have appropriate protection ratings for different environmental conditions:

- Aluminium tower protection class IP54
- EntryScreen protection class IP65
- EntryCam protection class IP67
- Bluetooth token protection class IP67
- QR code reader protection class IP54

What happens in the event of an internet or power outage - does the EntryTower remain functional?

The EntryTower is designed to ensure that access data remains reliably available even in exceptional situations. The whitelist is stored locally and can still be used in the event of an internet failure. Even in the event of a power failure, the whitelist is retained so that no data is lost.

How does EntryTower ensure data protection in accordance with the GDPR?

The processing of personal data is fully GDPR-compliant. The data is stored exclusively on servers within the EU - specifically in Germany and Finland.

Access to the profile can be controlled via clearly defined roles - admin, technician, and operator - so that only authorized persons can access the areas intended for them.

Data is stored for a maximum of 30 days after its validity expires and is then automatically deleted. The EntryCam only transmits the recognized license plate number and does not store any images. The whitelist only checks the license plate number against the camera data. In addition, the camera's recording area can be precisely defined to capture only the required image section.

Currently, no events are logged and invalid license plates are not transmitted to the cloud. The only regular cloud communication is the whitelist update, which takes place every 10 minutes in data saving mode and every 60 seconds without active data saving mode.

How is the EntryTower protected against IT security threats and unauthorized access?

Two-factor authentication via YubiKey is available as an option for accessing the system, ensuring that only uniquely verified users are granted access.

In addition, the entire system architecture was reviewed by independent security experts. We had our system audited and specifically tested for vulnerabilities by the company SSYS from Tübingen.

How is the security of communication between EntryTower and the server ensured?

All data is transmitted exclusively via secure connections. EntryTower uses HTTPS, MQTT, and TLS encryption to reliably protect communications from unauthorized access.

How can incorrect operation or configuration of the EntryTower be prevented?

The EntryTower is designed in such a way that malfunctions due to incorrect settings or operating errors are largely ruled out. Different roles with graduated rights ensure that only authorized persons can make configurations. Entrance can be controlled using various easy-to-use methods such as license plates, QR codes, or apps, and the user interface is deliberately designed to be intuitive. We also offer training courses to support the safe use of the system.

How does maintenance of the EntryTower work - and do service technicians have their own access?

Yes, service technicians receive their own login, which is specifically intended for maintenance and service tasks. In addition, a viewable maintenance log ensures full transparency regarding all work performed and system statuses.