Ubiquitous Passwordless Authentication with FIDO Passkeys

Unauthorized or fraudulent access remains the number-one attack vector and will likely remain so as long as passwords are used. In fact, compromised end-user credentials accounted for half of all data breaches in 2021, according to the 2022 ForgeRock Consumer Identity Breach Report.

Passwords not only create a security risk, they introduce unnecessary friction by forcing users to first create, then remember, strong and unique passwords. They are also expensive to maintain, as password reset calls to your help desk cost roughly $140 per user per year. These high costs are compounded by the poor experience that customers face in dealing with password-related issues, resulting in dropped transactions and lost business.

Forward-thinking organizations are taking steps to reduce their dependence on passwords. Passwordless authentication strengthens security while improving the end-customer experience with a simple, convenient, and seamless login process that involves no passwords.

By making passwordless a part of your multi-factor authentication (MFA) strategy, you not only improve the customer experience, but you also substantially limit the attack radius and strengthen your defenses against new forms of attacks, such as phishing, credential stuffing, and account takeovers (ATO), that rely on the weakness of passwords to steal valuable customer data.

FIDO Passkeys: Streamlined Passwordless Experiences for Web and Mobile Devices

Multi-device FIDO Credentials, commonly known as passkeys, were introduced in April 2022 and represent an important step forward in achieving truly seamless digital experiences that eliminate passwords. Passkeys improve usability on web and mobile devices, allowing for broad adoption of passwordless authentication on mobile phones. They enable an easy-to-use passwordless credential management system that synchronizes credentials across different devices, offering users access from anywhere and from any mobile device without ever requiring a password.

How Passkeys Work

Passkeys are based on the FIDO2 WebAuthn standard and offer the convenience and security of biometrics, such as a fingerprint or facial scan. WebAuthn eliminates the need to enter a password by utilizing private and public key cryptography for secure authentication. By being tied to the device cryptographically, they are much harder to compromise or phish than passwords, which must transit between devices and the servers to which they're connecting.

An important new capability in passkeys builds upon the current WebAuthn single-device credential support. Passkeys now enable passwordless credentials to be stored in the device provider's cloud, so they can be shared across multiple devices. This ability removes the reliance on hardware, which creates challenges when a user changes mobile devices or gets a new one.

ForgeRock Passkeys Support

ForgeRock pursues an open standards approach with built-in support for FIDO passkeys. This support provides you with extensibility and flexibility for broader and faster deployment of passwordless across mobile authenticators such as mobile phones, smart cards, biometric devices, digital certificates, and web browsers.

Key Capabilities

- Unlike solutions that require coding and upgrades to support them, the ForgeRock Identity Platform provides built-in support for passkeys without requiring any coding changes or upgrades to the platform. The platform does not distinguish between, and equally supports, both device-bound and non-device–bound passkeys.
- ForgeRock offers pre-built support (nodes) to integrate FIDO2 WebAuthn device registration and authentication in user journeys through our market-leading no-code orchestration engine.
- With passkeys already supported by ForgeRock WebAuthn nodes, they can be easily embedded in user journeys, which then steer towards different passwordless paths based on run-time signals.
- ForgeRock provides built-in support for passkeys so organizations can provide diverse passwordless authentication choices to customers, depending on the user's specific mobile device. By choosing passkeys in their authentication journey, customers can log in when they change devices or get a new one, without having to re-enroll their credentials in order to authenticate.
- App builders can turn on passkeys using a toggle in the dashboard and without touching their code.

Benefits

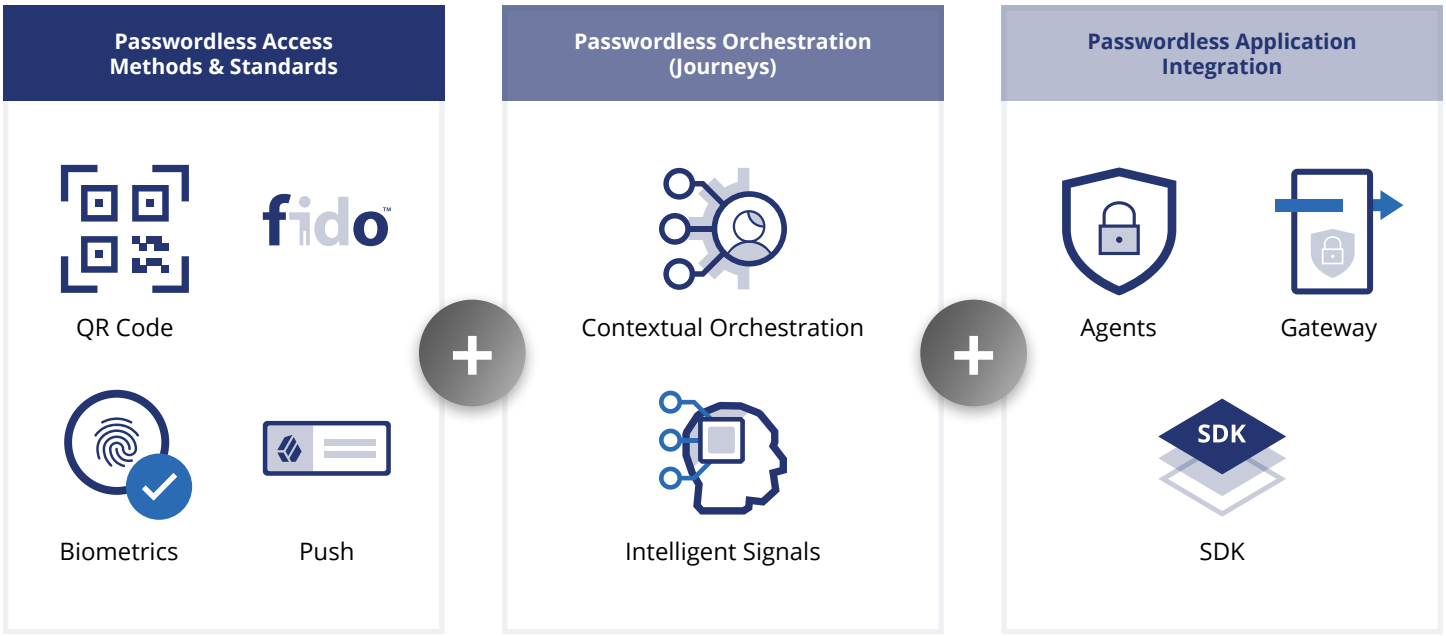
- **Strong security** – Users benefit from the strong security of ForgeRock passwordless because a password — also known as a static shared secret — is never stored or transmitted between systems.
- **Frictionless multi-device experience** – The user experience improves dramatically. Your customers get the convenience of using their mobile devices as a passwordless access credential (using passkeys that are built into the device).
- **Reduced helpdesk costs** – Forgotten or stolen password escalations to customer support go away, and the volume of help desk calls associated with passwords is reduced, resulting in operational and cost efficiencies.
- **Increased revenues** – The elimination of passwords not only improves the customer experience, but it can also reduce the number of abandoned logins, increasing transactions and revenues.
- **Easy implementation** – Pre-built support for passkeys avoids the need for costly development time; simply drag-and-drop WebAuthn nodes to create a passwordless journey with passkeys authentication.

 |

No-Code Passwordless Journeys with Passkeys

Organizations are already building no-code passwordless authentication journeys with ForgeRock **Intelligent Access**, which facilitates **journey orchestration** in the identity platform. ForgeRock provides prebuilt integrations (nodes) for the FIDO2 WebAuthn standard in ForgeRock Intelligent Access. With passkeys already supported in WebAuthn, you can offer passkeys as an authentication method to your customers, depending on a user's specific mobile device.

Building a passwordless user journey with Passkeys is quick and easy — you simply drag and drop the pre-built WebAuthn nodes and adjust the authentication journey to meet your needs. Supported in WebAuthn nodes, Passkeys are easily embedded in user journeys, which then steer towards different passwordless paths based on run-time signals from the device or risk signals based on authentication context.



About ForgeRock

ForgeRock® (NYSE: FORG) is a global digital identity leader helping people simply and safely access the connected world. The ForgeRock Identity Platform delivers enterprise-grade identity solutions at scale for customers, employees, and connected devices. More than 1,300 organizations depend on ForgeRock's comprehensive platform to manage and secure identities with identity orchestration, dynamic access controls, governance, and APIs in any cloud or hybrid environment. For more information, visit: **www.forgerock.com**.

Follow Us

ForgeRock