Hardware Security

As an access control company, the security of our hardware and IoT products is our number one priority. We are aligned with international standards such as ETSI en 303 645 requirements for IoT. The implementation of secure hardware is an essential part of our products, as we believe that for software to be secure, the underlying hardware must have built in security.

We ensure that our devices do not come with preset passwords that could be easily guessed or exploited by attackers. Instead, we implement secure password mechanisms that require users to create strong, unique passwords to access the device.

In addition, we make sure our products are securely updateable, in order to let the customer apply our regularly released updates and patches to fix any security vulnerabilities and ensure that our products are secure.

Another essential security feature is the fact that we ensure that sensitive security parameters are securely stored, and that our devices communicate securely to protect personal data from unauthorised access. For this goal, we use strong cryptographic algorithms, and we protect data stored and transmitted from unauthorised access and modification via secure means including encryption or secure elements.

We also minimise exposed attack surfaces, by disabling unnecessary interfaces, implementing secure coding standards, and performing regular reviews and pentests to our devices. This includes having strong physical security controls to prevent unauthorised access or tampering, and having all security features enabled by default. Lastly, resiliency is built into our solutions taking into account the possibility of outages of data network and power.

Disclaimer:

salto /\
INSPIRED ACCESS