TOKEN2 Sàrl
Geneva, Switzerland
www.token2.com

Token2 Pico - RP2350-Based FIDO2 Security Key

Part no: pico · T2-114









Description

Warning: This device is intended for developers and FIDO enthusiasts. It is **not recommended for production use**—using it in such environments is possible, but at your own risk. Some services, such as AGOV or ID-Austria, are **not compatible**, and others, such as Microsoft Entra ID, **require advanced configuration**.
A compact and affordable **FIDO2 / WebAuthn security key** based on the Raspberry Pi **RP2350** microcontroller. Designed for phishing-resistant authentication, development, testing, and everyday secure logins. Ideal as a **primary or backup hardware key** for users who want standards compliance without premium secure-element pricing.

The firmware is based on a modified open-source fork of the pico-fido project, and the hardware is openly designed and documented

about pico-fido project

Key Highlights

- FIDO2 / WebAuthn compliant (CTAP1 & CTAP2)
- Passwordless and phishing-resistant authentication
- Physical button for user presence verification
- Preloaded firmware, user-upgradeable
- Open and developer-friendly design
- Excellent price-to-performance ratio
- Fully manageable with Token2's open-source tools (FIDO2/passkey and OTP)

Management Tools

This key can be fully managed using Token2's open-source tools, covering both **FIDO2 / passkey** and **OTP** management:

- • **Token2 Companion - Rust edition (Keyroost)** – cross-platform desktop tool for Windows, macOS, and Linux.
  Keyroost

- • **Libre Key Companion** – Android app (a USB-A to USB-C adapter may be needed).
  Libre Key Companion

Technical Specifications

Specification	Details
Product Type	FIDO2 / WebAuthn Security Key
Microcontroller	RP2350 (Dual-core ARM Cortex-M33 + RISC-V)
Interface	USB-A
Authentication Standards	FIDO2, WebAuthn, CTAP 1 & 2
User Presence	Physical button
Firmware	Pre-installed, upgradeable
Secure Element	No
Attestation	Not supported
Supported OS	Windows, macOS, Linux
Management Tools	Keyroost (desktop), Libre Key Companion (Android)
Typical Use Cases	Passwordless login, 2FA, development, backup key

System Compatibility

- AGOV – Not compatible
- ID-Austria – Not compatible

- Entra ID – Requires disabling attestation checks
- Other systems – Check with us before ordering

Good to Know

This device does **not** include a hardware secure element or attestation, making it best suited for **general use, development, and controlled environments**, rather than high-assurance enterprise deployments. Both FIDO2/passkey credentials and OTP profiles can be managed using **Token2 Companion - Rust edition (Keyroost)** on desktop and the **Libre Key Companion** Android app.

Specifications

GENERAL	
Form factor	Bare PCB (USB-A)
Interface	USB-A
CONNECTIVITY	
USB-A	Yes
USB-C	No
NFC	No
Smart card	No
FIDO	
U2F	Yes
FIDO certification	Not certified
Minimum PIN policy	6 digits, complexity enforced
Biometric	No
DIMENSIONS	
Dimensions	19×7×2.4