The Right Mix:

Intuit's Journey with FIDO Authentication

How Intuit chose FIDO to get the right balance of security and convenience across its mobile apps

Millions of Intuit customers place their trust in Intuit to protect their sensitive information, and Intuit takes this responsibility very seriously. Insecure password-only authentication is a common practice in the industry; however, Intuit wanted to provide additional layers of security to protect their customers' data that also wouldn't add friction to the user experience. But as everyone in the security community knows, it is hard to come across a solution that can do both.

Intuit applied the best of both worlds working with Nok Nok Labs to deploy FIDO Authentication. Today, Intuit's users sign into its portfolio of mobile apps seamlessly with unique biometric identifiers like their fingerprint or facial recognition patterns, or even your phone's passcode. And Intuit's login process isn't just more convenient. It offers another level of security – thanks to FIDO Authentication.

Intuit's Authentication Priorities

On its mission to implement a mobile authentication solution, Intuit identified three fundamental priorities:

1. **User experience.**
   Signing in on a mobile device using a password can be frustrating – it's easy to make mistakes when typing on a mobile device. Intuit wanted the experience of signing in to the app to be frictionless for users.

2. **Security.**
   In today's threat landscape, there are so many ways a hacker can take advantage of poor security in mobile devices and apps. While infrequent sign-ins are common, Intuit wanted to make the process so easy they could regularly sign users out and invalidate their tokens to help prevent unauthorized access to accounts without negatively impacting the user experience.

3. **Account Takeover.**
   Intuit is constantly using technology and techniques to minimize account takeover, and needed a solution that would help decrease these types of opportunities for hackers.

Overview

Customer

Intuit, Inc. is a technology company that develops financial, accounting, and tax preparation software and related services for small businesses, accountants and individuals.

Challenge

Intuit needed to implement a mobile authentication solution for its suite of apps that provided added layers of security against common threats such as account takeover while still providing a seamless user experience.

Solution

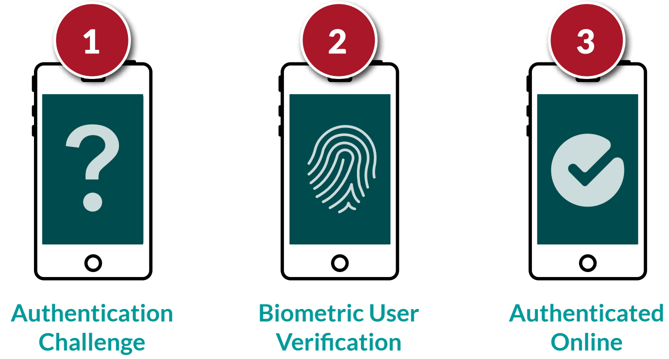
Intuit implemented the standards-based FIDO Authentication using the FIDO UAF passwordless experience, which fit into its overall model for managing identity.

Results

Intuit reports that phishing attempts have greatly decreased since its rollout of FIDO Authentication. It has also seen notable improvements in usability with a significant 20% reduction in the time it takes a user to sign in on its mobile apps, and a 6% increase in login success rates – a huge gain in a space where moving the needle by a single point is very hard.

Finding the Right Security and Usability Balance

With standards already at the center of Intuit's overall model for managing identity, FIDO Authentication fit right into that strategy. The company ultimately decided on the FIDO UAF biometrics standard for a passwordless authentication experience on mobile devices.



The FIDO protocols, including FIDO UAF, use standard public key cryptography techniques instead of shared secrets to provide stronger authentication. The protocols are also designed from the ground up to protect user privacy. The protocols do not provide information that can be used by different online services to collaborate and track a user across the services, and biometric information never leaves the user's device. This is all balanced with a user-friendly and secure user experience through a simple action at log in, such as swiping a finger, entering a PIN, speaking into a microphone, inserting a second-factor device or pressing a button.

With all of these positive factors, Intuit felt FIDO was a win for both security and for user experience. The company implemented FIDO as a central platform feature that could be used by any of its mobile app products.

Rolling Out FIDO Authentication

After making the decision to move forward with FIDO standards, Intuit evaluated vendors, educated internal customers, built out user experiences, migrated away from existing sign-in solutions and made adjustments to improve sign-in flow.

First, Intuit evaluated vendors based on criteria related to security, platform readiness, customer references and cost. The company decided to use Nok Nok Labs's S3 Platform to implement their FIDO solution, then built a service on top of this and exposed it to internal customers using a mobile SDK for iOS and Android.

Before rolling out to a broader user base including business units, Intuit launched an educational campaign for product managers, engineers, customer care agents and others. The purpose of the campaign was to educate these stakeholders on what FIDO Authentication is, how it is different from using biometric challenges to unlock an app, and the potential benefits for security, user experience and conversion. This education was especially important for internal mobile app customers who were reluctant to change the way their end users authenticated when the new approach felt similar to what they were used to.

Intuit then built user experiences for registration, sign-in and settings, and launched the platform on its TurboTax app to learn as much as possible from internal customers on how to improve the service before ultimately launching across a number of its app services. It was also extremely important to capture metrics to determine success for user experience (considering sign-in and sign-up success rates) and abuse (account takeover rates).

During the rollout, Intuit overcame several challenges. One was migrating Intuit's business apps from their existing PIN solution to unlock the app to FIDO to sign in. This involved creating user experiences that would allow a user to migrate with limited friction.

Another challenge was the latency experienced in a sign in flow. Intuit's end users were used to seeing a locally-served fingerprint challenge that showed up immediately. With FIDO Authentication, the fingerprint challenge is slightly delayed to account for round trips to the server. Intuit tested its flow on a variety of simulated network conditions and had to invest in optimizations to make sure this delay was minimized. Intuit also had to adjust its analytics frameworks, metrics and dashboards to correctly account for success rates in this new flow that no longer involved a password or MFA challenges.

The Results:

Simpler, More Secure Passwordless Logins

With FIDO Authentication now successfully rolled out across a number of its business apps, Intuit has seen astounding improvements.

20%
Reduction in Sign in Time

6%
Increase in Login Success

On the security side, the company reports that successful phishing attempts have greatly decreased since its rollout of FIDO Authentication. It has also seen notable improvements in usability with a **20% reduction** in the time it takes a user to sign in on its mobile apps, and a **6% increase** in login success rates – a huge gain in a space where moving the needle by a single point is very hard.

Because of its simpler user experience, FIDO also created opportunities for Intuit to enhance other security features. This includes asking the user to sign in more frequently, shortening the life of the authentication tokens and dramatically decreasing the potential attack surface.

With such strong reports of success, Intuit has ingrained FIDO into its authentication roadmap and plans to implement another FIDO protocol, FIDO2, for sign-in experiences on the web. The company also plans to enhance a number of step up flows, tests of user presence, and others such as phone push notifications with FIDO Authentication.

Intuit Insights:

Advice for Rolling out FIDO Authentication

1. Consider outsourcing components of the solution as needed. If outsourcing, evaluate vendors based on criteria related to security, platform readiness, customer references and cost
2. Have clear, well-defined goals in terms of reduction in abuse and improvements in user experience
3. Consider the implications on your current analytics frameworks, and how a FIDO passwordless sign in will change the way you measure conversion
4. Have a careful plan to migrate mobile apps from a local PIN or biometric challenge to unlock the app to FIDO to sign in
5. Educate product managers, engineers, customer care agents and others within your organization on what FIDO Authentication is, how it is different from using biometric challenges to unlock an app, the potential benefits for security, user experience and conversion
6. Consider a progressive approach to registration; that is, build registration flows where people provide their biometric challenge in a way that can be presented after subsequent sign-ins to minimize friction
7. Plan a simulation or pre-launch of the new registration and sign in process to work out any kinks before rolling out to your wider customer base
8. Pair your FIDO implementation with a plan to shorten security token lifetimes to realize the full security benefits
9. Plan for scalability, high availability and disaster recovery, especially if you are moving the service to the cloud

> *At Intuit, we are the stewards of our customers' most sensitive information. The trust they put in our products and our company is taken very seriously. Their financial identity safety – and financial prosperity – depends on our ability to successfully protect their accounts and profile data. Relying only on password-based authentication is not an option. Our vision to provide intelligent, adaptive authentication that moves away from passwords is being accelerated by our FIDO integration. We are looking forward to the next phases of our FIDO deployment, including support for additional authenticators and passwordless experiences in our web/browser-based scenarios. FIDO is a very important part of our Intuit Identity and Profile Platform strategy."*

Marcio Mello
Head of Product Management,
Identity & Profile Platform, Intuit