RSA

DATASHEET

RSA iShield Key 2 Series for Federal Agencies

Nearly all federal and governmental agencies, both civilian and defense, trust RSA to secure the most critical systems—from civilian compliance mandates to DOD enforcement of phishing-resistant MFA requirements. Whether protecting classified information or securing federal networks, RSA® ID Plus for Government is your go-to solution for robust, compliant authentication.

Integrating the RSA iShield Key 2 with RSA ID Plus for Government provides U.S. federal agencies, contractors, and systems integrators with yet another method of secure authentication. Employing a FIPS 140-3 Level 3 certified cryptographic module (certificate #4679) that supports both the FIDO2 and PIV Smart Card standards, the RSA iShield Key 2 FIPS models ensure that government systems are protected and compliant with White House Executive Order (EO) 14028, OMB M-22-09, and OMB M-24-14, which require federal agencies to secure cloud services, develop and implement Zero Trust Architecture (ZTA), and deploy phishing-resistant multi-factor authentication (MFA). Together, the iShield Key 2 FIPS and the RSA ID Plus platform support these efforts, delivering robust security compliance by default with solutions that are secure by design.

One key. Every clearance level. Every mandate.

The RSA iShield Key 2 Series delivers secure, passwordless authentication aligned with NIST digital identity guidance and federal phishing-resistant MFA initiatives. The solution supports FIDO2 passkeys, OATH HOTP OTP, and PIV smart cards, providing flexible and resilient authentication across a wide range of government use cases. Federal agencies can rely on RSA to secure access for remote workers, personnel operating in classified environments, and privileged administrators accessing critical systems.

- **FIPS 140-3 Level 3 certified**: The iShield Key 2 FIPS employs a FIPS 140-3 certified cryptographic module (Overall level: 3, and a Physical Security level: 4, certificate #4679), one of the highest levels of cryptographic certification available. FIPS 140-3 certification is now required for all new federal deployments, with NIST setting September 21, 2026 as the date after which FIPS 140-2 modules move to Historical status.
- **No hardware recalls**: Secure, field-updatable firmware lets users apply new features and bug fixes to deployed units without replacing and re-registering hardware authenticators.
- **300 resident passkeys**: Holds 300 FIDO passkeys and 24 smart card certificates—three times the passkey capacity of leading alternatives.
- **Phishing-resistant**: FIDO passkeys and PIV provide strong, phishing-resistant authentication, protecting federal systems from credential-based attacks.
- **Smart card functionality**: PIV support offers secure, tamper-resistant storage for digital certificates and credentials.
- **Compatible** with both legacy and modern systems, providing broad support for all agency applications.
- **End-to-end identity protection**: Easily integrates with the FedRAMP-authorized RSA ID Plus for Government, giving you full control over your IAM strategy. Enhances federal-private sector collaboration, ensuring secure access and compliance with federal mandates.
- **Flexible usage**: FIDO passkey and PIV smart card are available via both USB and contactless NFC. OATH HOTP OTP is available via USB.
- **Ruggedized form factor**: Fully molded, robust, and waterproof—built to withstand the environments federal personnel actually work in.

Benefits

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

- **Compliance with federal standards**: FIPS 140-3 certified cryptographic module, meeting the latest U.S. government requirements for cryptographic security.
- **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 iShield Key 2 series supports a secure and frictionless passwordless journey across all federal systems.
- **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.

RSA iShield Key 2 benefits

RSA ID Plus and the RSA iShield Key 2 provide key benefits to federal agencies, including:

- **Compliance with federal standards**: FIPS 140-3 Level 3 certified cryptographic module (certificate #4679), meeting the highest U.S. government requirements for cryptographic security. Aligns with EO 14028, OMB M-22-09, OMB M-24-14, and NIST SP 800-63B AAL3 hardware authentication guidance.
- **A capable alternative to CAC for modern federal environments**: The RSA iShield Key 2 FIPS supports PIV smart card, FIDO2, OATH HOTP OTP, and multi-protocol authentication—meeting the same use cases required of hardware authenticators across federal civilian and defense environments. RSA ID Plus, already trusted by 90% of U.S. federal agencies, delivers the identity platform to match.
- **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 iShield Key 2 series supports a secure and frictionless passwordless journey across all federal systems.

RSA iShield Key 2 specifications

Supported standards / features	FIDO2/ WebAuthn/CTAP2.1, FIDO Universal 2nd Factor (U2F)/CTAP1, OATH HOTP OTP (Event-based), Smartcard (PIV-compatible) 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 Level 3 secure element (certificate 4679), FIDO Universal 2nd Factor (U2F/CTAP1), FIDO2 Level 1
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, 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

RSA is the identity standard for government agencies, finance, and high-assurance organizations. RSA provides the identity intelligence, authentication, access, governance, and lifecycle capabilities needed to prevent threats, secure access, maintain operations, and surpass 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.