Your Security, More Simple

The Challenge with Passwords

NTT DOCOMO, INC. is Japan's largest mobile network operator with over 78 million subscriptions — and is responsible for protecting the data of each one.

To provide access to DOCOMO-branded services, partner services and carrier billing payments, DOCOMO long allowed customers to log in and authenticate using passwords including a four-digit password. This created a number of challenges — particularly because passwords are frustrating to use, and it is difficult to have to remember multiple passwords.

DOCOMO needed to find a solution that may resolve their password-related issues.

The Best of Both Worlds with FIDO Authentication

After reviewing the different approaches to authentication available, DOCOMO settled on the FIDO authentication model as the best strategy for solving the current and future authentication needs of its customers. It found that by deploying cross-platform FIDO-enabled, privacy-respecting biometric authentication, they could have a solution that is simultaneously more secure and convenient. It is worth noting that such biometric information never leaves their devices for their privacy.

FIDO-based biometric authentication relies on FIDO standards that use public key cryptography to protect users against a variety of attacks including phishing, brute force and man-in-the-middle attacks. Users register their on-device biometric with any online service that supports the protocol.

When considering a new authentication approach, DOCOMO found FIDO to be the best option because it allowed them to:

- Implement in a straightforward manner that aligns with the FIDO ecosystem for long-term sustainability and continuity of authentication as a service
- Utilize the standards in a way that allows different types of authenticators, such as fingerprint sensors and iris scanners
- Protect the security of users and ecosystem partners with FIDO's privacy policy that states biometric data and private cryptographic keys will never leave the user's device

Overview

In May 2015, NTT DOCOMO began offering FIDO Authentication in four devices (including the world's first iris scanner equipped smartphone) from multiple OEMs and a FIDO-enabled server. With this, DOCOMO became the world's first mobile network operator to deploy FIDO Authentication throughout its network, delivering simple, strong authentication for DOCOMO's millions of customers across multiple services with d ACCOUNT™, which is an OpenID based account for customers nationwide.

By eliminating passwords with FIDO standards, DOCOMO is able to deliver a superior end-user experience that includes enhanced security features. It is also able to introduce innovative new services and product offerings that can utilize standards-based platforms and devices.

NTT DOCOMO's FIDO-based Solutions in Practice

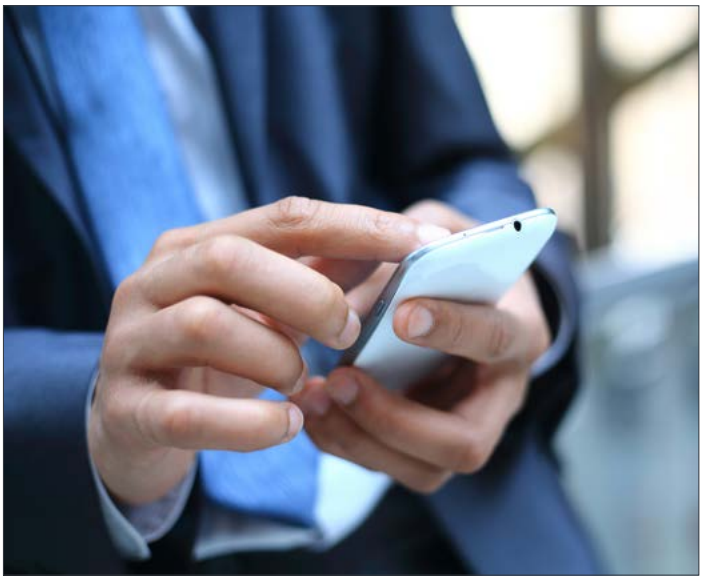
Today, DOCOMO has shipped an impressive suite of more than 60 FIDO-enabled d ACCOUNT Authentication compliant Android devices. Of these, DOCOMO has shipped 36 FIDO UAF 1.0 Certified Android devices, while newer devices have been shipped with a pre-installed FIDO UAF 1.1 application to utilize Android's built-in FIDO capabilities.

In addition, all Touch ID/Face ID-equipped iOS devices are also available for d ACCOUNT Authentication.

Using FIDO specifications, DOCOMO is enabling its customers to securely authenticate themselves with fingerprint or iris biometrics instead of a password with the DOCOMO d ACCOUNT app that incorporates FIDO Authentication. From there, they have secure access to DOCOMO account details, billing and services, including mobile gaming and music platforms d game™ and d music™, and shopping sites such as d delivery™ and d shopping™. DOCOMO also replaced carrier billing password authentication, allowing customers to approve their payments via biometrics built into their device.

In addition to DOCOMO-branded services at d market™, various partner services are able to utilize FIDO Authentication through carrier billing payment and as a federated ID utilizing OpenID Connect without any modifications.

DOCOMO also provides FIDO Authentication at scale by allowing other relying parties to utilize its FIDO Certified on-device biometrics. For example, Mizuho Bank, a major bank in Japan, uses DOCOMO's FIDO Certified authenticator to allow its own customers to access their mobile banking app.



Enabling a More Secure Future

As a market leader with a clear strategic investment in the FIDO ecosystem, DOCOMO joined the FIDO Alliance as a Board Director in 2015 and has been contributing to the development of FIDO standards and best practices.

DOCOMO is responsible for establishing and chairing the FIDO Deployment-at-Scale Working Group (D@SWG), which was formed to accelerate overall deployments of FIDO solutions by bringing together online service providers and device manufacturers to share lessons learned, produce case studies, and establish industry best practices for deploying FIDO Authentication at internet scale. This group has since spun off three Deployment Working Groups for consumer, enterprise, and government, with DOCOMO chairing the FIDO Consumer Deployment Working Group (CDWG).

In addition, DOCOMO drove the formation of the FIDO Japan Working Group (FJWG) in 2016 and has taken a leadership role as Chair. The FJWG has been driving FIDO adoption in Japan by facilitating communication, cooperation and improved awareness of FIDO Alliance and FIDO Authentication in Japan.

