swissbit®

Made in Germany

Hardware Authentifizierung für den Gesundheitssektor

Der universelle Security Key für digitalen und physischen Zugang

Der Gesundheitssektor bleibt ein vorrangiges Ziel für Cyberangriffe. 2025 meldeten die USA 710 schwere Datenschutzverletzungen im Gesundheitswesen, bei denen Gesundheitsdaten von mindestens 61,5 Millionen Menschen offengelegt wurden. Das BSI verzeichnete in Deutschland 138 Gesundheitsvorfälle, darunter 43 bei Leistungserbringern wie Krankenhäusern. 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.

fido CERTIFIED FIDO2

MIFARE

140-3 FIPS

HID seos

www.swissbit.com/iShield-Key

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 Krankenhaussystemen 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 rauhe 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

iShield Key 2 – Key Features

- **Standards:** Unterstützt FIDO U2F, FIDO2 (CTAP 2.1), FIPS 140-3 Level 3 sowie optionale Enterprise Attestation
- **Remote-Updates:** Unterstützt sichere Remote-Firmware-Updates
- **Digitale Signaturen:** Ermöglicht digitales Signieren
- **Physischer Zugang:** Unterstützt MIFARE DESFire EV3 für sichere Zutritts- und Zahlungsanwendungen, optional mit HID Seos und LEGIC advant/neon
- **Passkey-Kapazität:** Speichert bis zu 300 Passkeys
- **Made in Germany:** Gefertigt mit Präzision und Qualität

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.