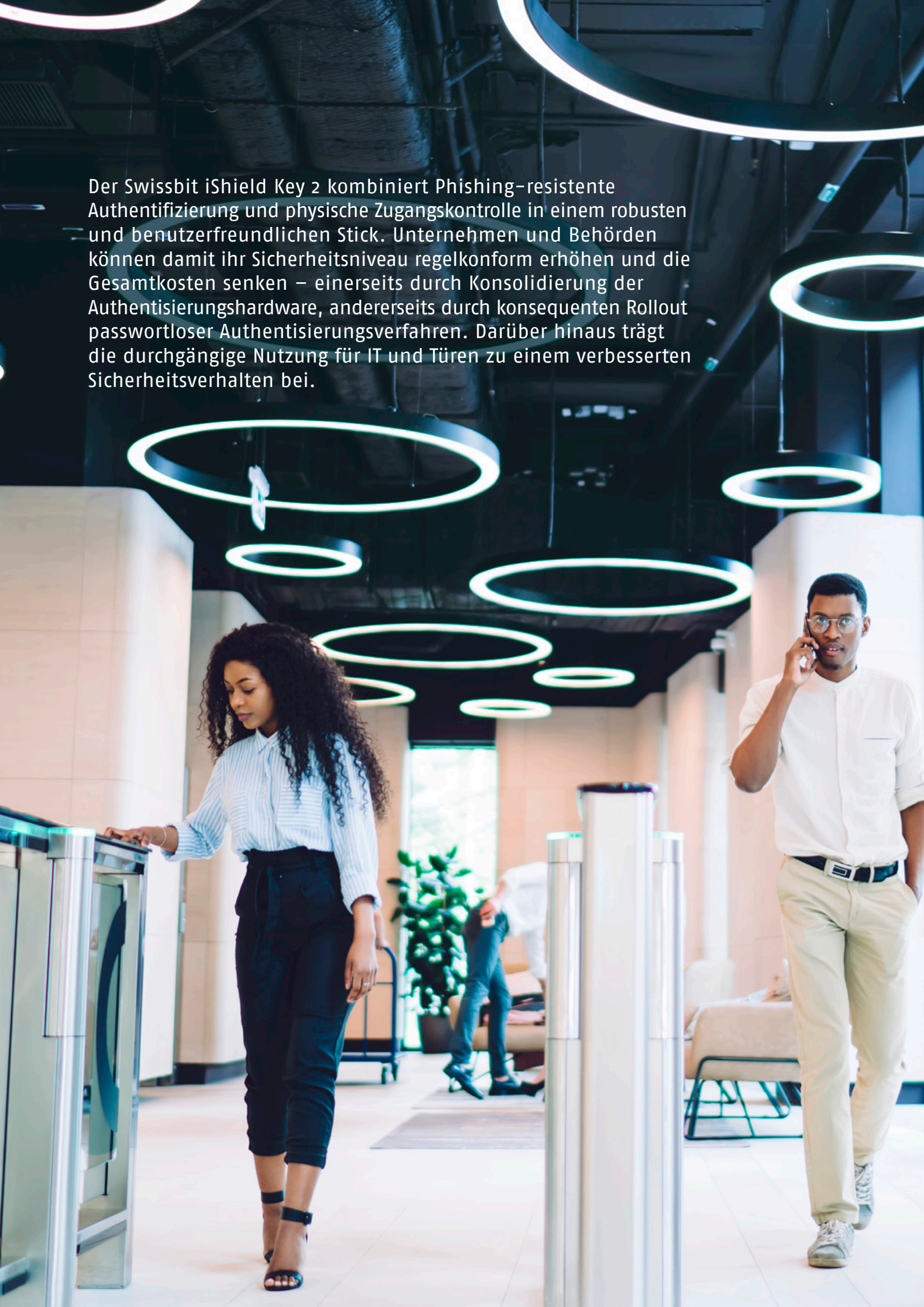
swissbit®

Swissbit iShield Key 2

All-in-one-Sicherheitsschlüssel für digitalen und physischen Zugang



Der Swissbit iShield Key 2 kombiniert Phishing-resistente Authentifizierung und physische Zugangskontrolle in einem robusten und benutzerfreundlichen Stick. Unternehmen und Behörden können damit ihr Sicherheitsniveau regelkonform erhöhen und die Gesamtkosten senken – einerseits durch Konsolidierung der Authentisierungshardware, andererseits durch konsequenten Rollout passwortloser Authentisierungsverfahren. Darüber hinaus trägt die durchgängige Nutzung für IT und Türen zu einem verbesserten Sicherheitsverhalten bei.

Mehr Sicherheit mit weniger Aufwand – geht das?

Steigende Cyberbedrohungen, hybride Arbeitsmodelle und regulatorische Vorgaben wie KRITIS-V, DORA, NIS2 oder CRA erfordern starke Authentifizierungslösungen in Unternehmen und Behörden. Gleichzeitig unterstützen physische Zugangskontrollen in Form von Karten oder Transpondern (Keyfob) zunehmend digitale Zugangsdaten. Warum also nicht beide Herausforderungen mit einem einzigen, kosteneffizienten und skalierbaren All-in-One-Sicherheitsschlüssel meistern?

Swissbit iShield Key 2: Ein Schlüssel für digitale & physische Authentifizierung

Mit dem iShield Key 2 von Swissbit können Unternehmen und Behörden nicht nur digitale Identitäten, sondern auch physische Räume vor unbefugtem Zutritt schützen. Sicherheitsverantwortliche behalten jederzeit die Kontrolle über alle wichtigen Assets und Credentials. Als Mehrwert lassen sich praktische Zusatzfunktionen realisieren – vom sicheren Drucken (FollowMe-Printing) bis hin zu Bezahlfunktionen.

Der iShield Key 2 ist eine flexible und skalierbare Lösung für bestehende IAM-Systeme (Identity Access Management), mit der sich das Sicherheitsniveau in Unternehmen und Behörden bedarfsgerecht erhöhen und neue Sicherheitsfunktionen sukzessive ausrollen lassen. Darüber hinaus bewährt sich der Multi-Protokoll-Key als Einstiegspunkt für die Einführung einer sicheren Zwei-Faktor-Authentifizierung. Das Multitalent für mehr Sicherheit minimiert damit auch den Verwaltungs- und Supportaufwand durch eine IT-Praxis mit weniger oder gar keinen Passwörtern (less passwords/passwordless).

Chance zur Verbesserung des Nutzerverhaltens

Die zusätzlich integrierte Zutrittskontrolle hilft Unternehmen und Behörden, das Sicherheitsverhalten ihrer Mitarbeiterinnen und Mitarbeiter positiv zu beeinflussen und Security- bzw. MFA-Fatigue vorzubeugen. Unter anderem führt der Einsatz des multifunktionalen Security-Keys dazu, dass der Schlüssel in den Pausen und nach der Arbeit konsequent aus dem Computer gezogen wird und dieser dadurch automatisch gesperrt werden kann.

Einsatzszenarien & Vorteile

Als Ausgangspunkt für ein gesamtheitliches Sicherheitskonzept eröffnet der Swissbit iShield Key 2 vielfältige Verbesserungspotenziale – von der digitalen und physischen Sicherheit bis hin zu Kosteneinsparungen und verbesserter Usability.

Sicherheitsniveau erhöhen

Ziele

- Schwache, passwortbasierte Anmeldeverfahren ersetzen
- Konformität mit regulatorischen Anforderungen herstellen

Warum iShield Key 2?

- **Hohe Sicherheit** durch FIDO2-Standard
- **Kompatibilität** zu bestehenden Systemen
- **Skalierbarkeit & sukzessiver Ausbau** der Security-Landschaft (IAM, Türen, etc.)
- **Usability:** einfache Nutzung und tägliche Routine (z. B. Token am Schlüsselbund)

Physischen Zugang integrieren & konsolidieren

Ziele

- Hardware konsolidieren (1 Token)
- Verwaltungsaufwand reduzieren
- Physischen Zugang integrieren: Büro, Labor, Rechenzentrum etc.

Warum iShield Key 2?

- **User Adoption:** Token als ständiger Begleiter für physischen und digitalen Zugang
- **On- und Offline:** wichtig für kritische Anwendungen, z. B. in Krankenhäusern
- **Kompatibilität mit bestehenden Systemen** (MIFARE, HID Seos, LEGIC advant/neon)

Kosten senken

Ziele

- IAM-Wartungskosten senken (Passwörter rücksetzen/freischalten)
- Mehrere Technologien konsolidieren (z. B. FIDO2 & MIFARE)

Warum iShield Key 2?

- **Keine vergessenen oder notierten Passwörter**
- **Einfache Verwaltung** (iShield Key Manager)
- **Einfachere Compliance-Umsetzungen**
- **Kostengünstiger** durch Hardware-Konsolidierung: der iShield Key 2 ersetzt separate Smartcards und Kartenleser

Usability steigern

Ziele

- Sicherheitspraxis vereinfachen
- Security-/MFA-Fatigue vorbeugen
- Komplexität in der Security senken

Warum iShield Key 2?

- **Einfache Bedienung:** Einstecken & PIN eingeben, Touch-Authentifizierung auf der Geräterückseite
- **Hohe User-Akzeptanz,** gerade bei häufigen Vorgängen
- **Einfaches Handling:** ein robustes Gerät für eine (oder mehrere) klar definierte Aufgabe(n)

Technologie

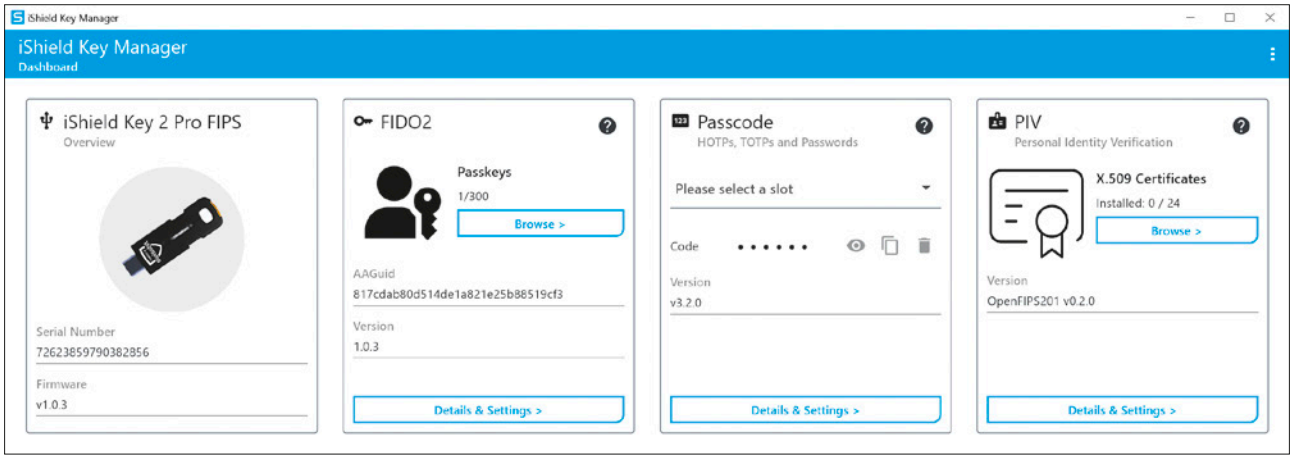
Der iShield Key 2 ist ein **All-in-One-Sicherheitsschlüssel**, der gleichzeitig zur digitalen und physischen Authentisierung sowie für praktische Zusatzfunktionen wie Bezahlkarte, digitaler Ausweis etc. eingesetzt werden kann.

Digitale Authentifizierung: Zur sicheren Anmeldung an Betriebssystemen, Webseiten und Online-Diensten unterstützt der Hardware Authenticator mit USB-A/C und NFC-Schnittstelle alle relevanten Sicherheitsstandards, darunter **FIDO2/Passkeys** als Phishing-resistentes Protokoll zum Schutz digitalenr Identitäten mit bis zu **300 Passkeys** als Passwortersatz. Zu den weiteren Standards zählen **HOTP & TOTP** zur Erstellung von One-Time-Passwords sowie PIV für Smartcard-Funktionen. Die Smart-Card-basierte Kryptographie mit öffentlichem und privatem Schlüssel gewährleistet ein hohes Sicherheitsniveau.

Physische Authentifizierung: Für die Zutrittskontrolle zu restriktiven Bereichen unterstützt der iShield Key 2 die Technologien **MIFARE DESFire EV3, HID Seos** oder **LEGIC advant/neon** – inklusive Implementierungsoptionen für Zusatz-Applikationen auf Basis des MIFARE-Stacks.

Effizientes Management

Sobald der iShield Key mit einem Computer oder NFC-fähigen Mobilgerät verbunden ist, kann er mit dem **iShield Key Manager** (iKM) konfiguriert werden. Der iKM unterstützt Windows, macOS, iOS, Linux und Android – auf Mobilgeräten unter iOS und Android steht dabei die TOTP-Funktionalität zur Verfügung.



MIFARE: Mehr als nur Zutrittskontrolle

Der **iShield Key 2** mit **MIFARE-Unterstützung** basiert auf einem **NXP-Chip** und bietet weit mehr als nur Zutrittskontrolle! Denn die leistungsfähige Plattform ermöglicht die Implementierung attraktiver Zusatz-Applikationen auf Basis der MIFARE-Technologie. Die Palette reicht von der Zeiterfassung über Bezahlfunktionen für Kantine und Cafeteria bis hin zu Mitglieds- oder Campusausweisen.

Sicherer und flexibler All-in-one-Schlüssel

Digitale Authentifizierung

Vorteile iShield Key 2

- **Plug-and-Play:** Kompatibilität mit vielen Services (Google, Microsoft, AWS, ...)
- **Passwordless:** bis zu 300 Passkeys
- **Mobil:** Tap-and-go-Authentifizierung über NFC-fähige Mobilgeräte
- **Multi-Protokoll-Unterstützung**
  - FIDO2/Passkeys
  - OATH-HOTP (Standard RFC4226)
  - OATH-TOTP (Standard RFC6238)
  - PIV

&

Zugangskontrolle

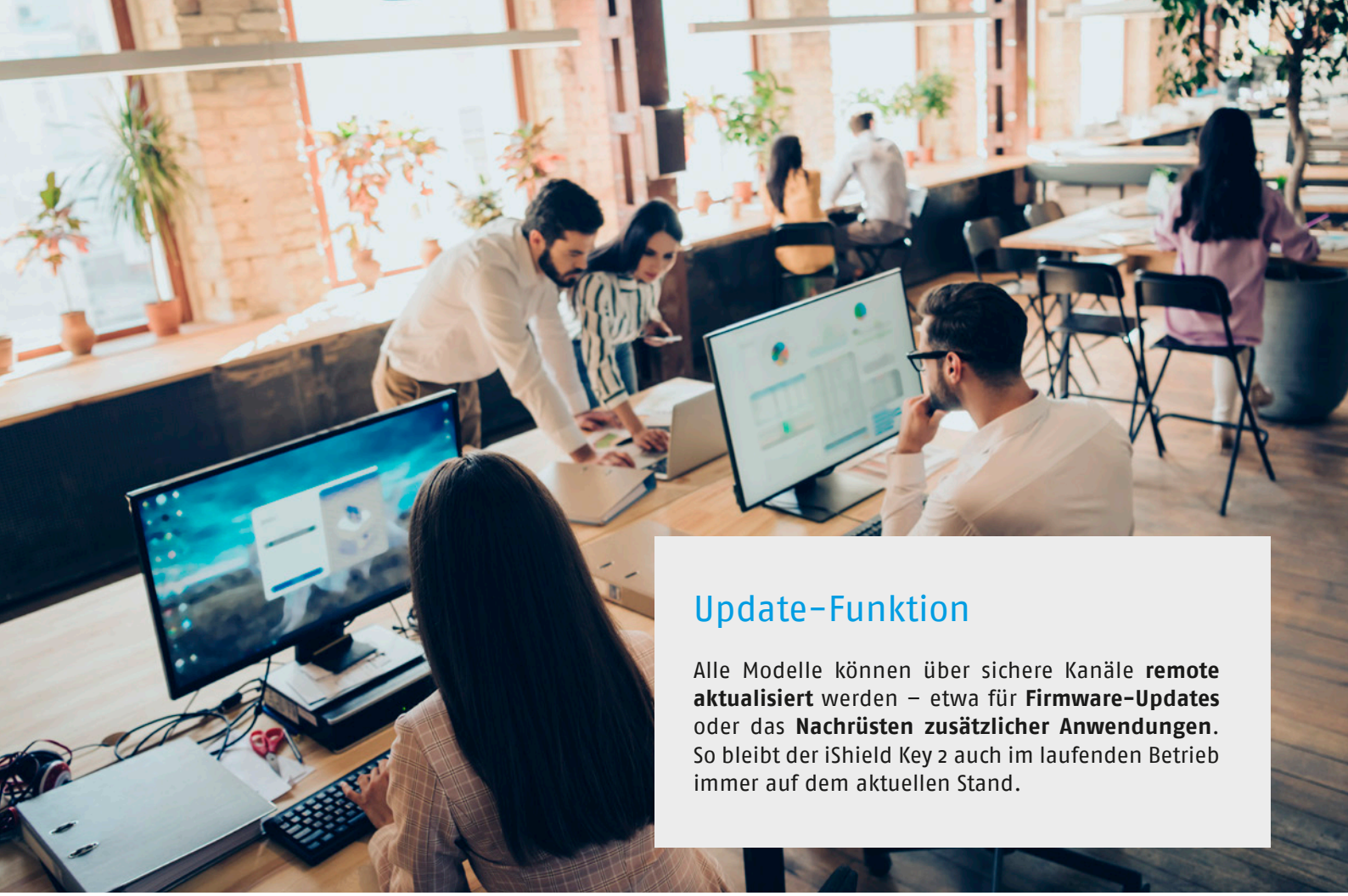
Vorteile iShield Key 2

- **Optionale Technologien** für zusätzliche Anforderungen in Unternehmen/Behörden
- **Langlebig:** robust und wasserfest
- **Handlich:** schlank & leicht mit Schlüsselring
- **Unterstützte Technologien**
  - MIFARE DESFire EV3 (NXP)
  - HID Seos (optional)
  - LEGIC advant/neon (optional)

Sicherheit & Zertifizierungen

Für höchste Sicherheitsanforderungen von Unternehmen und Behörden ist der iShield Key 2 von Swissbit **FIDO-zertifiziert**, optional auch nach **FIPS140-3 Level 3**. Für die offene Smartcard-Integration ist der Sicherheitsschlüssel zudem **OpenSC-kompatibel**. Eine Version mit **FIDO Enterprise Attestation** ist ebenfalls erhältlich. Dies hilft Unternehmen sicherzustellen, dass nur vertrauenswürdige, selbst ausgegebene FIDO Keys auf die eigenen Systeme zugreifen können.

Funktion	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					✓	✓



Update-Funktion

Alle Modelle können über sichere Kanäle **remote aktualisiert** werden – etwa für **Firmware-Updates** oder das **Nachrüsten zusätzlicher Anwendungen**. So bleibt der iShield Key 2 auch im laufenden Betrieb immer auf dem aktuellen Stand.

2-in-1 für maximale Sicherheit und Effizienz!

Mit dem iShield Key 2 können Sicherheitsverantwortliche die zentralen Aufgaben der digitalen und physischen Zugangskontrolle mit einem einzigen, robusten und benutzerfreundlichen All-in-One-Schlüssel erledigen. Im Ergebnis profitieren Unternehmen und Behörden von einem **höheren Sicherheitsniveau, geringeren IAM- und Gesamtkosten sowie einer verbesserten Benutzerfreundlichkeit**.

Klingt interessant? Gehen Sie jetzt den nächsten Schritt und machen Sie Ihre Authentifizierungsstrategie fit für die Zukunft – mit einer einfach zu handhabenden, flexiblen und standardkonformen Lösung – natürlich datenschutzkonform und in höchster Qualität Made in Germany!

swissbit®

Sie haben Fragen zum iShield Key 2 oder einer konkreten Anwendung?

Swissbit Europe (HQ)
Tel. +41 71 913 03 00
sales@swissbit.com

Swissbit North America
Tel. +1 978-490-3252
salesna@swissbit.com

Swissbit Japan
Tel. +81 3 6258 0521
sales-japan@swissbit.com

Swissbit Asia
Tel. +886 912 059 197
salesasia@swissbit.com

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.

Swissbit wurde 2001 gegründet und verfügt über Niederlassungen in der Schweiz (Hauptsitz), Deutschland, den USA, Japan und Taiwan sowie über eine hochmoderne Elektronikfertigung am Standort Berlin.

www.swissbit.com

www.swissbit.com/ishield-key

Made in Germany