RSA

DATASHEET

RSA iShield Key 2 Series, Powered By Swissbit

Secure, compliant authentication

One key. Nothing to steal. Nowhere for the attack to land

RSA iShield Key 2 Series, powered by Swissbit, eliminates the credential entirely. Authentication happens on the device—a cryptographic proof of possession, not a secret that travels across a network. No shared secret. No replay attack surface. No way to phish what was never transmitted.

Integrated with **RSA® ID Plus**, iShield delivers phishing-resistant, hardware-based multi-factor authentication (MFA) across your entire enterprise—protecting sensitive data and intellectual property with a solution built to adapt as threats evolve.

FIPS 140-3 Level 3. Not because it's required. Because Level 2 is no longer enough

The RSA iShield Key 2 Series is built on a FIPS 140-3 Level 3 certified cryptographic module (certificate 4679), the second highest overall security level available under the current NIST standards, and meets the NIST AAL3 hardware authenticator requirement. For enterprises operating under the most demanding compliance mandates, this isn't a feature. It's the baseline you've been asked to reach.

Every user. Every system. A hardware authenticator that doesn't expire

RSA iShield Key 2 Series delivers phishing-resistant, passwordless authentication with FIDO Passkey, smart card, and OATH OTP support across modern and legacy environments.

- **No hardware recall:** No re-enrollment. Field-updatable firmware pushes security fixes and new features to deployed units. Your hardware investment doesn't expire when standards evolve
- **300 stored passkeys**: Enterprise-scale FIDO passkey capacity without re-registration overhead
- **Phishing-resistant by design**: FIDO passkey and PIV smartcard authentication eliminate credential-based attacks. No shared secret to intercept, replay, or steal
- **Flexible usage**: Modern FIDO passkey and . PIV smart card authentication are available via USB or contactless NFC. OATH HOTP. Modernpasswordless, certificate-based smart card, and OTP for legacy systems via USB or contactless NFC
- **Versatile by design**: Compatible with legacy and modern systems across financial services, healthcare, energy, and other highly regulated organizations
- **End-to-end identity protection**: Integrates with RSA ID Plus, giving you full control over your IAM strategy
- **Built for the field**: Fully molded, robust, and waterproof housing

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 series provides robust, phishing-resistant, passwordless authentication that ensures only trusted, authorized users gain access to critical systems, helping enterprises achieve their Zero Trust goals.

Benefits

RSA ID Plus and the RSA iShield Key 2 series provide key benefits to organizations, including:

- **Enterprise-grade security and compliance**: FIPS 140-3 certified cryptographic module, ensuring compliance with global security standards
- **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
- **Seamless passwordless experience:** With FIDO2 certification, the RSA RSA iShield Key 2 series supports a secure and frictionless passwordless journey across all your protected resources

Benefits

- **Control and flexibility**: Manage and deploy passkeys with ease, tailored to the specific needs of organizations
- **Secure Self-Service capabilities with ID Plus**: End-users can easily register, update, and manage their credentials with ID Plus minimizing the burden on IT teams while enhancing the user experience

Specifications

Supported standards / features	FIDO2/CTAP2.1,/WebAuthn, FIDO Universal 2nd Factor (U2F) / CTAP1, OATH HOTP OTP (Event-based),HOTP (Event), Smartcard (PIV-compatible), USB 2., OpenSC-compatible, and USB 2 OpenSC-compatible for non-management PIV operations, Swissbit provided iShield-specific OpenSC mini driver (LSA signed by Microsoft) for PIV management.
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 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	FIPS 140-3 certified secure element **(certificate 4679)** FIPS 140-3 smart chip certified, FIDO Universal 2nd Factor (U2F/CTAP1) Level 1, FIDO2 CTAP2.1 Level 12
Temperature Range	Storage: -25°C to 85°C ExtendedOperational: -25°C to 70°C
Multi-platform support	Operating Systems: Windows 10/11, macOS, iOS, iPadOS, Linux, Chrome OS, Android Browsers: Firefox, MS Edge, Chrome, Apple Safari
Storage	Holds up to 267 300 FIDO passkeys and 24 smart card certificates
Secure element	NXP P71D600 running JCOP 4.5
Water resistant	IP68 compliant