FIDO ALLIANCE

National Health Service uses FIDO Authentication for Enhanced Login

To make it easier and faster for patients throughout England to securely access multiple digital health and social care services, the National Health Service (NHS) created NHS login, an authentication and identity verification service based on OpenID Connect that allows the public to access NHS resources with a single login. NHS login can be used to securely access confidential health and care information through apps and websites that display the NHS login button.

The NHS App, which provides simple and secure access to a range of NHS services such as booking medical appointments and ordering repeat prescriptions on iOS and Android, was the first service to use NHS login to identify and verify users. NHS login and the NHS App were initially rolled out in tandem, which created a natural opportunity for the two programmes to work closely and gather initial user feedback.

With NHS login and the NHS App, the NHS was challenged with delivering secure, user-friendly multifactor authentication mechanisms which met the standards and guidelines set for public services in a short timeframe. The NHS turned to FIDO Authentication to solve the challenge.

CHALLENGE

Compliant, User-Friendly Login

Due to the sensitive nature of the information provided by the NHS App, security is of utmost importance. As such, users had to use a two-factor authentication (2FA) method when logging into the app, which required both a password and an SMS one-time passcode (OTP). It quickly became evident that the method of authentication was too cumbersome for users and became a real barrier to adoption. The NHS realized an alternative, password-free login method was needed to simplify everyday access for users.

This posed a challenge for the NHS Digital team that created NHS login and the NHS App: Not only did the new solution need to meet the security standards and guidelines set for public services, it had to be done on a very tight deadline due to a ministerial-level commitment.

THE ROAD TO FIDO:

The NHS's Evaluation Process for NHS login & NHS App

A fundamental requirement of NHS login and NHS App is a nationally agreed-upon approach to identity management for health and care, conformant with identity assurance principles endorsed by the U.K. government. NHS Digital decided that to meet these standards, biometric login would be the alternative login method for the applications. Since NHS login was already using OpenID Connect Authorisation Code Flow protocol – an open standard and decentralized authentication protocol – for user authentication, any platform used to develop biometric login would need to place great emphasis on developing a platform with open and scalable standards.

Overview

NHS

The Challenge

Multifactor identifications when logging into websites displaying the NHS login button and the NHS App, which required both a password and a one-time SMS password, was becoming a significant barrier for people trying to access medical information and services.

The Solution

NHS Digital decided that biometric authentication would best address its needs and, following a search of platforms that complied with their requirements, FIDO UAF from the FIDO Alliance was found to best fulfill the criteria, including open and scalable standards and support for mobile browsers.

The Results

NHS App with the option for biometric authentication login has a user base of approximately 1.2 million and is growing at an average rate of 32,000 new users per week. The number of SMS OTPs that NHS Digital has needed to send to users has dropped by nearly two-thirds, to about 1.5 per user per month down from about four per user per month, which represents a significant cost savings for the organisation.

The NHS login team looked at a number of platforms that could meet their needs, and measured each on six criteria including:

1. Open, scalable standards
2. Public key cryptography
3. Biometric information stored on the user's device, not the NHS or medical provider's servers
4. Support for Android and iOS mobile platforms
5. Market/sector agnostic
6. Used by well-established applications and organizations

The NHS login team's research revealed that FIDO Authentication, specifically the FIDO UAF protocol from FIDO Alliance, met all of the above criteria. They found that using FIDO in combination with the OpenID Connect Authorisation Code Flow would help NHS login to enable their partners to offer an enhanced login experience to their patients through device-based biometric authentication.

FIDO UAF development

The NHS used its in-house development team to integrate FIDO UAF, employing the Open Source UAF server from eBay. Also, since NHS login is a serverless architecture, NHS Digital needed to rewrite the FIDO server to run optimally on AWS Lambda, which they did in Python, backed by DynamoDB.

The NHS App also used the eBay Open Source UAF client as a guide for the Android implementation. This required quite a few tweaks, including rewriting it in Kotlin, and packaging it as a client. The NHS App also created an iOS UAF client using the Swift programming language packaged using Cocoapods.

Deployment and user experience with FIDO UAF

After initially believing it needed to utilize FIDO UAF to build NHS App as a comprehensive gateway for patients, NHS Digital only had to include just the basic information patients would normally seek online. By keeping it "thin," NHS Digital could allow those using the platform to come up with their own features on top of NHS App. To facilitate user development, NHS Digital exposed the APIs so others could develop their own unique apps to meet their own users' specific needs, while still granting safe, secure access to their data.

As of October 2020, there are 20 live partners and services integrated with NHS login. NHS App—with the option for biometric authentication login—has a user base of approximately 1.2 million, with an average of 250,000 FIDO authorization requests being done each week. Meanwhile, the user base continues to grow at a rate of 32,000 new users per week, of which roughly 25,000 of them set up the FIDO UAF biometric authentication. The biometric authentication has greatly reduced the number of SMS one-time passwords (OTP) NHS Digital has had to send to users by nearly two-thirds, to 1.5 users a month down from about four per user per month. This also represents a significant cost savings for the organisation since the average cost of each SMS OTP is 1.58p plus value-added tax.

FUTURE IMPROVEMENTS

NHS digital is committed to open source the solution and FIDO client libraries are already available for both iOS and Android and are working to make FIDO server libraries open source.

For the future, NHS Digital is looking at employing FIDO2 WebAuthn to support a wider range of use cases and applications.

Inside the FIDO protocols

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 fingerprint or facial biometrics.

"FIDO biometrics has enabled users to use device-based authentication making access to NHS services using an NHS login even easier. We continually receive positive feedback regarding the speed and straightforwardness of accessing health and care websites and apps using fingerprint and facial recognition."

Melissa Ruscoe
Programme Head at NHS login

