swissbit®

Made in Germany

Hardware Authentication Solutions for Airports

All-in-one security key for digital and physical access

Airports are important data hubs. They are also part of critical infrastructure. This makes them vulnerable to cyberattacks. In 2025, the global aviation industry saw a 24% surge in cyberattacks on airports. Nearly all of the world's largest airports have clear vulnerabilities. Cyberattacks, which are primarily phishing-based, target three main areas: flight scheduling software, security access control, and employee data. In order to maintain flight operations and avoid financial losses, the airport industry must improve its security and resilience. Airports must comply with global regulations, such as ICAO Standards, TSA Regulations and FAA (U.S.), EASA Regulations, NIS2, EU GDPR and KRITIS (EU & Germany).

fido CERTIFIED FIDO2 L2

MIFARE

140-3 FIPS

HID seos

www.swissbit.com/iShield-Key

Challenges

- **Phishing Attacks:** Attackers are impersonating authorities & targeting airport employees, attacking flight planning software, baggage systems, air traffic control & security access systems.
- **Use Cases:** Securing air traffic control & surveillance systems as well as access to airport employee data, buildings, offices, and data sharing with third party vendors.
- **Regulations:** ICAO Standards, TSA Regulations and FAA (U.S.), EASA Regulations, NIS2, GDPR and KRITIS (EU & Germany).

The commercial aviation industry saw a 24 % rise in cyber attacks in 2025 targeting airports.

Source: airwaysmag.com, 2025

Solution

FIDO passkeys and hardware keys poised to become the gold standard in authentication by 2027.

Source: 2025 HYPR State of Passwordless Identity Assurance

- **Digital and Physical Access in One Device:** Any Airport environment can be seamlessly integrated thanks to support for all major physical access systems (MIFARE, HID, LEGIC).
- **Certified Security:** The built-in smart card chip guarantees the highest level of security, with FIPS 140-3 Level 3 and CC EAL6+ certification.
- **Remote Update Capability:** Keeps all protocols up to date to meet the highest security requirements.

Benefits

- **Unified Authentication Across Systems:** In addition to supporting FIDO2, the iShield Key 2 can be used flexibly and seamlessly in heterogeneous system landscapes because it also supports PKI and OTP applications.
- **Reduced Complexity and Cost Efficiency:** The iShield Key 2 helps reduce security incidents, support efforts, and device management costs by unifying digital and physical access in a single device.
- **Perfect for Robust Use:** The highly durable iShield Key 2 is ideal for airport environments and can be used in areas where smartphones and other electronic devices are not permitted.

Do you have any questions? Get in touch!

sales@swissbit.com
www.swissbit.com

iShield Key 2 – Key Features

- **Standards:** Supports FIDO U2F, FIDO2 (CTAP 2.1), FIPS 140-3 Level 3, and optional Enterprise Attestation
- **Remote updates:** Supports secure remote firmware updates
- **Digital signatures:** Enables digital signing capabilities
- **Physical access:** Supports MIFARE DESFire EV3 for secure access and payment applications, with optional support for HID Seos and LEGIC advant/neon
- **Passkey capacity:** Stores up to 300 passkeys for scalable passwordless authentication
- **Manufactured in Germany:** Built with precision and quality

About Swissbit

Swissbit AG is the leading European technology company for data storage and security solutions.
Our vision is to build a connected world where data and identities are trusted, ensuring digital sovereignty.