

Hardware Authentifizierung für den Finanzsektor

Made in Germany



Der universelle Security Key für digitalen und physischen Zugang

Cyberangriffe zielen zunehmend auf den Finanzsektor ab. 64% der Finanzinstitute gaben an, in den letzten 12 Monaten von Cybersicherheitsvorfällen betroffen gewesen zu sein. Diese können schwerwiegende Folgen haben, darunter erhebliche finanzielle Verluste und die Unterbrechung der Wirtschaftstätigkeit in einem oder mehreren Ländern.

Um die finanzielle Stabilität, private Finanzdaten und kritische Infrastrukturen zu schützen, muss der Finanzsektor strenge Sicherheitsmaßnahmen ergreifen und seine Resilienz stärken. Er muss globale Vorschriften wie die Cybersecurity Regulation (23 NYCRR 500), Third-Party Risk Management Guidance (USA), PSD2 SCA, FDA, NIS2, DORA oder KRITIS (EU & Deutschland) einhalten.



Herausforderungen

- **Phishing:** Phishing-Angriffe zielen in erster Linie auf Finanzbetrug ab, z.B. auf den Diebstahl von Kontodaten & Anmeldeinformationen.
- **Use Cases:** Sichere Identitätsüberprüfung für Finanzdienstleistungen, sicherer Zugang zu Geldüberweisungen & Online-Chats und -Anrufe von Kunden, sichere zentralisierte Finanz-IT-Systeme sowie der Zugang zu Gebäuden und Büros.
- **Vorschriften:** 23 NYCRR 500 & Third-Party Risk Management Guidance (USA), PSD2 SCA, NIS2, DORA, FIDA & KRITIS (EU & Deutschland)

49% der Cyberangriffe gegen Finanzinstitutionen erfolgten durch Phishing

Source: Trustwave 2024 Financial Services Threat Reports

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

Source: 2025 HYPR State of Passwordless Identity Assurance

Lösung

- **Digitaler & physischer Zugang mit einem Gerät:** Unterstützung aller wichtigen Zugangssysteme (MIFARE, HID, LEGIC), um jede Finanzumgebung 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 zu erfüllen.

Vorteile

- **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, indem er den digitalen und physischen Zugang in einem Gerät vereint.
- **Einhaltung von Vorschriften:** Der iShield Key 2 unterstützt Finanzinsitute bei der Erfüllung ihrer Compliance-Anforderungen gemäß (inter-) nationaler Vorschriften.

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.