swissbit®

Made in Germany

Hardware Authentifizierung für Bildungseinrichtungen

Der universelle Security Key für digitalen und physischen Zugang

Universitäten und Schulen sind wichtige Datenzentren und anfällig für Cyberangriffe. Der globale Bildungssektor verzeichnete einen Anstieg von 41 % gegenüber dem Vorjahr. Damit ist er 2025 die weltweit am stärksten betroffene Branche. Aufgrund der saisonalen digitalen Aktivitäten sind Universitäten & Schulen Ziele für Phishing-, Ransomware- und Social Engineering-Kampagnen.

Cyberkriminelle nutzen Phishing, um an Anmeldedaten, personenbezogene Daten oder IT-Systeme zu gelangen. Bildungseinrichtungen müssen ihre Sicherheit und Resilienz verbessern, um den Betrieb aufrechterhalten zu können. Sie müssen globale Vorschriften wie ISO/IEC 27001, NIST, FERPA, CIPA, NIS2 und DSGVO (EU), BSiG & IT-SiG 2.0 (Deutschland) einhalten.

fido CERTIFIED FIDO2 L2

MIFARE

140-3 FIPS

HID

www.swissbit.com/iShield-Key

Herausforderungen

- **Phishing:** Angreifer versuchen, sich Zugang zu sensiblen Daten – von Studentenakten bis hin zu Forschungsergebenissen – sowie zu IT-Systemen zu verschaffen.
- **Use Cases:** Sicherung von Daten von Studierenden und Lehrkräften, IT- und Verwaltungssystemen und Zugriff auf Anmeldedaten von Mitarbeitern, Gebäude, Büros und Daten-austausch mit Drittanbietern.
- **Vorschriften:** ISO/IEC 27001, NIST, FERPA, CIPA, NIS2 & DSGVO (EU), BSiG & IT-SiG 2.0 (Deutschland).

Der Bildungssektor wird 2025 weltweit der am stärksten von Cyberangriffen betroffene Bereich sein.

Source: checkpoint.com, 2025

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

Source: 2025 HYPR State of Passwordless Identity Assurance

Lösung

- **Digital and Physical Access in One Device:** Unterstützung aller wichtigen Zugangssysteme (MIFARE, HID, LEGIC), um jede Umgebung einer Bildungseinrichtung nahtlos zu integrieren.
- **Certified Security:** 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 zu erfüllen.

Benefits

- **Einheitliche Authentifizierung über Systeme hinweg:** Der iShield Key 2 unterstützt nicht nur FIDO2, sondern kann aufgrund der Unterstützung von PKI- und OTP-Anwendungen flexibel & nahtlos in heterogenen Systemen eingesetzt werden.
- **Geringere Komplexität und Kosteneffizienz:** Der iShield Key 2 reduziert Sicherheitsvorfälle, Support-Aufwand und Kosten für das Gerätemanagement, in dem er den digitalen und physischen Zugang in einem Gerät verwendet.
- **Perfekt für den robusten Einsatz:** Der robuste iShield Key 2 ist ideal für Umgebungen von Bildungseinrichtungen geeignet. Er kann dort eingesetzt werden, wo Smartphones nicht erlaubt sind.

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

Über 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.