swissbit®

Made in Germany

Hardware Authentication Solutions for Manufacturing

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

Cyberattacks continue to target the manufacturing industry, which accounted for 26% of IBM X-Force incident response cases in 2024 – making it the top target for the fourth year in a row. Phishing remains a growing risk, with IBM reporting a sharp rise in infostealer phishing emails in 2025. In Germany, phishing caused damage at 22% of companies in 2025. The attack surface has grown due to Industry 4.0 technologies such as IIoT devices, cloud-based systems, and embedded and OT systems. To improve production, minimize losses, and protect supply chains, the manufacturing industry needs to strengthen security and resilience. It also needs to comply with global regulations such as FDA, OSHA, EPA, ISO, NIS2, and KRITIS.

fido CERTIFIED FIDO2 L2

MIFARE

140-3 FIPS

HID SEOS

www.swissbit.com/iShield-Key

Challenges

- **Phishing Attacks:** In the manufacturing industry, phishing is usually how ransomware is introduced into a company's IT and OT systems and can lead to production having to stop.
- **Use Cases:** Securing industry-relevant data and connected work processes, central IT networks and OT systems, access to buildings, offices and production sites.
- **Regulations:** FDA, OSHA standards (USA), EPA guidelines (USA), ISO 9001, GMP requirements, or NIS2 and KRITIS (EU and Germany).

Business email compromise attacks targeting manufacturers have increased 56% year over year.

Source: CSO Online, 2024

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

Source: HYPR State of Passwordless Identity Assurance, 2025

Solution

- **Digital and Physical Access in One Device:** Any manufacturing 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 production 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.