Data Sheet

# Passkey:YOU

No phones. No tokens. No problem.

## What are Passkeys?

Passkeys are a new type of login credential that allows you to log in to sites and services without entering a password. They aim to provide greater security to all your accounts by using passwordless authentication, with each passkey being a unique digital key that cannot be reused. They're built on the FIDO2 WebAuthn standard, which uses public-key cryptography to protect your data and accounts better. Best of all, passkeys eliminate the need for passwords.

## Why Passkeys?

In a nutshell, passkeys are more secure – and easier to use – than passwords and many traditional authentication methods. Most security breaches can be traced back to compromised and/or phished passwords. As the cybersecurity community addressed this problem by implementing strong authentication solutions, cyber-attackers also evolved. They increased the sophistication and frequency of their attacks, putting many first-generation strong MFA options like OTPs and Push Notifications under attack. Passkeys are a major upgrade for both security and usability, in the following ways, specifically:

### (1) Passkeys Are More Convenient

Passwords can be shared, forgotten, stolen, and phished. By replacing the burdensome password approach with a simple biometric scan, synced passkeys allow users to:

- Automatically access their FIDO log-in credentials across multiple devices.
- Easily recover passkeys if devices are lost.

Additionally, a Google study revealed how much quicker the login process is with passkeys vs passwords: 14.9 seconds on average with passkeys and 30 seconds on average with passwords.

The convenience and usability are just half of the story, however. The security component of passkeys is leaps and bounds superior.

### (2) Passkeys are Phishing-Resistant

The use of public key cryptography is a game-changer. With passkeys, the user's private key is securely stored on his or her device, and the organization only stores the user's public key – rendering the information unvaluable to any bad actors attempting to execute theft. Between this and the end-to-end encryption, passkeys drastically reduce risk and exposure to attack for both users and admins.

### (3) Implicit, Strong MFA

MFA naturally requires two or more authentication factors across something you have, something you know, and something you are. Because passkeys are kept on a user's device and can only be executed by that user via FIDO-approved authentication methods, they implicitly satisfy the requirements for multi-factor authentication and provide a major upgrade over more traditional methods, like magic links and OTPs.

BIO-key®

## What Is Passkey Authentication With BIO-key's Identity-Bound Biometrics?

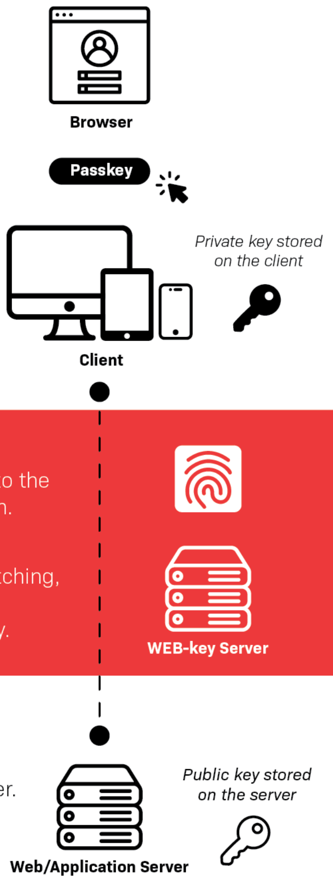
**No phones. No tokens. No problem.**

Passkey:YOU is an innovative authentication solution that makes using passkeys to eliminate passwords simple and effortless. It leverages the FIDO standard's newest capabilities to allow a user to authenticate to any software or service relying party with only a touch of a finger instead of carrying a hardware token or mobile device. Best of all – it can be easily and quickly integrated into existing technology stacks.

## How BIO-key Passkey Authentication Beats Out the Competition: The Identity-Bound Biometrics Advantage

BIO-key's Passkey:YOU is the best of both worlds: a software approach secured by strong, FIDO-compliant biometric authentication. It provides an innovative biometrics-based passkey that enables compliance-ready security while delivering an enhanced user experience and excellent value. With low-friction integration and deployment, you can spend less time on security management and focus more on what matters most: your core business.

- It is the only passwordless authentication solution that does not require the use of phones or hardware tokens.
- Enterprise-controlled enrollment prevents unauthorized users and account handovers.
- BIO-key's Passkey:YOU can be layered directly into industry-standard IDPs. If you want to add advanced, easy-to-use, technology to your existing infrastructure investment, we offer a low-friction, high-speed deployment that works hand in hand with it. Have an enterprise IDP already? No problem – seamless integration.


Browser
Passkey
Private key stored on the client
Client
WEB-key Server
Public key stored on the server
Web/Application Server

1 The user navigates to a site through a browser and is prompted by a login field.

2 The user clicks a button to initiate passkey authentication.

3 BIO-key WEB-key server notifies the client to begin the biometric authentication process.

4 The user places their finger on the fingerprint reader, which is then sent to the WEB-key server for a fingerprint match.

5 WEB-key performs biometric data matching, returning the user's information with industry-leading accuracy and security.

6 If the fingerprint match is confirmed, the private key is unlocked and used to sign the authentication challenge provided by the Web/Application server.

7 The Web/Application server accepts and completes the log on event.

## Supported Authentication Methods

Flexible Options For All Users

### BIO-key WEB-key

WEB-key is a comprehensive, multi-tenant, enterprise IBB management platform built around one of the world's most accurate and scalable biometrics engines. It has achieved the highest independently tested and verified NIST benchmarks for fingerprint identification speed and accuracy.

### BIO-key MobileAuth™

The only multi-factor authentication app to offer IBB authentication options. MobileAuth safeguards access to critical data, and offers multiple, easy to use authentication methods to choose from – including palm scanning and facial recognition.

### Hardware

BIO-key offers a variety of fingerprint scanners in various form factors for use with our IAM solutions, as well as support for Microsoft Windows Hello scanners.

Fingerprint Scanners

- ✓ SideSwipe
- ✓ SidePass
- ✓ SideTouch
- ✓ PIV-Pro
- ✓ EcoID II
- ✓ Pocket10

POS Terminal

- ✓ MobilePOS Pro

BIO-key®

# *Passkey:YOU – Fusing the uncompromising security of FIDO-compliant authentication with software's user-first approach everyone loves.*

## Key Benefits of Passkey:YOU

### Security

*Our biometrics-based approach avoids the shortcomings of many software authentication solutions, including the vulnerability to be hacked.*

– **Secure the data.** Centrally managed, enterprise-grade biometrics are fully encrypted. That means they're immune to dangerous attacks like man-in-the-middle and replay attacks.

– **Don't make the sacrifice.** We marry the security of biometric authentication with the low cost and convenience of software passkeys to ensure users get the best of both worlds, both in terms of deployment and capital.

– **Get the easy win.** Why leave yourself open to attack with a single point of failure? With Passkey:You, physical devices are removed as potential vulnerabilities so it isn't even a concern.

### Cost & Efficiency

*In today's business world, efficiency is everything – so why pay more and do more if you aren't getting more? Passkey:YOU empowers your organization to stay laser focused on top priorities while always keeping budget top-of-mind.*

– **Streamline your operations** – and your budget. Eliminates the need for cumbersome hardware tokens.

– **Don't pay more to get less.** BIO-key's Passkey:YOU cuts lifecycle costs by 50 – 70% compared to hardware tokens (and provides stronger security).

– **Let us handle the compliance.** Critical business operations and security protocols should be top of mind for you – not the ins and outs of industry and/or government compliance. Passkey:YOU is built compliance-ready so you can focus on what really matters to the organization while never needing to worry about increased cyber insurance fees or dropped coverage.

### Flexibility & Familiarity

*Authenticating shouldn't feel like a chore, or an accomplishment. We believe it should be a quick and easy step in the process; one that you don't even need to think about.*

– **Cater to everyone, always.** Phones and hardware tokens aren't always the answer. When they're not, you can turn to BIO-key's Passkey:YOU to ensure all users can easily and securely authenticate how they want to.

– **Enroll once, authenticate anywhere.** Whether they're using a desktop on Monday and a tablet on Wednesday, a single, one-time enrollment enables access anywhere. Your users will thank you for the convenience.

– **No ripping, no replacing.** Passkey:YOU is easily integrated into existing tech stacks, systems, applications and infrastructure.

## Ideal Use Cases for Passkey:YOU

- Passwordless workflows
- Roving users & shared workstations
- Zero-trust frameworks
- Remote workforce
- Mobile devices not permitted
- Customer IAM