



Made in Germany

## iShield Key 2: Authentifizierung der nächsten Generation



## Der universelle Security Key für digitalen und physischen Zugang

- **Weniger Hardware & Aufwand:** Kombiniert FIDO2 und Access Control in einem Gerät.
- **Sichere digitale Anmeldung:** Ersetzt bzw. erhöht die Sicherheit von Passwörtern mit FIDO2, PIV & OTP.
- **Physische Zugangskontrolle:** Für Büros, Rechenzentren & Sicherheitsbereiche.
- **Plug-and-Play:** Kompatibel mit Google, Microsoft, AWS und vielem mehr.
- **Kosteneffizient:** Senkt Wartungs- und Verwaltungskosten.
- **Robust & einfach:** Hohe Nutzerakzeptanz, zuverlässige Sicherheit.



## iShield Key 2 – Der Schlüssel zu ganzheitlicher Sicherheit

Der neue **Swissbit iShield Key 2** vereint digitale und physische Zugangskontrolle in einem Gerät und ermöglicht eine **effiziente Authentifizierung** für IT-Systeme, Gebäude oder sichere Drucklösungen. Als Hybridschlüssel schafft er zahlreiche Touchpoints im Arbeitsalltag und unterstützt einen ganzheitlichen Security-Ansatz.

Unternehmen können **das Sicherheitsniveau sofort erhöhen** und neue Features schrittweise ausrollen. Der iShield Key 2 ist ein **Schlüsselement einer Zero-Trust-Strategie** und

erleichtert die **Einführung von MFA** sowie die **Erfüllung regulatorischer Vorgaben wie NIS2, CRA, DORA** oder der **Executive Order** zur Cybersicherheit.

Mit **MIFARE-, HID Seos- und FIPS-Varianten** setzt er neue Maßstäbe: Er ist der erste FIDO-Sicherheitsschlüssel, der **MIFARE DESFire EV3** und **HID Seos** unterstützt und eine nach **FIPS 140-3 Level 3** zertifizierte Variante bietet – und damit maximale Sicherheit für anspruchsvolle Anwendungen gewährleistet.

### Technologie

#### Digital Authentifizierung

- FIDO2 / WebAuthn, CTAP 2.1 und U2F
- Bis zu 300 Passkeys
- Optional HOTP, TOTP und PIV-Unterstützung

#### Physischer Zugang

- MIFARE DESFire EV3
- HID Seos
- LEGIC advant/neon

#### Sicherheit und Zertifikate

- FIDO2-zertifiziert
- Optional FIPS 140-3 Level 3
- Optional Enterprise Attestation



## iShield Key 2 – Features auf einen Blick



- Ein Sicherheitsschlüssel für digitalen und physischen Zugriff
- Phishing-resistente MFA und passwortlose Anmeldung
- Sichere Authentifizierung für Websites, Anwendungen, Netzwerke und Cloud-Dienste
- Ermöglicht digitale Signaturfunktionen
- Unterstützt Zero-Trust- und Compliance-orientierte Sicherheitsstrategien
- Skalierbar für den Einsatz in Unternehmen
- Robust, benutzerfreundlich und für alltägliche Arbeitsabläufe konzipiert
- Unterstützt sichere Remote-Firmware-Updates
- Erhältlich in Varianten für diverse Authentifizierungs- und Zugriffskontrollanforderungen