DATASHEET

RSA iShield Key 2 MIFARE Series, Powered by Swissbit

ONE SECURITY KEY FOR EVERY DOOR, EVERY APP, EVERY ENDPOINT

Badge in. Log in. Same tap.

Most organizations deprovision physical and digital access separately—different teams, different systems, different timelines. That gap is a risk. The RSA iShield Key 2 MIFARE models, powered by Swissbit, are the only FIDO-certified security keys that support the MIFARE physical access standard. Building entry, cafeteria payments, desktops, SaaS, VPNs, and legacy systems, all protected by one rugged key.

Integrate iShield Key 2 MIFARE with **RSA® ID Plus** and your organization gains NIST AAL3 hardware authentication—phishing-resistant, hardware-based MFA that protects sensitive data and intellectual property with a solution capable of adapting to evolving threats. One vendor. One policy engine. Phishing-resistant access for everyone, everywhere, even when offline.

FIDO passkey and multi-protocol support

The iShield Key 2 offers secure, passwordless authentication with FIDO passkey, smart card, and OTP support for legacy compatibility. Whether your organization needs to secure access, safeguard remote work, or protect sensitive data, the RSA iShield Key 2 MIFARE provides versatile and resilient authentication. Key features include:

- Unified digital AND physical access: Built-in MIFARE and FIDO support lets users tap the same key at building entrances, clock in and out, make cafeteria purchases, and access desktops, legacy systems, and SaaS portals. Ideal for financial services organizations, healthcare, energy, and other highly regulated organizations.
- Stop phishing: FIDO and PIV smart card support provide strong, phishing-resistant authentication, protecting enterprise systems from credential theft—with capacity for 300 stored passkeys and 24 smart card credentials.
- Lifecycle savings: Secure, field-updatable firmware adds new features and fixes issues without hardware recalls or re-enrollment. Cut replacement cycles. Eliminate re-registration costs.
- Audit-ready out of the box: Aligns with NIS2, DORA, US EO 14028, and NIST SP 800-63-4 AAL3 hardware authentication guidance.
- End-to-end identity protection: Integrates with RSA ID Plus, giving you full control over your IAM strategy.

Phishing-resistant passwordless access for optimal Zero Trust maturity

Eliminate credential-based threats while driving your organization toward the highest levels of Zero Trust maturity. The RSA iShield Key 2 provides robust, hardware-based, phishing-resistant, passwordless authentication that ensures only trusted, authorized users gain access to critical systems, helping enterprises achieve their Zero Trust goals.

RSA iShield Key 2 MIFARE Series Benefits

- **One tap, everywhere**: swipe through turnstiles and log into desktop or cloud apps with the same key. Passwordless for everyone, everywhere, every time.
- **Zero Trust identity protection**: RSA ID Plus integrates a range of identity security capabilities—including **contextual, risk-based authentication**, **mobile passkeys**, and **ID verification**—to advance ZTA and protect every component of your organization.
- **Ruggedized form factor**: Fully molded, robust, and waterproof housing.

RSA iShield Key 2 MIFARE Series benefits

- Physical and Logical Access. One Authenticator: Provision one authenticator instead of separate security and access cards, cutting onboarding time and lost badge tickets.
- Reduce hardware inventory: Retire separate proximity cards and reduce replacement spend.
- Privacy built-in: Cryptographic keys never leave the authenticator.
- Secure end-to-end supply chain: From semiconductor chips to assembly to dropship, all in a single factory.
- Self-service with ID Plus: End users can easily register, update, and manage their credentials with ID Plus My Page—minimizing the burden on IT teams while enhancing the user experience.

Specifications

Supported standards / features	FIDO2 / WebAuthn / CTAP2.1, FIDO Universal 2nd Factor (U2F)/CTAP1, OATH HOTP OTP (Event-based), Smartcard (PIV-compatible), MIFARE DESFire EV3 OpenSC-compatible for non-management PIV operations, Swissbit provided iShield-specific OpenSC mini driver (LSA signed by Microsoft) for PIV management, USB 2.0
Dimensions and weight	USB-A: 65 x 16 x 5.2 mm, 5g USB-C: 60 x 16 x 5.2 mm, 5g
Form factor / device type	USB 2.0 Composite Device: HID FIDO, CCID Smartcard, HID keyboard, USB-A or USB-C, VID: 1370, PID: 0911 Near Field Communication (NFC) interface and multi-color LED
Certifications	FIDO2 CTAP 2.1 Level 2, FIDO Universal 2nd Factor (U2F/CTAP1) Level 1
Operating temperature range	Storage: -25°C to 85°C Operational: -25°C to 70°C
Multi-platform support	Operating Systems: Windows 10/11, macOS, iOS, iPadOS, Linux, Chrome OS, Android Browsers: Firefox, MS Edge, Google Chrome, Apple Safari
Storage	Holds 300 FIDO passkeys and 24 smart card certificates
Secure element	NXP P71D600 running JCOP 4.5
Water resistant	IP68 compliant

About RSA

The AI-powered RSA Unified Identity Platform protects the world's most secure organizations from today's and tomorrow's highest-risk cyberattacks. RSA provides the identity intelligence, authentication, access, governance, and lifecycle capabilities needed to prevent threats, secure access, and enable compliance. More than 9,000 security-first organizations trust RSA to manage more than 60 million identities across on-premises, hybrid, and multi-cloud environments. For additional information, visit our website to **contact sales**, **find a partner**, or **learn more** about RSA.

RSA