

Made in Germany

Hardware Authentication Solutions for Education



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

Educational institutions are important data hubs, making them vulnerable to cyberattacks. The global education sector recorded a 41% year-over-year increase, becoming the most targeted industry worldwide in 2025. Universities and schools are attractive targets for phishing, ransomware, and social engineering campaigns due to their seasonal digital

activities. Cybercriminals use phishing to gain access to login details, personal data, or IT systems. The education industry must improve its security and resilience to maintain operations. The education industry must comply with global regulations such as ISO/IEC 27001, NIST, FERPA, CIPA, NIS2 and GDPR (EU), BSI and IT Security Act 2.0 (Germany).



Challenges

- **Phishing Attacks:** Attackers attempt to gain access to sensitive data (from student records to research results) and IT systems.
- **Use Cases:** Securing student and faculty data, IT and administrative systems, as well as access to employee login details, buildings, offices, and data exchange with third-party vendors.
- **Regulations:** ISO/IEC 27001, NIST, FERPA, CIPA, NIS2 and GDPR (EU), BSI and IT Security Act 2.0 (Germany).

Education will remain the most targeted industry worldwide in 2025.

Source: [checkpoint.com](https://www.checkpoint.com), 2025

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 Education 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 education 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.