

Made in Germany

Hardware Authentication Solutions for Healthcare



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

The healthcare sector remains a prime target for cyberattacks. In 2025, the USA reported 710 major healthcare data breaches, exposing health data of at least 61.5 million people. Germany's BSI also recorded 138 healthcare-related incidents, including 43 affecting providers such as hospitals.

To safeguard health, patient data and critical infrastructure, the sector must implement strong security measures. It must also follow global regulations, such as HIPAA and JCAHO (USA) or NIS2 and KRITIS (EU and Germany) and MHLW guidelines (Japan).



Challenges

- **Heterogenous Systems:** Healthcare providers use several systems from medical records to access management.
- **Use Cases:** Secure access to emergency rooms, radiology departments, maternity wards, parking lots, central hospital systems, and settings on medical equipment and operating rooms.
- **Regulations:** For example, there are HIPAA and JCAHO (USA), NIS2 and KRITIS (EU and Germany), and MHLW guidelines (Japan).

Phishing remains a perennial cybersecurity threat. Phishing attacks increased by 58 % in 2023, with an estimated financial impact of 3.5 billion USD in 2024.

Source: 2024 Microsoft Cyber Digital Defense Report

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 healthcare 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:** iShield Key 2 users can access patient records and secure portals with a single tap.
- **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 Harsh Environments and Gloves:** The iShield Key 2 is a durable device designed for medical settings (e.g., disinfectants) and extreme conditions, even when used with robust or medical gloves.

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.