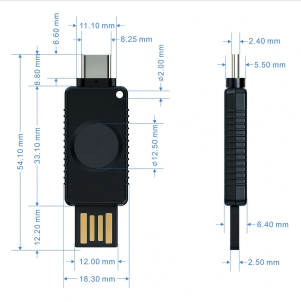
TOKEN2 Sàrl
Geneva, Switzerland
www.token2.com

Token2 PIN+Bio3 R3.4 FIDO2 Security Key with Biometric Authentication - PIV & NFC version

Part no: T2F2Bio3R3.4 · T2-129







Description

The **Token2 PIN+ Bio3** is a **FIDO2 security key** with USB-A, USB-C and NFC, designed for strong, phishing-resistant authentication. Featuring a high-resolution, round fingerprint sensor (ø12.5mm), it enables fast and secure PIN + biometric login when connected via USB. Over NFC, the key works with the PIN only. The key includes a **leather protective case** to shield the fingerprint sensor from physical damage and wear. Even among the most rugged biometric devices, exposed sensors are vulnerable to impact and contamination — the included case ensures long-term reliability.

Where the fingerprint works

The fingerprint sensor works only via USB, and only with FIDO2, PIV and OTP. In every other case the key is used with the PIN.

	USB (USB-A / USB-C)	NFC
FIDO2 / Passkeys	Fingerprint or PIN	PIN only
PIV	Fingerprint or PIN	PIN only
OTP	Fingerprint or password	Password only
OpenPGP	PIN only	PIN only

How NFC works: tap the key on the phone or NFC reader and enter the PIN on that device when asked. The fingerprint sensor is not active over NFC: touching it during a tap has no effect, and there is no fingerprint prompt.

Why no fingerprint over NFC? Over NFC the key has no power source of its own: it is powered entirely by the energy its antenna picks up from the phone or reader. A key of this size can only hold a small antenna, and the energy it collects is

enough to run the secure chip but not the fingerprint sensor, which needs considerably more power to capture and match a fingerprint. Over USB the key is powered by the port, so the sensor is fully available. This is a physical limitation of the compact key format, not a software setting, and it cannot be changed by configuration.

If you want to sign in with your fingerprint on a phone or tablet, connect the key to its USB-C port instead of tapping it. NFC cannot be switched off, and the PIN always remains available as a verification method.

Fingerprint storage and reset

Fingerprints are enrolled and stored in the FIDO2 part of the key (up to 29 fingerprints, PIN required to enrol or manage them). PIV and OTP do not keep their own fingerprints: they rely on the ones enrolled for FIDO2.

- **Resetting FIDO2 erases all enrolled fingerprints.** The reset does not delete your OTP profiles or PIV certificates, but fingerprint verification stops working for PIV and OTP as well, because the fingerprints are gone.
- After a reset, set a new FIDO2 PIN and enrol your fingerprints again.
- **For PIV, the fingerprint has to be bound again** after the fingerprints are re-enrolled. Until then, PIV works with the PIN only.

Fingerprints can be enrolled and managed with the tools listed on our Tools for FIDO security keys page.

New in Release3.4

- **PIV Applet:** NIST SP 800-73-5 compliant PIV with RSA2048, RSA3072 and RSA4096 keys, and Secure Messaging (encrypted communication) over NFC.
- **Fingerprint beyond FIDO2:** when connected via USB, fingerprint verification can now unlock OTP profiles and, with the latest Token2 minidriver, be used for smart card logon to Windows workstations. **OpenPGP is not covered: it uses the PIN only.**
- **Protected OTPs:** TOTP and HOTP profiles can be protected with a password or fingerprint, with a security lockout after 100 failed attempts and a 5-minute authenticated session.
- **HOTP Support:** HOTP (SHA-1 / SHA-256) is now available alongside TOTP.
- **NFC:** the key can be used over NFC with PIN verification only (the fingerprint sensor is not active over NFC).
- **FIDO2:** user verification is always required by default (always_uv), and passkeys can be managed over USB on iOS.
- **OpenPGP Applet:** updated applet with broad compatibility with OpenPGP software for secure digital signing, encryption, and authentication. OpenPGP operations are protected by the PIN; the fingerprint sensor is not used for OpenPGP.
- **USB-C:** improved compatibility with certain devices and high-voltage protection for docking stations.

Manage Passkeys and Fingerprints

No special software is needed to start using the key. For managing passkeys, fingerprints, OTP profiles and certificates on Windows, macOS, Linux, Android and iOS, see our **Tools for FIDO security keys** page.

Technical Specifications

Feature	Details
Interfaces	USB-A, USB-C, NFC (PIN only)
Firmware	FIDO 2.1 Token2 PIN complexity enforcement Release3.4
Authentication Protocols	FIDO2 / WebAuthn, PIV, OpenPGP, OATH TOTP / HOTP
User Verification	Fingerprint: via USB only, and only for FIDO2, PIV and OTP NFC: PIN only (fingerprint sensor not active) OpenPGP: PIN only on both interfaces
Passkey Storage	Up to 300 credentials always_uv enabled by default
OTP Profiles	Up to 50 entries (TOTP and HOTP, SHA-1 / SHA-256) Optional protection by password or fingerprint (fingerprint via USB only); lockout after 100 failed attempts
HOTP Support	Supported (HID-HOTP disabled by default)
PIV	NIST SP 800-73-5 compliant RSA2048, RSA3072, RSA4096 Secure Messaging over NFC Windows smart card logon with fingerprint (USB, Token2 minidriver)
OpenPGP	RSA2048, RSA3072, RSA4096 secp256r1, secp256k1, secp384r1, secp521r1 ed25519, x25519 User Interaction Flags (UIF), Key Derived Function (KDF) **PIN only, no fingerprint verification**
Fingerprint Sensor	Round, 14mm diameter, 508 DPI resolution
Verification Time	~0.9 seconds
False Acceptance Rate (FAR)	< 0.0001%
False Rejection Rate (FRR)	~1%
Max Fingerprints Stored	29 (stored in the FIDO2 applet; erased by a FIDO2 reset)
Included Accessories	**Leather protective case**

Compatibility & Use Cases

For supported platforms, services, and usage examples, visit our overview page:

Token2 FIDO2 Key Overview & Compatibility Guide

Why Choose Token2 PIN+ Bio3?

- Secure biometric authentication over USB, with PIN fallback
- USB-A and USB-C with fingerprint, plus NFC with PIN, for broad device support
- FIDO2, PIV, OpenPGP and OTP on a single key
- Up to 300 passkeys and 50 OTP profiles
- Fingerprint for passkeys, OTPs and Windows smart card logon (via USB; OpenPGP uses the PIN)
- Includes leather case to protect the fingerprint sensor

Fingerprint verification is available via USB only, and only for FIDO2, PIV and OTP.

Over NFC the key always asks for the PIN, never the fingerprint. OpenPGP always uses the PIN. Please ensure your device has a USB-A or USB-C port if you want to use the fingerprint sensor.

Biometric sensor

The Token2 Bio3 runs our FIDO2 L2-certified PIN+ firmware and features the same biometric sensor as used in our previous Bio and Bio2 models. Certification of the biometric component follows a separate assessment process, which is currently underway. With Release3.4, fingerprint verification applies to FIDO2, OTP and PIV (Windows smart card logon with the Token2 minidriver) when the key is connected via USB; over NFC all of these use the PIN. **The fingerprint is never used for OpenPGP, on any firmware release.** Please note that for devices running firmware earlier than R3.4 the biometric protection only applies for FIDO2 protocols, not OTP nor PGP

OpenPGP works with the PIN, not the fingerprint

The fingerprint sensor cannot be used to unlock or authorise OpenPGP operations (signing, decryption, authentication), neither over USB nor over NFC. OpenPGP keys are protected by the OpenPGP PIN. If User Interaction Flags (UIF) are enabled, the key asks for a simple touch to confirm presence: any finger works, and the touch does not verify your fingerprint. This limitation comes from the open-source SmartPGP applet our implementation is based on, not from our hardware.

LED indicator

The PIV and OpenPGP applets are enabled by default. While either of them is enabled, the LED may stay on constantly when the key is plugged in. This is normal behaviour of the smart card (CCID) interface.

Specifications

GENERAL	
Form factor	Plastic case
Interface	USB-A, USB-C
CONNECTIVITY	
USB-A	Yes
USB-C	Yes
NFC	Yes

Smart card	No
OTP	
OTP protocols	TOTP
TOTP	Yes
FIDO	
U2F	Yes
FIDO certification	L2
Minimum PIN policy	6 digits, complexity enforced
OpenPGP support	Yes
Biometric	Yes
AAGUID	eabb46cc-e241-80bf-ae9e-96fa6d2975cf
DIMENSIONS	
Dimensions	54.1 × 18.3 × 6.4