swissbit®

Made in Germany

Hardware Authentication Solutions for Finance

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

Cyberattacks are increasingly targeting the global financial sector. 64% of financial institutions reported being affected by cyber security incidents in the last 12 months. These cyberattacks can have serious consequences, including significant financial losses and the curtailment of economic activity in one or more countries. To protect financial stability, private financial data, and critical infrastructure, the financial sector must adopt stringent security measures and increase its resilience. It must comply with global regulations such as the Cybersecurity Regulation (23 NYCRR 500), Third-Party Risk Management Guidance (USA), PSD2 SCA, FIDA, NIS2, DORA or KRITIS (EU & Germany).

FIDO CERTIFIED FIDO2 L2

MIFARE

140-3 FIPS

HID seos

www.swissbit.com/iShield-Key

Challenges

- **Phishing attacks:** In the financial sector, cyberattacks via phishing primarily target financial fraud, such as the theft of bank account data and login information.
- **Use Cases:** Secure financial services identity verification, secure access to money transfers, online chats and calls from customers, secure central financial IT systems and networks, access to buildings and offices.
- **Regulations:** 23 NYCRR 500 and Third-Party Risk Management Guidance (USA), PSD2 SCA,NIS2, DORA, FIDA and KRITIS (EU and Germany)

49% of attacks against financial institutions originated from phishing.

Source: Trustwave 2024 Financial Services Threat Reports

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 financial 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.
- **Compliance:** The iShield Key 2 helps financial institutions meet their compliance requirements under international and national standards and regulations.

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.