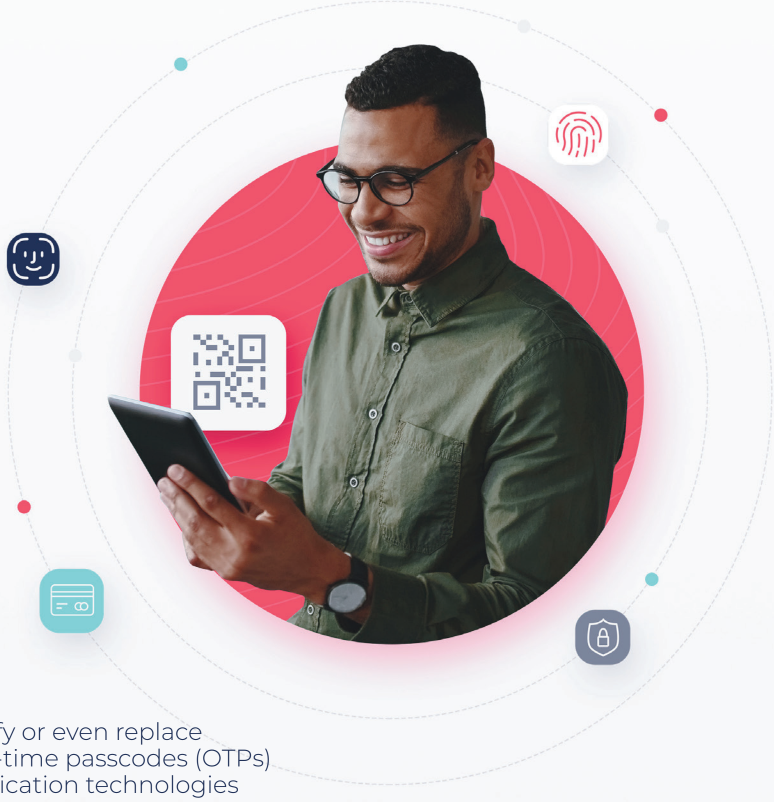
transmit security

DATASHEET

Bind ID™

The Only Mobile App-less Authenticator



Many of the various technologies that were designed to fortify or even replace passwords are no longer effective. Email and text-based one-time passcodes (OTPs) have proven vulnerable and even the best of today's authentication technologies can be bypassed using security gaps created by improper configurations and weak device registration processes.

Dedicated mobile apps with biometrics deliver strong user authentication, but they struggle to be adopted by customers. They also present security challenges if devices are replaced or the application has to be reinstalled.

BindID: The Future of Customer Authentication

BindID is the industry's first app-less, self-binding mobile authenticator that uses strong device-based biometrics for accurate, reliable and consistent authentication across every channel. With one-click to sign into existing accounts, BindID eliminates passwords and the inconveniences of traditional credential-based logins.

App-less Biometric Mobile Authentication

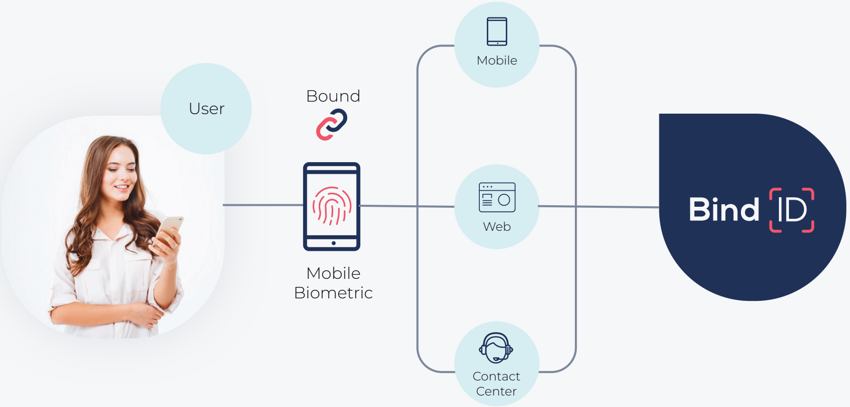
Biometric mobile authentication is a trusted and secure method to validate users, however it's only of use if a user has downloaded an application to their phone for authentication. BindID's innovative approach ties together strong FIDO-based biometrics such as fingerprint and facial recognition with an advanced real-time trust engine for true, secure 2-factor authentication without the need for deployment and maintenance of a mobile app.

- **Secure 2-factor authentication**
- **One-click, passwordless login**
- **No application to download**
- **Automatic device bind/rebind**
- **Consistent cross-channel experience**

Feature	Benefit
Biometrics without an app	Secure 2-factor authentication without the need for users to download a mobile app
One-click authentication	No user ids, no passwords, and no hassles for users to worry about
Consistent across channels	Reduce confusion and eliminate security gaps with a single, secure authenticator for web, mobile, and the call center
Network of trust	Always up-to-date user information and automatic device rebinding with shared user profiles

Frictionless Authentication without Passwords

BindID eliminates the hassles of remembering or resetting password-based credentials. Users simply scan their face or fingerprint to authenticate. From there BindID takes over to accurately match and validate the user with their BindID profile then returns the result.



BindID provides a consistent, secure authentication experience across all channels in an organization

One Authenticator for All Your Channels

Whether from the web, mobile devices or even a call center, BindID provides a consistent experience. Using techniques including QR codes and text messaging, any application or service can use the mobile device to complete authentication in exactly the same way.

The Power of Network-Based Trust

BindID employs network-based trust at the user level and across all BindID member applications. User profiles and a network of shared trust let users associate other biometric-enabled devices such as laptops and tablets to accounts, and provides up-to-date user and device information across the entire BindID member network.

The BindID Passport

Behind the scenes every user is assigned a BindID Passport containing detailed device, location, access times, network, email address and other information used to uniquely identify them. Member organizations can request as little or as much information to authenticate the user and be sure that any personal information is safe and meets all compliance standards globally.

First-Time User Authentication

If the BindID network has never encountered a user, the service performs a thorough check of the user and the device using a series of trust checks using know-your-customer (KYC) tools like government identification checks, mobile-network operator (MNO) validation, and other services such as Google, Microsoft, and Apple. If the user passes, their device will be bound and shared across all member organizations.

Extending Trust to Other Devices

Once a user is established in the BindID network, additional biometric devices can be associated with their BindID Passport. BindID automatically detects if a device is FIDO compliant and will prompt the user to add it to their account. The next time a user logs in from a registered biometric device like a laptop or tablet, they can simply log in with a fingerprint or face scan.

Automatic Device Rebinding

One of the biggest challenges facing any biometric authentication technology today is the process to securely replace a device if it is lost, stolen, or simply upgraded. The current methods fall back on insecure practices like one-time passcodes or password-based credentials. BindID uses the trust network to automatically and securely rebind a device. When BindID detects the unknown device, it is run through the same sets of trust checks used for first-time user authentication then registers the device to the user's account. If a user has already registered another biometric device like a laptop, that can be used to extend trust to the replacement mobile device as well.

Always Up-to-Date

Organizations with infrequent user visits can leverage the power of the BindID trust network to provide the latest user and device information without having to reauthorize the user, device and biometrics all over again. No matter how often a user visits a member site, their profile will be current based on their last visit to any BindID-enabled member service across the network.

Deploy Quickly

Open standards and APIs, let organizations deploy BindID quickly in any channel. Using OpenID Connect, most development teams can have it up and running within a single agile sprint.

transmit security

transmitsecurity.com