swissbit®

Made in Germany

Hardware Authentication Solutions for Federal Agencies

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

Government agencies and ministries generate large amounts of data, including classified information, making them attractive targets for cyberattacks. Worldwide, the public sector is increasingly targeted by cyberattacks. In 2025 alone, around 1,000 cyber incidents in which sensitive data was disclosed were recorded. Authorities are attractive targets for phishing due to their email-centric bureaucracies. Cybercriminals use phishing to gain access to credentials or emails. To maintain public administration, authorities must improve their security and resilience. They must comply with global regulations such as ISO/IEC 27001:2022, EO 14028, NIST, OMB M-22-09, CER, CISA, NIS2, and GDPR (EU), BSIG and IT-SiG 2.0 (Germany).

fido CERTIFIED FIDO2 L2

MIFARE

140-3 FIPS

HID SEOS

www.swissbit.com/iShield-Key

Challenges

- **Phishing Attacks:** Attackers attempt to gain access to high-value data (policy drafts, citizen files) and IT systems.
- **Use Cases:** Securing high value data, IT and administrative systems, as well as access to employee credentials, buildings, offices, and data exchange with third-party vendors.
- **Regulations:** ISO/IEC 27001:2022, EO 14028, NIST, OMB M-22-09, CER, CISA, NIS2, and GDPR (EU), BSIG and IT-SiG 2.0 (Germany).

The 2025 Threat Landscape report highlights the continued targeting of EU digital infrastructure.

Source: enisa.europa.eu, 2025

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

Source: 2025 HYPR State of Passwordless Identity Assurance

Solution

- **Digital and Physical Access in One Device:** Any public administration 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 public administration 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.