

Hardware Authentifizierung für den Gesundheitssektor

Made in Germany



Der universelle Security Key für digitalen und physischen Zugang

Der Gesundheitssektor ist zunehmend Ziel von Cyberangriffen. Im Jahr 2024 gab es in den USA etwa 700 Cybervorfälle, bei denen über 180 Millionen Menschen und ihre Gesundheitsdaten betroffen waren. Auch in Deutschland gehörten Krankenhäuser und Dienstleister zu den Zielen, was zum Teil lebensbedrohliche Folgen für Patienten hatte.

Um Gesundheit, Patientendaten und kritische Infrastrukturen zu schützen, muss der Sektor strenge Sicherheitsmaßnahmen ergreifen und die Resilienz stärken. Zudem muss er globale Vorschriften wie HIPAA und JCAHO (USA), NIS2 und KRITIS (EU & Deutschland) sowie MHLW-Richtlinien (Japan) beachten.



Herausforderungen

- **Heterogene Systeme:** Gesundheitsdienstleister nutzen in der Regel mehrere Systeme, von der Krankenakte bis zur Zugangsverwaltung.
- **Use Cases:** Sicherer Zugang zu Notaufnahmen, zur Radiologie, Entbindungsstationen, zentralen Krankenhausssystemen und Einstellungen an medizinischen Geräten & Operationssälen.
- **Vorschriften:** HIPAA & JCAHO (USA), NIS2 & KRITIS (EU & Deutschland), und MHLW-Richtlinien (Japan).

Phishing Angriffe nahmen 2023 um 58% zu und verursachten im Jahr 2024 einen geschätzten finanziellen Schaden von 3,5 Mrd. USD.

Source: 2024 Microsoft Cyber Digital Defense Report

Lösung

FIDO Passkeys und Security Keys werden bis 2027 der Goldstandard für die Authentifizierung.

Source: 2025 HYPR State of Passwordless Identity Assurance

- **Digitaler & physischer Zugang mit einem Gerät:** Unterstützung aller wichtigen Zugangssysteme (MIFARE, HID, LEGIC), um jede Umgebung im Gesundheitssektor nahtlos zu integrieren.
- **Zertifizierte Sicherheit:** Der Smartcard-Chip garantiert mit FIPS 140-3 Level 3 & CC EAL6+ Zertifizierung höchste Sicherheit.
- **Remote-Update-Fähigkeit:** Hält alle Protokolle aktuell, um höchste Sicherheitsanforderungen erfüllen zu können.

Vorteile

- **Authentifizierung über Systeme hinweg:** iShield Key 2 ermöglicht es seinen Benutzern, mit nur einem Fingertipp auf Patientenakten und sichere Portale zuzugreifen.
- **Geringere Komplexität und Kosteneffizienz:** Der iShield Key 2 reduziert Sicherheitsvorfälle, Support-Aufwand und Kosten für das Gerätemanagement, indem er den digitalen und physischen Zugang in einem Gerät vereint.
- **Perfekt für raue Umgebungen und Handschuhe:** iShield Key 2 ist ein robustes Gerät für den medizinischen Einsatz, z.B. bei der Verwendung von Desinfektionsmitteln, Einsatz mit Handschuhen & unter extremen Bedingungen.

Sie haben Fragen?
Kontaktieren Sie uns!

sales@swissbit.com
www.swissbit.com



Feature	iShield Key 2 FIDO2	iShield Key 2 Pro	iShield Key 2 FIDO2 MIFARE	iShield Key 2 Pro MIFARE	iShield Key 2 FIDO2 FIPS	iShield Key 2 Pro FIPS
FIDO2	✓	✓	✓	✓	✓	✓
PIV (Smartcard)		✓		✓		✓
OTP (HOTP, TOTP)		✓		✓		✓
300 Passkeys	✓	✓	✓	✓	✓	✓
MIFARE			✓	✓		
FIPS					✓	✓

© Swissbit AG 2025

About Swissbit

Die Swissbit AG ist das führende europäische Technologieunternehmen für Speicherprodukte und Sicherheitslösungen. Unsere Vision ist eine vernetzte Welt, in der Daten und Identitäten jederzeit vertrauenswürdig sind, um die digitale Souveränität zu gewährleisten.