swissbit®

Made in Germany

Hardware Authentication Solutions for Cities

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

Local governments are important local data hubs and critical infrastructure, which makes them vulnerable to cyberattacks. Approximately 50% of cities experience cyberattacks hourly or at least once a day. Local authorities remain prime targets, and the number of attacks is expected to rise in 2026. Cities are attractive targets for phishing and ransomware due to their extensive population data.

Cybercriminals use phishing to abuse trust chains in public administration or to gain entry to smart city and critical services ecosystems. Cities must improve their security and resilience to maintain public life and ensure the supply of goods and services. They must comply with global regulations such as CIRCIA (US), NIS2, GDPR, CRA, DORA, CER (EU), and KRITIS (Germany).

fido CERTIFIED FIDO2 L2

MIFARE

140-3 FIPS

HID seos

www.swissbit.com/iShield-Key

Challenges

- **Phishing Attacks:** Attackers impersonating trusted partners or higher government bodies and compromises city IT accounts via phishing, then pivots into connected operational systems or suppliers.
- **Use Cases:** Securing population data and IT systems, as well as access to employee credentials, buildings, offices, and data sharing with third party vendors and superior authorities.
- **Regulations:** CIRCIA (US), NIS2, GDPR, CRA, DORA and CER (EU), NIS2 and KRITIS (Germany).

Approximately 50% of cities experience cyberattacks hourly or at least once a day.

Source: sciencedirect.com, 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 city or local 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 city or local 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.