TOKEN

TokenCore.com

Wearable identity. Cryptographic certainty.

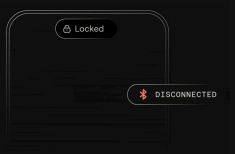
TokenCore™ Wearable is the only biometric-enforced, cryptographic identity wearable that proves human presence at every login, in real time. For organizations operating in high-consequence environments — trading floors, critical infrastructure, defense, healthcare — the cost of identity failure is not theoretical. TokenCore™ Wearable eliminates the conditions under which failure occurs.

Legacy MFA authenticates credentials. Not humans.

When attackers already have passwords and MFA codes, they log in. PAM secures credentials. Passkeys sync to the cloud. USB keys prove device presence. None prove that the authorized individual is present at the moment of access. TokenCore™ Wearable solves this problem.

HOW IT WORKS

Authentication rebuilt for the human. Zero friction.



1	Presence Detected	2	Identify Verified	3	Crypotgraphy Executed
Bluetooth proximity (3ft) confirms you are physically there.		Your fingerprint unlocks the device (EAL5+) locally, on-device		A domain-bound credential is generated and signed ES256 elliptical curve cryptography.	

Built for environments where failure is not an option.

Wireless by Design

BLE 5.4 and encrypted NFC eliminate USB friction. Works across iOS, Android, Windows, and macOS without drivers or middleware.

FIDO2 / WebAuthn Certified

Fully compliant with FIDO 2.1, including FIDO U2F and FIDO2 protocols. Delivers phishing resistant, passwordless authentication at enterprise scale.

EAL5+ Secure Element

Credentials are stored in a tamperproof, hardware-certified secure element. No network path, no cloud exposure — the ring is the vault.

Full IAM Interoperability

Integrates with Okta, Microsoft Entra, and Ping within hours. No middleware, no rip-and-replace. Deploys alongside the identity stack already in place.

Upgradable Firmware

Security posture evolves without hardware replacement. TokenCore™ Wearable is the only wearable authenticator offering OTA firmware upgrades — future proofing the investment.

Operational in 30 Days

Pilot and initial rollout complete without replacing existing infrastructure. User enrollment takes 10–15 minutes with guided setup and direct support.

TOKEN

TokenCore.com

TARGET ENVIRONMENTS

Designed for high-stakes access.

TokenCore™ Wearable is deployed in environments where a compromised identity has direct operational, financial, or safety consequences

Financial Services

Trading floors, wire authorization, and privileged system access where a single fraudulent session can result in eight-figure losses.

Healthcare

Clinical systems, EHR access, and pharmaceutical controls where patient safety depends on verified human identity at point of care.

Aerospace & Defense

CMMC Level 2 compliance, privileged infrastructure access, and classified system authentication for defense contractors and federal agencies

Critical Infrastructure

Operational technology and SCADA environments where remote compromise carries physical consequences.

TokenCore™ Wearable Technical Specs

Battery Life	5-7 days
Charge Time	90 minutes (fully charged), 5 minutes recovery charge
Secure Element	EAL5+ verified, tamper resistant
Credential Storage	100 FIDO credentials
Connectivity	BLE 5.4 + NFC, encrypted, touch enabled
Platform Compatibility	iOS, Android, Windows, MacOS

Durability Rating	IP67 rated
Security Standard	FIDO2 / WebAuthn
Fingerprint Sensor	Capacitive, FIDO2-compliant
Cryptography	ES256 elliptic curve (domain-bound)
Biometric Storage	On-device only (never transmitted)
Firmware	Over-the-air upgradeable

BUSINESS VALUE

Identity assurance drives measurable outcomes.

TokenCore™ Wearable shifts the identity conversation from risk mitigation to capability enablement. Organizations gain the ability to prove human presence — the answer cyber insurers, regulators, and boards are requiring.

Cyber Insurance

Satisfies phishing-resistant authentication mandates. Reduces premium exposure from 50–100% increases carriers are applying to organizations without hardware identity controls.

CMMC Compliance

Meets cryptographic identity requirements for CMMC Level 2 certification, accelerating defense contractor qualification.

Helpdesk Cost Reduction

Eliminates password reset volume and MFA fatigue incidents. Reduces operational overhead across privileged user populations

Zero Trust Enablement

Provides the cryptographic identity layer that Zero Trust architectures require but traditional MFA cannot deliver.

Make Identity Absolute

SOC Certified • FIDO2 Certified

Identity is the last control that cannot fail.