# Build vs. Buy: A Guide To Deploying Passkey-Based Authentication

Evaluating the best strategy for your digital business

TRUSONA

trusona.com/contact

# Contents

# Overview

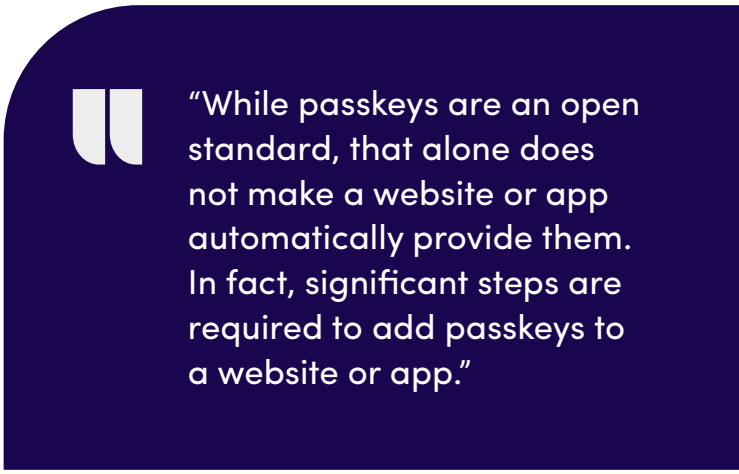
According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), passkeys are poised to become the "gold standard" of authentication for the internet — replacing passwords and legacy 2FA such as OTP over SMS that lack security, usability and cost-effectiveness.

While passkeys are an open standard, that alone does not make a website or app automatically provide them. In fact, significant steps are required to add passkeys to a website or app.

When considering a passkey implementation, organizations face the choice between developing a solution themselves ("build") or purchasing a ready-made, off-the-shelf solution ("buy").

This whitepaper outlines the key requirements for implementing passkeys and explores the advantages and disadvantages of both approaches, providing digital businesses with the ability to make an informed decision regarding the best option for their business. A successful passkey implementation means a better customer experience, more revenue and strong security.

# An Introduction to Passkeys




Passkeys represent one of the most significant advancements on the internet since the emergence of web browsers in the mid-90s. Passwords on the other hand are a source of endless user friction, are universally disliked and are no longer effective in protecting user identities and accounts.

Passkeys serve as a convenient alternative to passwords and OTPs, enabling faster, more successful and more secure sign-ins across all of a user's devices. Like the unlocking of a smartphone, passkeys rely on the same biometrics (e.g., Touch ID and Face ID) or PIN that the user has set up. Their usage brings significant security advantages too, as they offer robust protection and are phishing-resistant.

Thanks to industry leaders such as Apple, Google and Microsoft, passkeys have become widely adopted, supported on billions of devices, including smartphones, tablets, laptops and desktop computers. For example, Google now offers passkeys to its 1.8 billion Gmail customers and it's a matter of time until all websites and apps offer them to their users. These companies collaborate within the FIDO Alliance, an open industry association dedicated to advancing passkey technology.

In today's digital landscape, the customer experience (CX) is now a primary differentiator for leading brands. A great CX is no longer a 'nice to have' — it's a requirement for business success. As such, passkeys differentiate and empower businesses by simplifying the CX, fueling increased user engagement and cultivating heightened brand loyalty.

Embracing passkeys enables digital businesses to streamline the processes of account creation and sign-in, leading to notable improvements in customer engagement. Passkeys can reduce sign-in times by 50% and elevate the first-time sign-in success rate to almost 100%.

The benefits of passkeys extend beyond the customer and positively impact the business too. Passkeys can decrease user abandonment and attrition rates, boost customer lifetime value (LTV), and fortify security. They effectively thwart large-scale hack attacks, minimizing the risk of account takeovers and phishing incidents. And since they are multi-factor credentials, passkeys eliminate the need for SMS one-time passcodes (OTP) and mitigate account lockouts, leading to reduced costs and improved operational efficiency.

Many prominent digital brands across multiple industries — including CVS Health, eBay, Google, Hyatt, Kayak, PayPal, Shopify and The Home Depot — have already embraced passkeys, further highlighting their value and effectiveness.

# Requirements for Adding Passkeys to Your Website

To add passkeys to a website, a comprehensive set of requirements must be met, including the following:

## 1) Set up a FIDO server

To enable passkeys on a website, a FIDO server is necessary on the back-end. The FIDO server manages user public key credentials and the associated account information. During registration and authentication, the server generates a cryptographic challenge and verifies the client's signature using the public key.

The FIDO server must be able to support the WebAuthn protocol for implementing the registration and authentication ceremonies. Additionally, it should also support security elements such as credential persistence, policy enforcement and event logging.

Ideally, the server should be FIDO2-certified which means it can accept any FIDO2-certified authenticator, irrespective of its manufacturer.

## 2) Develop client-side support of the WebAuthn protocol

The website must incorporate additional browser-based HTML code that utilizes the WebAuthn protocol for the registration and authentication ceremonies.

During registration, a unique public-private key pair is generated by the device's crypto-processor hardware. The private key (passkey) is securely stored on the user's device and synchronized with the platform vendor's cloud storage solution, such as Apple iCloud Keychain or Google Password Manager. Simultaneously, the public key is stored on the FIDO server in the application's back-end.

Once registered, users can 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.

## 3) Implement a multitude of new passkey user journeys

As CX is a critical success factor, the key determinant of passkey adoption lies in the thoughtful design and effective execution of the new passkey-related user journeys, such as:

- Creating a new account with a passkey
- Creating a passkey from within an existing account
- Creating a passkey during the forgotten password or account recovery process
- Signing in with a passkey

> "The key determinant of passkey adoption lies in the thoughtful design and effective execution of the new passkey-related user journeys."

Neglecting these end-user considerations makes the passkey experience unnecessarily confusing and impedes adoption.

Considerations should also include codifying the recommended best practices from FIDO's UX Guidelines, which identify the three most successful places to prompt users to create a passkey, as well as designing the user journeys, priming, graphics and overall UX for the 40 or so other user touchpoints required for a typical consumer use case.

It's also important to recognize that end-users demand flexibility with their sign-in modalities. This means that the added passkey support must also seamlessly integrate with other authentication modalities such as legacy two-factor authentication (2FA) and hardware security keys. Examples include:

- Usernames/passwords
- Email with OTP
- SMS with OTP
- Usernames/passwords followed by passkeys as a second factor
- Hardware security keys (e.g., YubiKey)
- Authenticator apps (e.g., Microsoft Authenticator, Google Authenticator) with support for OTP and push notifications

The bottom line is that to achieve success in implementing these user journeys and authentication flows, extensive user research and usability testing is required.

## 4) Provide passkey management settings for the end-user

When implementing passkey support on a website, it is also essential to update the user's account settings to enable them to conveniently view and manage their passkeys. This entails providing them with the ability to access a list of their registered passkeys for the website along with other pertinent data such as the time of registration, the operating system and browser. This is comparable to the concept of allowing users to view their own trusted devices.

It is also important to give users the option to permanently delete their passkeys from the website back-end should they want to revoke them. Although passkeys are phishing-resistant, implementing this best practice contributes to robust security measures and instills a sense of trust with the end-user.

## 5) Perform device compatibility checks & journey logic adaptation

While the vast majority of devices are now passkey-compliant, it's important to recognize that there will always be some devices that do not support passkeys. This can be due to several reasons, including:

- Usage of an older device lacking the necessary crypto-processor hardware
- Utilizing a modern device with an outdated version of the operating system (passkey support was initially introduced in iOS 16 and Android 9)
- Employing a specific browser version that is not up to date and compatible with passkeys
- The user has not set up the biometric capabilities or unlock features on their device
- The user has not enabled the pre-requisite features on their device (e.g., iCloud Keychain on their Apple device or Windows Hello on their PC)

Checking that a given user device is passkey-compliant therefore relies on a combination of the hardware, operating system version, browser version, and user device settings. And due to the nuanced passkey implementations across different browsers, features such as passkey autofill may yield different experiences.

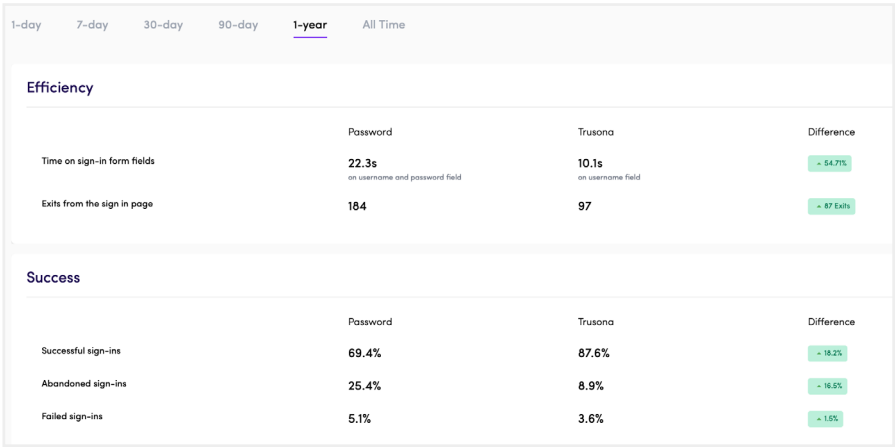
Consequently, a comprehensive set of real-time checks and tests should be conducted before every sign-up and sign-in action to determine passkey compatibility. Additionally, alternate user journeys should be implemented to gracefully handle those cases where a passkey cannot be used.

## 6) Instrumentation of performance metrics and audit logs

In order to accurately measure and compare the benefits of passkey authentication over existing password-based sign-ins, it is considered a best practice to instrument monitoring and performance tracking on the website front-end. These metrics can be instrumented using JavaScript tags and can be collected, stored and analyzed.

Such metrics should include:

- Account creation success rate
- Average time to create an account
- First try sign-in success rate
- Overall sign-in success rate
- Average time for successful sign ins
- Average time for abandoned sign-ins
- Average time for failed sign-ins



Additionally, every registration and authentication event should be logged with appropriate meta data which can later be used for troubleshooting and diagnostics or in support of compliance mandates such as audit trails.

## 7) Access to analytics and reporting systems

As noted above, the various data points collected need to be stored and managed in a repository so they can be used for reporting and analytics. This data can help provide visibility and insights into customer adoption and usage of passkeys compared with passwords to help highlight and quantify the improved levels of customer engagement.

## 8) Connectors & interfaces for integrating into existing enterprise systems

The additive passkey infrastructure will require multiple touchpoints into the existing system architecture. These include:

- Integrating into the enterprise Identity Provider (IdP) to implement user validation and access controls. Commonly supported authentication protocols include OIDC and SAML.
- Integrating into the enterprise analytics system to aid in the demonstration of key performance indicator (KPI) business outcomes.
- Transmitting security alerts into a Security Information and Event Management (SIEM) system to obtain real-time analysis of security alerts.

As such, various enterprise connectors and interfaces need to be in place to facilitate the data transfer between these systems.

## 9) Available, reliable and scalable infrastructure

The authentication function holds significant importance as a mission-critical component of any system. With the potential for millions of authentication events taking place each month, it becomes paramount to ensure that the new passkey-based infrastructure is not only available but also highly reliable and scalable.

- Availability refers to the ability of the infrastructure to remain accessible and functional at all times. Downtime or disruptions in the sign-in process can lead to frustration, loss of user trust, and potential financial implications for businesses.
- Reliability goes hand in hand with availability, emphasizing the consistency and dependability of the passkey-based infrastructure. A reliable infrastructure ensures that authentication events can be completed successfully, providing a seamless and trusted user experience.
- Scalability is a crucial aspect when dealing with a large volume of authentication events. Scalability ensures that the system can efficiently process authentication requests, regardless of the number of concurrent users or the intensity of the workload.

By prioritizing these aspects, businesses can establish an enterprise-grade system that consistently guarantees successful user sign-in experiences, even under high usage scenarios.

## 10) Ongoing maintenance (hardware, software, networking, etc.)

Many businesses find the ongoing maintenance of a successful passkey-based infrastructure difficult as it involves various activities to ensure the smooth functioning of hardware, software, networking and the addressing of any bugs or vulnerabilities. Key aspects of ongoing maintenance include:

- Hardware monitoring and periodic upgrades of the physical or virtualized infrastructure such as servers, storage devices and networking equipment.
- Software updates and patching to address bugs, add new features and improve performance.
- Security measures such as regular security audits and vulnerability assessments to identify and mitigate security risks.
- Performance monitoring and optimization of the system to identify bottlenecks, optimize resource utilization and ensure optimal user experience.
- Data backups and disaster recovery to safeguard critical information and ensure business continuity.

# Comparing Build vs. Buy

Digital businesses can passkey-enable their websites using a build or buy approach. The following table provides a high-level summary comparison of the two:

| | Build | Buy |
|---|---|---|
| **Cost** | Headcount, consultants, hardware, software and networking infrastructure | Licenses, services — typically lower than build |
| **Time-to-value** | +/- Months / years | +/- Weeks |
| **Resources** | Headcount, UX skills | Few / none |
| **Control** | Total control | Limited control |
| **Maintenance** | You build it, you maintain it | Done by vendor |

# When to Build

The largest brand name companies often prefer to have full control over their entire stack, including the physical or virtualized hardware, infrastructure, software and branding. Outsourcing the authentication competency to a 3rd party is viewed as a higher risk from an operational perspective. These companies tend to possess substantial financial resources and enjoy extensive access to a wide range of human resources and expertise.

Resources typically required for a passkey implementation include:

- Developers
- UX designers
- QA testers
- Web analysts
- Hardware managers
- IT operations personnel

A word of caution — the user journeys for a passkey implementation require thorough research and testing and will often be the determining factor between success (user adoption) and failure.

Note also that there are tools available today to help make the build process a little easier — although the organization will still need to tie these independent modules together into a cohesive entity.

Some examples of these include:

- Open-source FIDO servers
- SDK toolkits offering passkey capabilities
- OIDC/SAML connectors
- Orchestration and workflow engines
- Cloud computing services such as IaaS and PaaS

# When to Buy

For most organizations, the buy option is the most attractive and simple. A passkey-as-a-service solution from a cloud provider is a faster, more efficient and cost-effective option, which allows companies to stay focused on their core business while letting the cloud provider handle the authentication service and its intricacies.

Businesses who adopt this approach are typically cloud-first organizations looking for time-to-market advantages over their competitors and don't view authentication as a core competency of their business. They also view passkeys as an opportunity cost, meaning that time spent focusing on passkeys would be time not spent on other strategic opportunities.

Additionally, as CX is a critical success factor in passkey adoption by customers, organizations are often best served to seek cloud providers that are more experienced in curating thoughtful passkey user journeys and stay up-to-date on best practices from FIDO's UX Guidelines.

# Checklist of Questions to Help You Determine Build vs. Buy

The following questions should be used to help guide you to the best approach for your business:

| Item | Build | Buy |
|---|---|---|
| **Is there urgency to deploy passkeys?** | No | Yes |
| **Is authentication a core competency?** | Yes | No |
| **Do you need complete control over the passkey stack, including the FIDO architecture, user journeys and experiences?** | Yes | No |
| **Do you have the resources to plan, design, build, and manage the passkey stack over the coming years?** | Yes | No |
| **Do you have the necessary expertise in UX and user journeys for supporting passkeys?** | Yes | No |
| **Do you have a legacy or bespoke IDP architecture that doesn't support SAML or OIDC?** | Yes | No |

# Passkey-as-a-Service With Trusona Authentication Cloud

Trusona Authentication Cloud is a 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 customers.

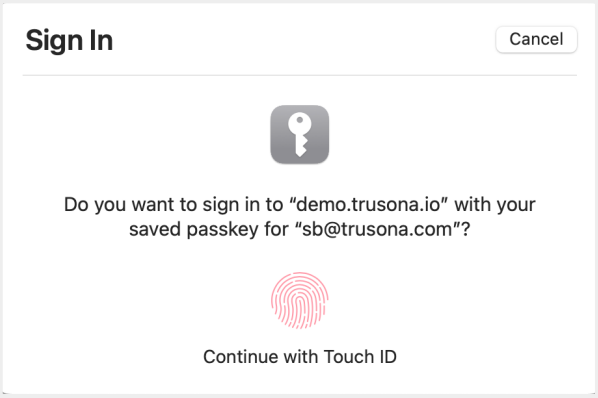
Trusona Authentication Cloud:

- Includes a highly scalable, integrated FIDO2-certified server
- Integrates quickly to your website IdP using standard authentication protocols (e.g., OIDC)
- Provides prebuilt, curated passkey journeys based on FIDO UX best practices, along with a tool for customized branding and styling, known as Journey Builder
- Delivers real-time analytics to show the improved user engagement compared with passwords
- Supports a wide range of authentication modalities, including primary and secondary authentication (2FA)
- Includes an SDK to supplement the out-of the-box capabilities for additional flexibility and control

## Business benefits

### Fastest time-to-value, minimal deployment risk

- Generally within 4-12 weeks
- Almost no CX and developer resources required
- Built-in user journeys leverage Trusona's passkey expertise




### Increase revenue

- Higher account creation conversion rate
- Higher customer lifetime value (LTV)

### Lower costs

- Eliminate SMS OTP costs for 2FA
- Reduce account fraud and theft
- Lower call center and user support costs

### Happier users

- Increased user engagement
- Lower attrition and abandonment
- Higher retention, lifetime value

# Passkey Requirements Checklist

| Item | Build |
|---|---|
| **FIDO server** | The back-end server responsible for managing the user public key credentials and cryptography services against the client. |
| **Client-side WebAuthn support** | The FIDO Alliance protocol that enables a user to register and sign in with a passkey through browser-based HTML code using public-private key pairs. |
| **Passkey user journeys & UX** | The most difficult and time-consuming aspect of any passkey implementation. Involves the thoughtful design of all the user journeys, such as new account creation, sign-in, account recovery and passkey management. Requires extensive research and usability testing. |
| **Passkey management settings for the end-user** | User account settings should be updated to allow convenient passkey management, including viewing and deleting them. This enhances security and instills user trust. |
| **Device compatibility checks** | Verifying that a given user device is passkey-compliant before every registration or authentication event. This requires checking the hardware, operating system, browser and user settings as well as offering alternative user journeys when a passkey cannot be used. |
| **Performance instrumentation** | Implemented on the web front-end, commonly using JavaScript tags, to help compare passkey sign-in performance against passwords. Also includes event logging on the back-end for troubleshooting and diagnostics or in support of compliance mandates. |
| **Reporting & analytics** | All the collected data points need to be stored and managed in a repository so they can be used for reporting and analytics. Real-time reports should be available to provide visibility and insights for analysis. |
| **Enterprise connectors & interfaces** | The additive passkey infrastructure will require multiple touchpoints into the existing system architecture. These include:<br>• Integrating into the IdP via common protocols like OIDC and SAML<br>• Integrating into the enterprise analytics system<br>• Integrating into a SIEM system to provide real-time analysis of security alerts |
| **Available, reliable & scalable infrastructure** | With the potential for millions of authentication events taking place each month, it becomes paramount to ensure that the new passkey-based infrastructure is not only available, but also highly reliable and scalable. |
| **Maintenance** | The ongoing maintenance of the passkey-based infrastructure involves various activities to ensure the smooth functioning of the system. These activities are essential for optimizing performance, enhancing security and providing a stable environment. |

# About Trusona

Trusona is the pioneering leader of passwordless authentication. Trusona Authentication Cloud delivers passkey best practices and improves business growth and profitability with sign-ins that delight your customers, mitigating top attack vectors like phishing and credential stuffing while providing a UX designed for the way people live and work.

Trusona is a FIDO Alliance Board member and serves as founder and chair of the FIDO UX Working Group, which provides UX Guidelines to make it simple for organizations to implement passkeys. Trusona, Google, U.S. Bank and 1Password are the financial underwriters of the FIDO Alliance UX research, "Passkey Creation and Sign-in."

Learn more about Trusona Authentication Cloud:

**trusona.com/authentication-cloud**


TRUSONA