LexisNexis®
RISK SOLUTIONS

WHITE PAPER

Passwordless Authentication Powered by Trusona

Learn how to passkey-enable your website or application to enable your users to quickly and easily sign in to their accounts.

Introduction

It's noteworthy that passkeys are now supported on over four billion devices, including smartphones, laptops and PCs.

However, it's common for individuals to be taken aback when they discover their websites do not automatically support passkeys. Although passkeys are an industry standard and compatible with the latest iPhones running on iOS 16 and Android 9 phones, this does not automatically make a website passkey-ready.

In this guide, we aim to provide a clear answer to the question of what actions an application owner must undertake on their website to enable their constituents to log in to their accounts using passkeys.

Behind the scenes

First, let's break our website or web application into three parts:

1) Client-side

This includes the physical device, operating system and browser during the user's interaction with the website. The passkey support that is touted for this part really means that they are passkey-capable — which, in technical terms, means they support the FIDO WebAuthn protocol.

Each of the three main platform vendors are at slightly different stages of their passkey support, as follows:

- Apple: Supported today from iOS 16, iPadOS 16 and macOS 13 Ventura
- Google: Supported today from Android 9
- Microsoft: Supported today from Windows 11 as a single device passkey, with full passkey support planned for the second half of 2023

FIDO support has grown rapidly over the past few years to the point of near ubiquity. Virtually every modern computing device now has FIDO support built in.

- 93% of active browsers
- 78% of desktops/laptops
- 95% of mobile devices

With each passing month, as people upgrade and replace their phones, more and more end users will have a passkey-capable device.

For a more complete reference matrix[1].

2) Application front-end

This refers to the browser-based HTML code that comprises the application user interface as it is presented on the client-side.

To passkey-enable a website, the website developer needs to incorporate additional browser HTML code that invokes the WebAuthn protocol for the registration and authentication ceremonies as follows:

- **Registration** — During passkey registration, a unique public/private key pair is generated by the device's crypto-processor. The private key (passkey) is securely stored on the user's device and synced with the platform vendor's cloud storage solution such as Apple Keychain or Google Password Manager. Meanwhile, the public key is stored on the FIDO server in the application back-end (see below).
- **Authentication** — After registration, users log in to the website using their biometrics, such as Face ID or Touch ID. This enables secure local access to the passkey which is then used to create a digital signature that is validated with the public key on the server. This implementation is facilitated through the WebAuthn protocol and results in a simplified and more secure login experience, eliminating the need for a username and password. The user login experience needs several subtle, but important changes that increase security while simplifying the end user experience.

It is also important to instrument monitoring and performance tracking for the web front-end, in order to accurately measure and compare the benefits of passkey authentication. Such metrics could include time to register, time to sign in, sign-in success rates and other relevant data points, allowing for a comprehensive evaluation of its performance against username and password sign-ins.

3) Application back-end

In the back-end of the application, the implementation of a new entity, referred to as a FIDO Server, is necessary. The FIDO Server is responsible for the storage and management of user public key credentials and associated account information. Upon receipt of a request from the application during the registration or authentication process, the server will generate a cryptographic challenge. The authenticity of the client's signature is then verified by the server using the associated public key, thus allowing the user to successfully log in.

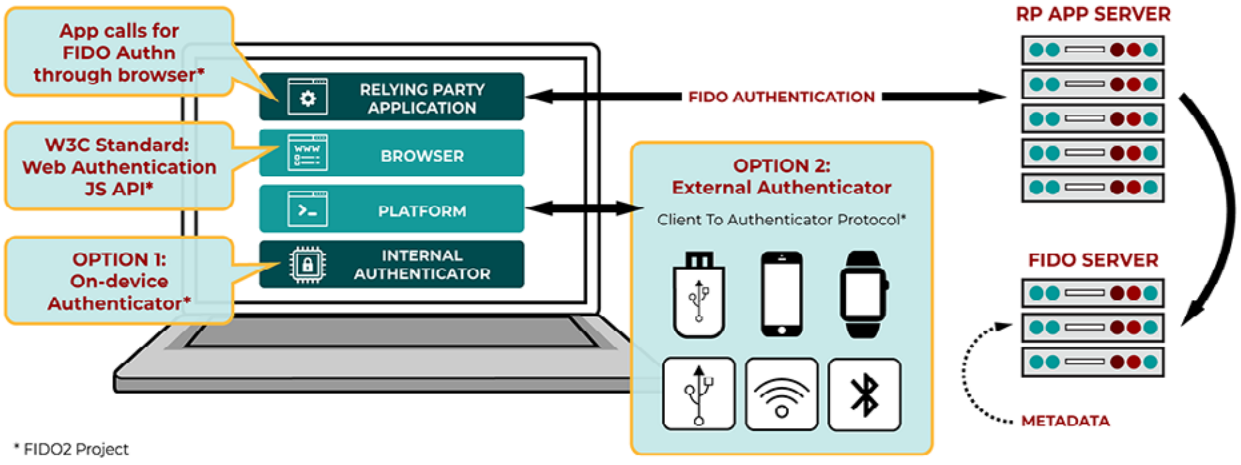
In order to effectively support the WebAuthn client, the server must meet a minimum set of requirements. These requirements include the ability to:

- Initiate a WebAuthn credential registration for a specified user, along with options for credential creation on the client side
- Complete a WebAuthn credential registration with the authenticator response from the client side
- Initiate a WebAuthn authentication for a known user or a user whose identity can be discovered from a given credential
- Complete a WebAuthn authentication with the client-side authenticator response

In addition to these minimum requirements, the server should also implement the following elements to ensure a comprehensive security solution:

- Persistence of credentials, including the capability to revoke existing credentials
- Policy enforcement mechanisms
- Auditable usage information, including registration and authentication events
- Scalability and reliability enhancements to withstand the expected number of users

The backend of the system should also be modified to incorporate a data layer integration with the enterprise analytics system. This integration will aid in the demonstration of key performance indicator (KPI) business outcomes.



The importance of user journeys and User Experience (UX)

It's crucial to acknowledge that the proper implementation of the aforementioned components is only one aspect of a successful passkey implementation project. The key determinant of success lies in the thoughtful design and effective execution of the user journeys, such as enrollment, sign-in, recovery and passkey management.

Neglecting the myriad of end user considerations can make the passkey experience unnecessarily confusing. Yet, when the user experience is thoughtfully managed, the passkey experience is radically simpler than with a username and password.

In fact, passkey success rates have been shown to yield:

- 50% reduction in the time to complete a registration (Nok Nok)[2]
- 2.6x faster vs. username and password, as reported by Yahoo!Japan (FIDO)[3]

Due to the novelty of the passkey end user experience for most website owners, there is a lack of understanding regarding the necessary modifications for optimizing the end user experience and realizing the benefits previously outlined.

Putting it all together

Passwordless Authentication Powered by Trusona is one such passkey-as-a-service platform, offering the simplest, quickest and lowest-cost way to passkey-enable your website. It improves business growth and profitability with faster, phishing-resistant sign-ins that delight your users .

The largest corporations often prefer to have full control over their entire stack, including hardware, infrastructure, software and branding. However, for many organizations, a passkey-as-a-service solution from a cloud provider is a faster, more efficient and cost-effective option, allowing them to stay focused on their core business while letting the cloud provider handle the authentication service and its intricacies.

Passkey-as-a-service: Passwordless Authentication Powered by Trusona

Passwordless Authentication is one such passkey-as-a-service platform, offering the simplest, quickest, and lowest-cost way to passkey-enable your website. It improves user experience and security with faster, phishing-resistant sign-ins that delight constituents.

Passwordless Authentication Powered by Trusona:

- Integrates quickly to your website using standard authentication protocols (e.g., OpenID Connect (OIDC))
- Provides prebuilt, curated passkey journeys based on UX best practices
- Delivers real-time analytics
- Supports both primary and secondary authentication (2FA)

LexisNexis®
RISK SOLUTIONS

For more information scan
or call 1-888-216-3544

About LexisNexis Risk Solutions

At LexisNexis Risk Solutions, we believe in the power of data and advanced analytics for better risk management. With over 40 years of expertise, we are the trusted data analytics provider for organizations seeking actionable insights to manage risks and improve results while upholding the highest standards for security and privacy. Headquartered in metro Atlanta USA, LexisNexis Risk Solutions serves customers in more than 100 countries and is part of RELX Group, a global provider of information and analytics for professional and business customers across industries. For more information, please visit www.lexisnexis.com/risk.

1. Device Support - passkeys.dev
2. Nok Nok case study, https://noknok.com/password-free-authentication-with-intuit-fido-authentication/
3. Yahoo! Japan case study: https://fidoalliance.org/yahoo-japans-password-free-authentication-reduced-inquiries-by-25-sped-up-sign-in-time-by-2-6x/