BIO-key®

Phone-less. Token-less.
Less is More for Passwordless Authentication

According to the World Economic Forum, weak and/or stolen passwords are the most common initial attack vector, representing 80% of all breaches. However, with 82% of business leaders saying they are ready and willing to implement a passwordless approach, it's clear that organizations across industries have recognized the glaring flaws of password-based authentication and are ready to move past it.

Moving away from the password-based authentication method is a step in the right direction – but the answer isn't always straightforward. Unfortunately, most passwordless options take a step backwards in terms of security by relying on tokens, devices or phones to execute the authentication process as a single factor. The core challenges with these methods include:

High Costs + Investments

Traditional passwordless methods typically require the purchasing of multiple tokens for each employee or separate mobile devices or data plans.

Insufficient Security

Trust is based on the device or token, both of which can be shared, lost or stolen, and not able to authenticate the actual person completing an action.

Implausible or unsafe for core business areas

Key groups, functions and use cases within organizations are hindered by methods that impose inefficient or unsafe work conditions on daily operations, which, in turn, can pose legal risk for the employer.

Ready to discover a better way to go passwordless? Keep reading to see how you can eliminate passwords – no phones or tokens required.

Passwordless Authentication with Identity-Bound Biometrics

Passwordless authentication with Identity-Bound Biometrics uses the person as the credential for authentication. With a simple scan of a finger at any device in any location, it is the safest, most efficient, most cost-effective, and most secure option for a range of scenarios and business-critical operations across industries.

The key benefits include →

BIO-key®

Phone-less. Token-less.
Less is More for Passwordless Authentication

Key Benefits of Passwordless with IBB

1 SECURITY

Positively identify the person completing an action with authentication powered by Identity-Bound Biometrics, ensuring the intended user and only that user - is gaining access.

2 PROCESS VALIDATION

Ensure that only authorized people are the ones completing steps or taking actions within a process or transaction. For example, this is extremely valuable for quality assurance on a manufacturing floor or to verify the clinician who prescribed a controlled substance.

3 EASE OF USE

Save countless hours and increase productivity with a consistent, frictionless user experience that's quick and easy, requiring just one-touch authentication for a passwordless login at each workstation - no mobile device, token or username necessary.

4 COST EFFICIENCY

Reduce your overall cost by installing just one fingerprint scanner per device for a minimal, one-time investment and eliminate the need to purchase multiple tokens or cover the cost of mobile devices.

When authentication is tied directly to the user's identity, you can experience passwordless authentication in its purest form, unencumbered by devices: phone-less and token-less.

Passwordless authentication with Identity-Bound Biometrics is an approach that you can trust because it is rooted in proven, tried-and-true pillars of cybersecurity - introducing less points of attack means less potential risk and vulnerabilities. When cybersecurity is built on assumptions - as it is with device-based passwordless methods - your private information becomes far more difficult to reliably protect.

Interested in learning more about passwordless authentication with Identity-Bound Biometrics? Visit us online at www.BIO-key.com to find helpful resources like datasheets, case studies, demo videos and FAQs. From there, you can also easily reach out to our professional and knowledgeable sales team to learn about taking the next step.