swissbit®

Made in Germany

Hardware Authentication Solutions for Airlines

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

Airlines are important data hubs and critical infrastructure, making them vulnerable to cyberattacks. The global aviation industry recorded a 24% increase in cyberattacks on airlines in 2025.

Airlines are attractive targets for phishing, ransomware, and social engineering campaigns due to their extensive passenger data and critical operations. Cybercriminals use phishing to disrupt operations, extort money, and steal personal data via trusted third partiers. The airline industry must improve its security and resilience to maintain flight operations and prevent financial losses.

Airlines must comply with global regulations such as ICAO, IATA, ISO/IEC 27001, NIS2 and GDPR (EU), BSI, KRITIS and TTDSG (Germany).

fido CERTIFIED FIDO2 L2

MIFARE

140-3 FIPS

HID seos

www.swissbit.com/iShield-Key

Challenges

- **Phishing Attacks:** Attackers are impersonating staff or contractors, breach airline partners, hijack loyalty programs, manipulate bookings, targeting scheduling or check-in.
- **Use Cases:** Securing passenger data, loyalty accounts & booking systems, as well as access to employee credentials, buildings, offices, and data sharing with third party vendors.
- **Regulations:** ICAO Standards, IATA, ISO/IEC 27001, NIS2 and GDPR (EU), BSI, KRITIS and TTDSG (Germany).

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

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 Airline 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 perfect for airline environments and can be used in places where smartphones and other electronic devices are not allowed.

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.