swissbit®

Made in Germany

Hardware Authentifizierung für Flughäfen

Der universelle Security Key für digitalen und physischen Zugang

Flughäfen sind zentrale Datenknotenpunkte. Als Teil der kritischen Infrastruktur sind sie anfällig für Cyberangriffe. Im Jahr 2025 verzeichnete die globale Luftfahrtindustrie einen Anstieg der Cyberangriffe auf Flughäfen um 24%. Fast alle der weltweit größten Flughäfen weisen Schwachstellen auf. Die Cyberangriffe basieren in der Regel auf Phishing und betreffen drei Bereiche: Flugplanungssoftware, Sicherheitskontrollen und Mitarbeiterdaten. Um den Flugbetrieb aufrechtzuerhalten und finanzielle Verluste zu vermeiden, müssen Flughäfen ihre Sicherheit und Resilienz stärken. Sie müssen globale Vorschriften wie ICAO-Standards, TSA-Vorschriften und FAA (USA), EASA-Vorschriften, NIS2, EU-DSGVO und KRITIS (EU & Deutschland) einhalten.

fido CERTIFIED FIDO2 L2

MIFARE

140-3 FIPS

HID

www.swissbit.com/iShield-Key

Herausforderungen

- **Phishing:** Angreifer geben sich als Behörden aus und nehmen Flughafenmitarbeiter ins Visier, greifen Flugplanungssoftware, Gepäcksysteme, Flugsicherung und Zugangssysteme an.
- **Use Cases:** Sicherung von Flugsicherungs- und Überwachungssystemen, des Zugriffs auf Daten von Flughafenmitarbeitern, Bürogebäuden und Datenaustausch mit Drittanbietern.
- **Vorschriften:** ICAO Standards, TSA-Vorschriften & FAA (USA), EASA Vorschriften, NIS2, EU-DSGVO & KRITIS (EU und Deutschland).

Die kommerzielle Luftfahrtindustrie verzeichnete im Jahr 2025 einen Anstieg der Cyberangriffe auf Flughäfen um 24%.

Source: airwaysmag.com, 2025

FIDO Passkeys und Security Keys werden bis 2027 der Goldstandard für die Authentifizierung.

Source: 2025 HYPR State of Passwordless Identity Assurance

Lösung

- **Digitaler & physischer Zugang mit einem Gerät:** Unterstützung aller wichtigen Zugangssysteme (MIFARE, HID, LEGIC), um jede Flughafenumgebung nahtlos zu integrieren.
- **Zertifizierte Sicherheit:** Der Smartcard-Chip garantiert mit FIPS 140-3 Level 3 & CC EAL6+ Zertifizierung höchste Sicherheit.
- **Remote-Update-Fähigkeit:** Hält alle Protokolle aktuell, um höchste Sicherheitsanforderungen zu erfüllen.

Benefits

- **Einheitliche Authentifizierung über Systeme hinweg:** Der iShield Key 2 unterstützt nicht nur FIDO2, sondern kann aufgrund der Unterstützung von PKI- und OTP-Anwendungen flexibel & nahtlos in heterogenen Systemen eingesetzt werden.
- **Geringere Komplexität und Kosteneffizienz:** Der iShield Key 2 reduziert Sicherheitsvorfälle, Support-Aufwand und Kosten für das Gerätemanagement, in dem er den digitalen und physischen Zugang in einem Gerät verwendet.
- **Perfekt für den robusten Einsatz:** Der äußerst robuste iShield Key 2 ist ideal für Flughafenumgebungen geeignet. Er kann dort eingesetzt werden, wo Smartphones nicht erlaubt sind.

Sie haben Fragen?
Kontaktieren Sie uns?

sales@swissbit.com
www.swissbit.com

iShield Key 2 – Key Features

- **Standards:** Unterstützt FIDO U2F, FIDO2 (CTAP 2.1), FIPS 140-3 Level 3 sowie optionale Enterprise Attestation
- **Remote-Updates:** Unterstützt sichere Remote-Firmware-Updates
- **Digitale Signaturen:** Ermöglicht digitales Signieren
- **Physischer Zugang:** Unterstützt MIFARE DESFire EV3 für sichere Zutritts- und Zahlungsanwendungen, optional mit HID Seos und LEGIC advant/neon
- **Passkey-Kapazität:** Speichert bis zu 300 Passkeys
- **Made in Germany:** Gefertigt mit Präzision und Qualität

© Swissbit AG 2026

Über Swissbit

Die Swissbit AG ist das führende europäische Technologieunternehmen für Speicherprodukte und Sicherheitslösungen. Unsere Vision ist eine vernetzte Welt, in der Daten und Identitäten jederzeit vertrauenswürdig sind, um die digitale Souveränität zu gewährleisten.