Token

Product Brief

BioStick Series

Stop Ransomware & Phishing with Next-Generation MFA

Phishing-Resistant

Phishing-resistant MFA eliminates the risk of account compromise by blocking phishing attempts, legacy MFA vulnerabilities, and man-in-the-middle attacks.

Secured with Biometrics

If a security key is lost or stolen, biometric verification ensures that only the registered user can utilize it. This stops cybercriminals even if they have possession of the key.

Field Upgradability

Token's BioStick can be easily updated in the field, ensuring it remains a cutting-edge tool in an enterprise's security arsenal, unlike other security keys.

The Future of Enterprise Authentication is Passwordless

Organizations of all types require a secure, passwordless login experience that provides the highest level of assurance and user convenience. This is the most effective way to stop phishing attacks and the escalating damages from ransomware and data breaches. Token's BioSticks deliver strong, next-generation MFA security and convenience.

Moving Beyond Legacy MFA

Next-generation MFA fixes the shortcomings of legacy authentication methods, including vulnerabilities to phishing, man-in-the-middle attacks, sim-swapping, and reliance on users to recognize threats.

Legacy MFA is a hassle for users, but the Token BioStick offers a simpler, passwordless login experience by replacing multiple steps with just a quick fingerprint scan.

Token offers a secure, scalable, and phishing-resistant solution, integrating all the benefits of hardware security keys with the flexibility of software-based management.

Compared to simple 2FA hardware security keys, Token BioSticks can only be used by their owner's fingerprint, making them highly secure validating the user at every login.

BioStick Highlights

Biometric and PIN-based authentication

FIDO authentication via USB, BLE or NFC

Tamper-Proof Secure Element for safe storage of credentials and biometrics

FIDO2/WebAuthn and FIDO U2F protocols

Works with Windows, MacOS, Android and iOS*

USB-rechargable

* The availability of non-USB connectivity is subject to the platform's compatibility.

TOKEN BIOSTICK FEATURES AND OPTIONS

	 Token BioStick	 **Token BioStick Plus**
USB-C	✓	✓
Bluetooth		✓
NFC		✓
Fingerprint and PIN Authentication	✓	✓
FIDO2 Compliant	✓	✓
FIDOU2F	✓	✓
Upgradable Firmware	✓	✓

Two Models. One Seamless User Experience.

Both models in the Token BioStick series are fully field-upgradable, work seamlessly with the same applications and the Token software platform and offer a consistent user experience across the board. This ensures that regardless of which Token BioStick is chosen, users and enterprises benefit from the same great features and ease of use.

The key difference between the models lie in their connectivity options. The base Token BioStick offers only USB connectivity, the Token BioStick Plus adds Bluetooth functionality and NFC capability. Additionally, the Plus has an internal, rechargeable battery to make it fully functional even when not connected to a USB port.

Technical Specifications

- Charges via 5V USB-C connection
- Operating Temperature: 0°C to 60°C (32°F to 140°F)
- Charging Time: Approximately 2 hours
- Tamper-Resistant Secure Element supports up to 100 unique resident keys/credentials
- 508 DPI capacitive fingerprint sensor
- BLE 5.4
- Battery Life: Lasts up to one week between charges
- Immediate Usability: Operates whenever plugged in, regardless of battery charge level

Authentication Use Cases: SSO and Passkeys

A common way to implement FIDO authentication and security hardware is to utilize these hardware authenticators to safeguard existing instances of single sign-on (SSO) or identity provider-based authentication. This approach offers the convenience that enterprise customers have sought for provisioning, deprovisioning, and managing access while simultaneously protecting, with the utmost security, control of these systems of authentication. Given the centralization of SSO and IDP systems, it is imperative for organizations to protect access to these systems.

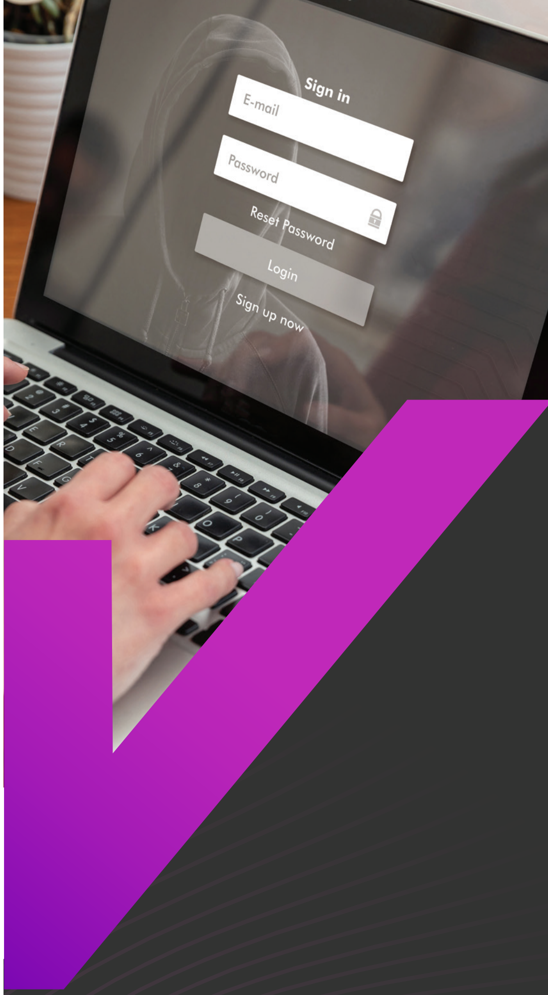
Additionally, a growing range of enterprise products and services are now supporting FIDO-based Passkeys for direct authentication between an end user and a relying party. Now, end users of Token hardware products have the flexibility to choose either (or both) as a deployment strategy that aligns with their organization's needs.

Token Prevents Ransomware

Ransomware payouts are rising dramatically with the average ransomware payment increasing 500% year-over-year.

These attacks can manifest in various ways, but most begin with the unauthorized disclosure of sensitive credentials such as passwords or two-factor authentication (TOTP) codes, or even the installation of malicious software.

Next-generation hardware devices, such as the Token BioStick, securely store and generate private keys for end-users, ensuring that they remain inaccessible to unauthorized parties, and there is nothing for the end user to accidentally divulge. Hardware security keys benefit from not being networked, eliminating the risk of remote accessibility and potential attack. Consequently, all sensitive data is protected within this secure hardware, while only public-key data is transmitted or stored on external servers, avoiding a centralized credential store that can become an attractive target for threat actors.



Ransomware payouts are rising dramatically year over year with

$1B+

in payments in 2023.[2]

The deployment of FIDO security keys resulted in **zero account takeovers, four times faster logins**, a **92% reduction in IT work calls** and a **95% reduction in password resets**.[1]

Reduction of IT Support Needs

Token hardware products are designed to address enterprise IT requirements in two distinct ways:

1. **Token BioSticks mitigate the risk of ransomware and data breaches resulting from inadequate authentication methods, including legacy forms of multifactor authentication (MFA).**
2. **Token BioStick authenticators significantly reduce the frequency of password resets, a common IT support request.**

Studies conducted by Google, Hyper, and others have demonstrated that the deployment of FIDO security keys resulted in zero account takeovers, four times faster logins, a 92% reduction in IT work calls and a 95% reduction in password resets.[1]

Designed for Mass Deployment

Organizations can manage their Token security hardware keys using the Token Authenticator Console. It offers seamless key management, ordering, shipping, and return processing. Administrators gain comprehensive access to hardware assignments, status updates, logging information, and the ability to customize Token security hardware for specific groups without compromising the security of biometric authentication or private keys.

[1] https://www.chainalysis.com/blog/ransomware-2024/.
[2] https://FIDOalliance.org/statistics-sources/.

fido CERTIFIED FIDO2

About Token

In a world of stolen identities and compromised user credentials, Token is changing the way our customers secure their organizations by providing passwordless, FIDO2 compliant, biometric, multifactor authentication. To learn more, visit **www.tokenring.com**.