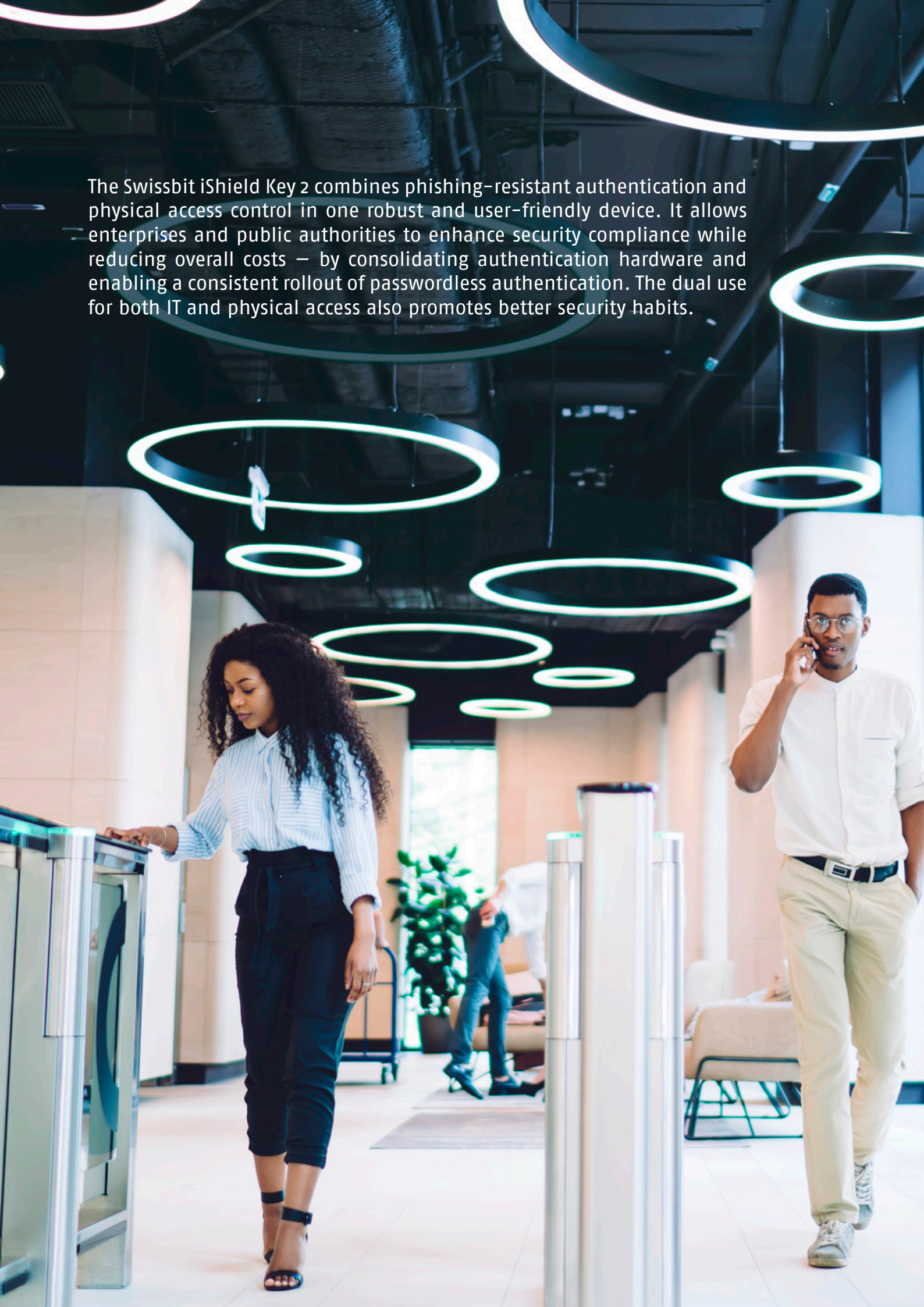
swissbit®

Swissbit iShield Key 2

All-in-one security key for digital and physical access



The Swissbit iShield Key 2 combines phishing-resistant authentication and physical access control in one robust and user-friendly device. It allows enterprises and public authorities to enhance security compliance while reducing overall costs – by consolidating authentication hardware and enabling a consistent rollout of passwordless authentication. The dual use for both IT and physical access also promotes better security habits.

More security with less effort – is that possible?

Increasing cyber threats, hybrid work models, and regulations such as KRITIS-V, DORA, NIS2, CRA, OMB M-22-09, and the U.S. Executive Order on cybersecurity demand strong authentication solutions for organizations and public sector institutions. Physical access controls have also evolved to support digital credentials, such as cards and fobs. Why not tackle both challenges with a single, cost-effective, and scalable all-in-one security key?

As a flexible and scalable solution for existing Identity Access Management (IAM) systems, the iShield Key 2 helps raise security levels and supports a gradual rollout of new authentication features. It also serves as an ideal entry point into secure two-factor authentication. This multi-protocol authenticator contributes to reduced administrative and support overhead by promoting IT practices with fewer – or no – passwords at all.

Swissbit iShield Key 2: One key for logical and physical access

The Swissbit iShield Key 2 enables organizations and authorities to protect not only digital identities but also physical spaces from unauthorized access. Security managers retain full control over all key assets and credentials. Additional benefits include convenient features such as secure printing (FollowMe printing) and payment capabilities.

Opportunity to improve user behavior

The integrated physical access function helps improve user security awareness and reduce MFA fatigue and burnout. For instance, using the multifunctional key encourages users to remove the authenticator when leaving a workstation unattended – automatically locking the computer and/or physically separating the workstation from the required authenticator to enhance endpoint protection.

Use cases & benefits

As a foundation for a comprehensive security strategy, the Swissbit iShield Key 2 opens up numerous opportunities – from digital and physical protection to cost savings and improved usability.

Increase security level

Goals

- Replace weak, password-based login methods
- Ensure compliance with regulatory requirements

Why iShield Key 2?

- **High security** through FIDO2 standard
- **Compatibility** with existing systems
- **Scalable rollout** of security infrastructure (IAM, doors, etc.)
- **Usability:** easy to use and integrate into daily routines (e.g., keychain token)

Integrate & consolidate physical access

Goals

- Consolidate hardware (1 token)
- Reduce administrative effort
- Integrate physical access: Buildings, offices, labs, data centers, etc.

Why iShield Key 2?

- **High user adoption:** one key for both digital and physical access
- **Online and offline use:** critical for applications in healthcare and other sectors
- **Compatibility with common systems** (MIFARE, HID SEOS, LEGIC advant/neon)

Reduce costs

Goals

- Reduce IAM maintenance costs (reset/unlock passwords)
- Consolidate several technologies (e.g. FIDO2 & MIFARE)

Why iShield Key 2?

- **No forgotten or written down passwords**
- **Simple administration** (iShield Key Manager)
- **Simpler compliance implementation**
- **More cost-effective** to consolidate hardware (e.g., the iShield Key 2 eliminates the need for a separate smart card and reader)

Increase usability

Goals

- Simplify security processes
- Preventing security/MFA fatigue
- Reducing complexity in security

Why iShield Key 2?

- **Simple to use:** plug in & enter PIN, touch sensor on back of device
- **High user acceptance**, especially for frequent processes
- **Easy handling:** a robust device for one (or more) clearly defined task(s)

Technology

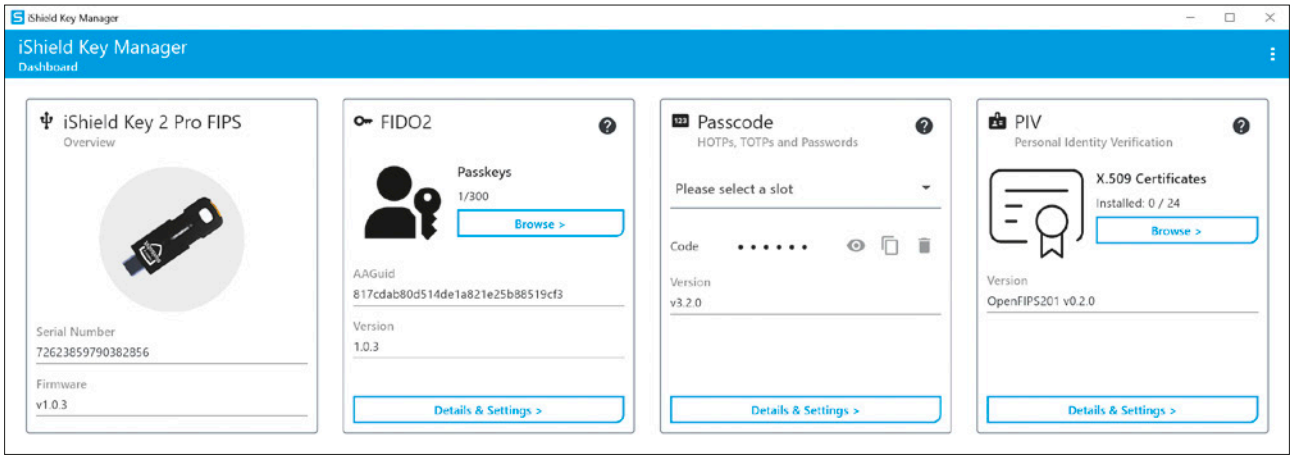
The Swissbit iShield Key 2 is an **all-in-one security key** designed for digital and physical access, as well as practical add-on features such as payment cards, digital IDs, and more.

Digital authentication: To securely log in to operating systems, websites, and online services, the hardware authenticator supports USB-A/C and NFC interfaces and complies with all relevant security standards. These include **FIDO2 / Passkeys**, a phishing-resistant protocol for protecting digital identities – supporting up to **300 passkeys** as a password alternative. Additional supported standards include **HOTP & TOTP** for generating one-time passwords and **PIV** for smartcard functionality. Smartcard-based public/private key cryptography ensures a high level of security.

Physical access: To control access to restricted areas, the iShield Key 2 supports technologies such as **MIFARE DESFire EV3, HID SEOS**, or **LEGIC advant/neon** – including options for implementing custom applications based on the MIFARE stack.

Efficient management

Once the iShield Key is connected to a computer or NFC-enabled mobile device, it can be configured using the **iShield Key Manager** (iKM). The iKM is compatible with Windows, macOS, and iOS, as well as Linux and Android devices (Android and iOS only with TOTP functionality).



MIFARE: More than just access control

The **iShield Key 2 with MIFARE support** is based on an **NXP chip** and offers much more than just access control. Its powerful platform enables the implementation of useful custom applications based on MIFARE technology. Possible use cases include time tracking, payment for cafeteria services, and membership or campus ID cards.

Secure and flexible all-in-one key

Digital authentication

Benefits of the iShield Key 2

- **Plug-and-play:** Compatible with a wide range of services (Google, Microsoft, AWS, ...)
- **Passwordless:** Stores up to 300 passkeys
- **Mobile:** Tap-and-go authentication via NFC-enabled mobile devices
- **Multi-protocol support**
  - FIDO2 / Passkeys
  - OATH-HOTP (Standard RFC4226)
  - OATH-TOTP (Standard RFC6238)
  - PIV

&

Access control

Benefits of the iShield Key 2

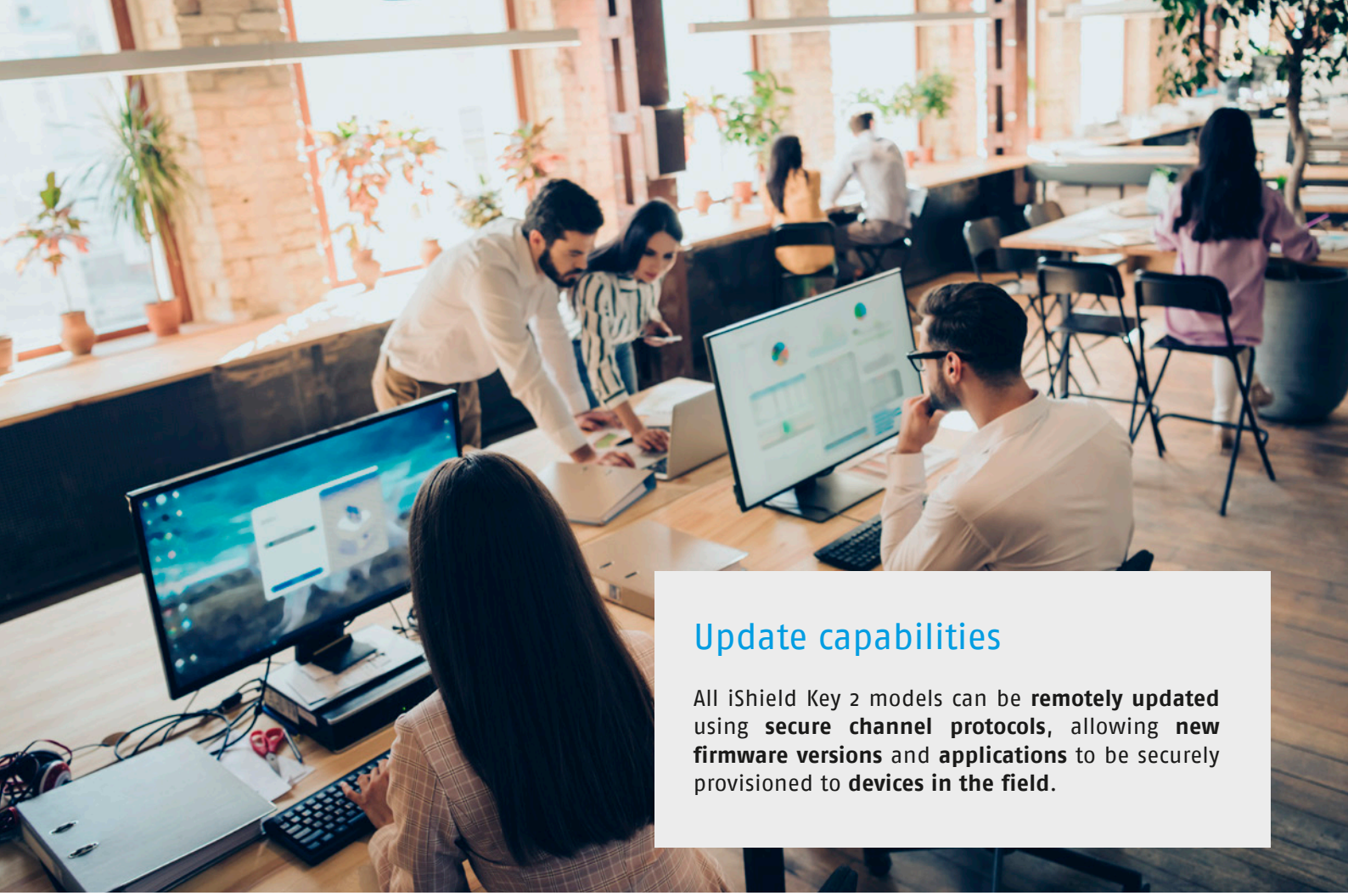
- **Optional technologies** for specific requirements in enterprises and public authorities
- **Durable:** Robust and water-resistant
- **Handy:** Slim, lightweight design with keyring
- **Supported technologies**
  - MIFARE DESFire EV3 (NXP)
  - HID SEOS (optional)
  - LEGIC advant/neon (optional)

Security & certifications

To meet the highest security requirements of enterprises and public authorities, the Swissbit iShield Key 2 is **FIDO**-certified and optionally available with **FIPS 140-3 Level 3** certification. For open smartcard integration, the security key is also **OpenSC-compatible**. A version with **FIDO Enterprise Attestation** is available as well, enabling organizations to ensure that only trusted, company-issued FIDO keys can access their systems.



Feature	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 capabilities

All iShield Key 2 models can be **remotely updated** using **secure channel protocols**, allowing **new firmware versions** and **applications** to be securely provisioned to **devices in the field**.

2-in-1 for maximum security and efficiency

With the iShield Key 2, security professionals can manage both digital and physical access with a single, robust, and user-friendly all-in-one key. The result: **higher security, reduced IAM and overall costs, and improved usability across the organization or agency.**

Sounds interesting? Take the next step and future-proof your authentication strategy – with a simple, flexible, and standards-compliant solution made to the highest quality standards, data privacy-ready, and proudly Made in Germany.

swissbit®

Have questions about the iShield Key 2 or a specific use case? Get in touch!

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

About Swissbit

Swissbit AG is the leading European technology company for data storage and security solutions. Our vision is to build a connected world where data and identities are trusted, ensuring digital sovereignty.

Founded in 2001, Swissbit operates offices in Switzerland (HQ), Germany, the USA, Japan, and Taiwan, and maintains its own semiconductor production facility in Berlin, Germany.

www.swissbit.com

www.swissbit.com/ishield-key

Made in Germany