Standardization (Special Articles)
FIDO Authentication | Security | Public Key Cryptography
Special Articles on Solving Password Problems with FIDO Authentication

NTT DOCOMO's Contributions to Standardization of Online Authentication at the FIDO Alliance

Product Department Koichi Moriyama
Yukiko Tomiyama Yukiko Makino

The FIDO®*1 Alliance is a global non-profit organization that focuses on reducing the reliance on passwords, with the goal of achieving both security and usability in online authentication. NTT DOCOMO joined the FIDO Alliance Board of Directors in 2015 and has been contributing to creating FIDO specifications and to developing a new ecosystem. This article describes an overview of the FIDO Alliance and FIDO Authentication. It also introduces contributions by DOCOMO and gives an overview of the expansion and future prospects for FIDO Authentication within and outside Japan.

1. Introduction

FIDO stands for Fast IDentity Online and represents the new online authentication model being advocated by the FIDO Alliance, as well as a set of specifications based on the online authentication model. The important feature of this authentication model is that it leverages public key cryptography*2 instead of using any "shared secrets" such as passwords. By combining the FIDO Authentication model with biometrics, simple and strong online authentication can be implemented and delivered, achieving both usability and security [1].

Recently, the need has been increasing for online authentication in various situations, such as cashless online settlement, while reports of unauthorized

*1 FIDO®: FIDO and the FIDO Alliance logo are trademarks or registered trademarks of the FIDO Alliance.

access and fraudulent transactions continue unabated. As such, it is increasingly important to provide a means of authentication that is both easy-to-use and secure. Amid these developments, DOCOMO deployed its d ACCOUNT®*3 Passwordless Authentication in March 2020. This was built on the foundation of d ACCOUNT Biometric Authentication [2], which utilizes FIDO Authentication and has expanded significantly since it was launched in May 2015. It now provides customers with the optional feature of disabling passwords and allowing only FIDO Authentication, so they can use online authentication with confidence [3] [4].

The successful introduction of d ACCOUNT® Passwordless Authentication is due to making the best use of FIDO Authentication technology as well as contributing to the FIDO Alliance and its ecosystem. As a Board member of the FIDO Alliance, we have used our experience to give feedback, pursued the potential of FIDO Authentication further, contributed to standardization efforts within the FIDO Alliance, and utilized the updated specifications. As a result, FIDO Authentication is starting to be used more widely and gaining attention both within and outside Japan.

This article describes the FIDO Alliance and FIDO Authentication, introduces the contributions by DOCOMO, examines the expansion of FIDO Authentication within and outside Japan, and discusses future prospects for this technology.

2. FIDO Alliance and FIDO Authentication

2.1 FIDO Authentication Model

FIDO Authentication is based on a new model for online authentication using public key cryptography, which is both easy-to-use and secure. The FIDO Authentication model is divided into two parts: a FIDO authenticator, which locally verifies that the user is the owner of the authenticator, and a part that establishes online authentication by verifying signatures using public key cryptography, with a public and private key pair (**Figure 1**).

The authenticator must be configured before authentication can be performed. This is done by first generating a public and private key pair with the authenticator; the private key is stored in the authenticator, and the public key is sent to and registered in the authentication server (**Figure 2** (a)). When a registration request is received, the server first sends a challenge code (a random value) to the authenticator. The authenticator generates a key pair, stores the private key in a safe area within the authenticator, signs the challenge code with the private key, and sends it back to the server together with the public key. Use of the challenge code guarantees that the exchange between the server and authenticator is one-to-one.

For an authentication request from the user, the server first sends a challenge code to the authenticator. The authenticator then verifies the user using some credential such as biometric information or knowledge that is only valid locally on the device (e.g., a device passcode). If the user is verified, the challenge code is signed with the private key and returned to the server. The server verifies the signed challenge code using the corresponding public key, and if this is successful, online authentication is established (Fig. 2 (b)).

Unlike legacy authentication using passwords, the FIDO Authentication model does not involve the

*2 Public key cryptography: An asymmetric cryptosystem using a public and private key pair. The private key must be kept safe, but the public key need not be hidden. This feature distinguishes it from the common key cryptosystem.

*3 d ACCOUNT®: A trademark or registered trademark of NTT DOCOMO, INC.

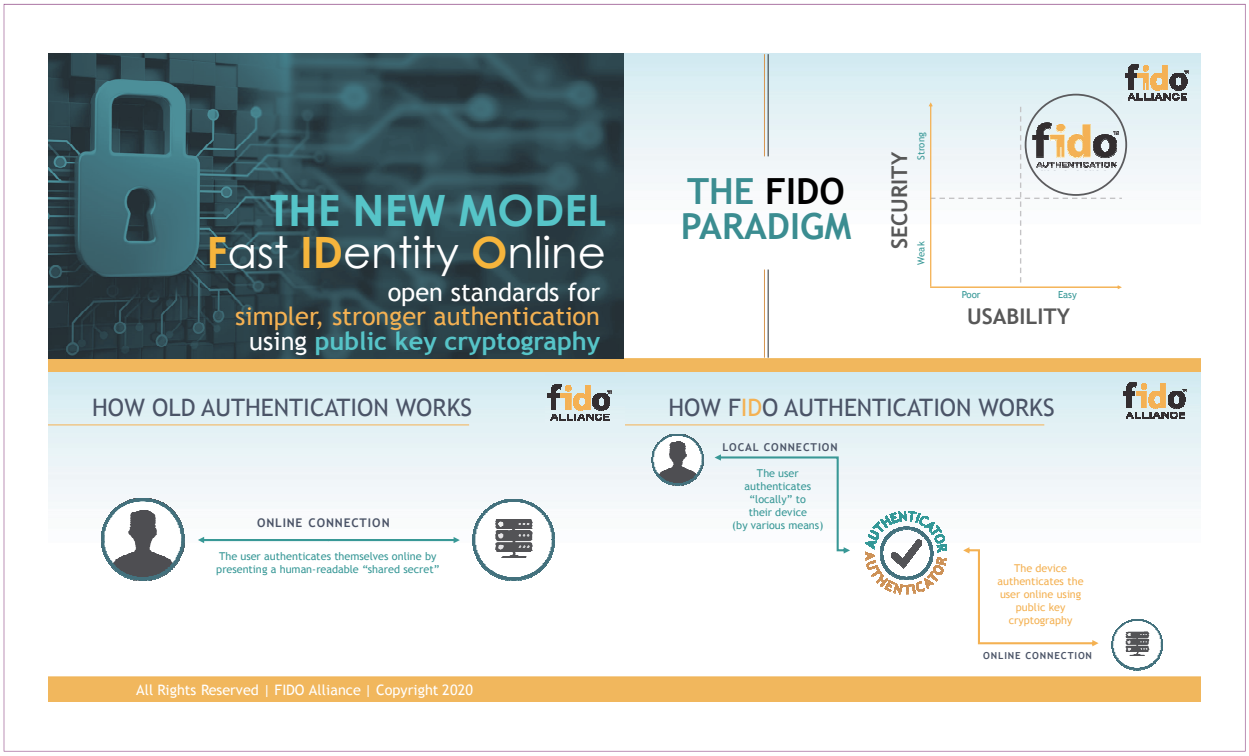

Figure 1 The FIDO Alliance's Goal and The New Authentication Model

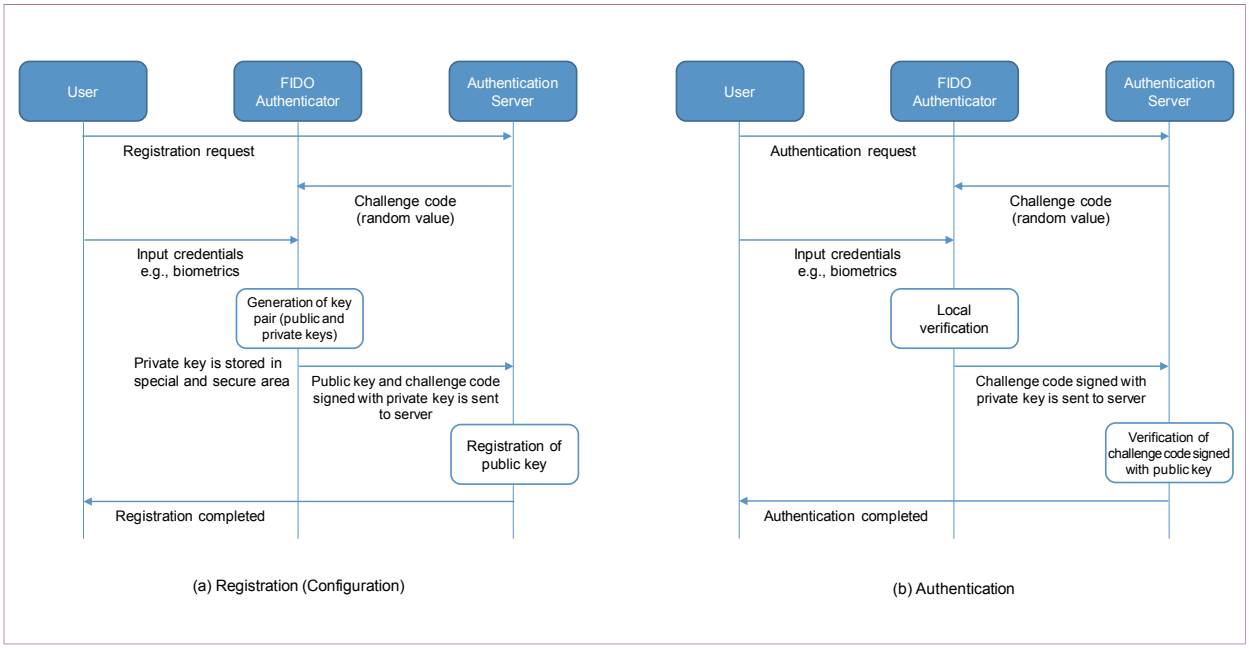

Figure 2 Sequence of FIDO Authentication – "Secrets" Never Passed over the Internet

sharing of "secrets" among the user, authenticator, and server, and no "shared secrets" are passed over the Internet. As such, it is not vulnerable to credential stuffing and phishing. Also, it can be used for user authentication by different service providers with the same user experience such as touching a fingerprint sensor. Thus, it can be used to implement online authentication that is both easy-to-use and secure.

2.2 FIDO Alliance

The FIDO Alliance is a global non-profit organization that was established in 2012 to focus on solving password problems. It promotes FIDO Authentication through creation of technical specifications based on the FIDO Authentication model, by operating a certification program that ensures interoperability, and by working with various international standardization organizations. Approximately 250 organizations participate in the Alliance, representing many industries and geographies (**Figure 3**).

1) Membership

Membership in the FIDO Alliance is divided into four membership levels and categories with different annual fees and benefits: Board members, Sponsor members, Associate members, and Government members. Within the FIDO Alliance, Board members in particular can play a leadership role.

Board members have the right to participate in decision making within the FIDO Alliance. They

Figure 3 FIDO Alliance Board Members

participate in Board meetings, discuss various proposals made to the Board, such as new strategies or establishing the Working Groups (WGs) needed to put them into practice, and can exercise their right to vote on these proposals. They also have the right to be elected as a member of the Executive Council representing the FIDO Alliance and the Board, to be elected as a chair or a co-chair of a WG, and to work in that capacity for a set term. They also have priority for participating in marketing activities.

DOCOMO has been a Board member of the FIDO Alliance since May 2015.

2) Working Groups

The core activities of the FIDO Alliance are driven mainly by the WGs, each with their respective roles. Currently there are 15 WGs in the FIDO Alliance. These are divided into three categories: Technical WGs, which create technical specifications for FIDO Authentication, security requirements, and certification programs; Adoption WGs, which promote introduction and expansion of FIDO Authentication; and Regional WGs, whose objective is to achieve the mission of the FIDO Alliance effectively in each country or region.

DOCOMO is or has worked as a chair or a co-chair in the following WGs.

- Consumer Deployment WG
- Security and Privacy Requirements WG
- FIDO Japan WG

2.3 FIDO Specifications

FIDO specifications, which enable implementation of the FIDO Authentication model, include the FIDO UAF (Universal Authentication Framework) and FIDO U2F (Universal Second Factor), both of which were released as version 1.0 in December 2014, and also FIDO2, which has been under active deployment since 2018 (**Figure 4**).

- FIDO UAF: Specification designed for passwordless authentication
- FIDO U2F: Specification designed for second factor authentication
- FIDO2: Specification to facilitate incorporating FIDO Authentication model into OS and browser platforms in order to promote broader expansion

One contribution from DOCOMO to the creation of FIDO specifications was FIDO UAF 1.1. This incorporated feedback from DOCOMO's experience in early adoption and commercialization of FIDO UAF 1.0 in our d ACCOUNT Biometric Authentication. By utilizing the KeyStore Key Attestation function in Android™*4 OS 8.0 and later, it enables device manufacturers to develop and include FIDO UAF applications without requiring customization for each device model. Commercial deployment of FIDO UAF 1.1 began in November 2017, and it was announced in December of the same year. This helped with deployment of FIDO Authentication without having to wait for the launch of FIDO2.

1) FIDO2 and Web Authentication

The FIDO Alliance decided that to further develop FIDO Authentication, it was essential to support platforms such as OSs and browsers. Since standardization by W3C®*5, the World Wide Web Consortium, is necessary for support in browsers, the FIDO Alliance submitted a basic draft specification of the Web components to W3C in November 2015, and contributed to standardizing it as a

*4 Android™: A trademark or registered trademark of Google, LLC.

*5 W3C®: An international organization promoting standardization of Web technologies. An abbreviation of "World Wide Web Consortium" and a trademark or registered trademark.

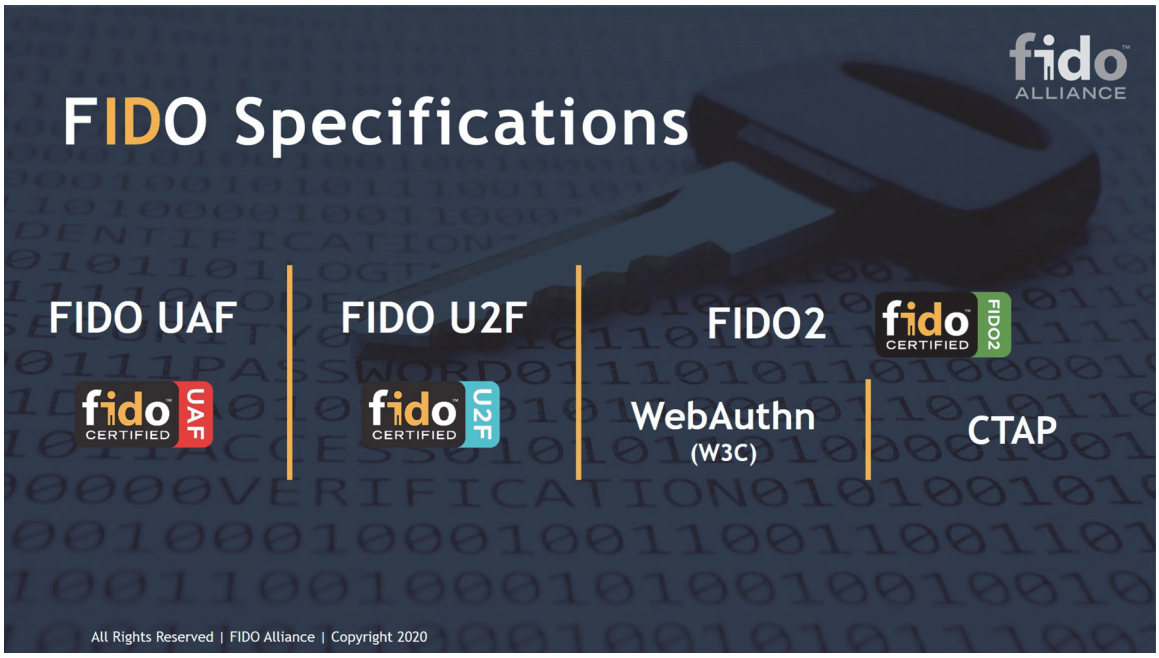

Figure 4 FIDO Specifications

liaison partner. A JavaScript[*6] API for Web Authentication was standardized as a formal recommendation, "Web Authentication: An API for accessing Public Key Credentials Level 1," in March 2019. Currently, all mainstream browsers support Web Authentication Level 1, and creating Level 2 specifications is in progress at W3C [5] [6].

As with Web Authentication, users are expected to use a FIDO authenticator. Either a platform authenticator, built into the device running the browser, or an external authenticator such as a security key, connected through USB, BLE, or NFC can be used. To enable implementation of external authenticators, the FIDO Alliance created the Client to Authenticator Protocol (CTAP) specification. CTAP was created as a successor to the corresponding parts of the FIDO U2F specification (which formally has been renamed CTAP 1 in order to clearly show this lineage).

2) International Standardization

The FIDO Alliance is also collaborating with international standardization organizations, and one result of this is that FIDO UAF and CTAP, which are necessary for implementing authenticators, were adopted by the International Telecommunication Union (ITU), Telecommunication Standardization Sector (ITU-T), in December 2018 as the following international standards.

- ITU-T Recommendation X.1277 - FIDO UAF 1.1
- ITU-T Recommendation X.1278 - FIDO2 CTAP (including U2F CTAP1)

*6 JavaScript: A script language designed for use in Web browsers. JavaScript is a registered trademark or trademark of Oracle Corporation, its subsidiaries and affiliates in the United States and other countries.

2.4 Certification Programs

The FIDO Alliance has established certification programs to validate that products supporting FIDO Authentication conform to FIDO specifications and to ensure interoperability, mainly between authenticator devices and servers. Companies receiving certification can apply the "FIDO® Certified" logo to their products. FIDO Alliance membership is not a requirement to participate in the FIDO certification programs.

To ensure interoperability, the certification programs include (i) conformance tests, conducted by developers on authenticator and server functions; (ii) interoperability tests, supported by the FIDO Alliance and hosted by FIDO Alliance member companies; and (iii) authenticator security certification, which is conducted in partnership with third-party laboratories.

Authenticator security certification validates compliance with security requirements for six levels: L1, L1+, L2, L2+, L3, and L3+, which are determined by the Security and Privacy Requirements WG described below. For any authenticator that needs to be certified, L1 certification must be obtained, while levels L1+ to L3+ are optional. In 2018, an optional (iv) biometric component certification program was also started to validate the performance of biometric sensors.

In April 2015, DOCOMO participated in the first interoperability testing held in San Jose, California, and has been able to use FIDO Certified devices for our commercial services since we began providing d ACCOUNT Biometrics Authentication using FIDO UAF 1.0 in May 2015. We have also hosted interoperability testing since the early days of the FIDO certification program at DOCOMO Innovations, Inc., our office in Palo Alto, California, and have contributed feedback including experience from this work.

The first interoperability testing in Japan was held in November 2019, with participation from 14 companies from ten countries and regions. Three new products from Japan obtained FIDO certification.

3. DOCOMO's Contributions to the FIDO Alliance

DOCOMO currently has several roles within the FIDO Alliance. One of them is as a Board member company. The Board makes decisions within the FIDO Alliance, and DOCOMO is a member of the Board. As a Board member company, DOCOMO is also taking other leadership roles such as contributing to the establishment of several WGs and acting as a WG chair or a co-chair. We also have roles in several committees within the Board. Since 2019, we have also served on the Executive Council, consisting of seven members elected from Board member company representatives, and this is another important role.

Other contributions worthy of particular mention are DOCOMO's deployment of FIDO Authentication, proactively utilizing its features, and the resulting feedback to the FIDO ecosystem through various channels.

3.1 Contributions to WGs as Chair or Co-Chair

1) Consumer Deployment WG

At the second Board meeting after DOCOMO joined the FIDO Alliance in June 2015, we gave a

presentation introducing our deployment of FIDO Authentication and the main issues we encountered in the process. This increased momentum to establish a working group to promote wider deployment of FIDO Authentication. We proposed a Deployment-at-Scale WG (D@S WG), which was the first Adoption WG within the FIDO Alliance, and after discussion and approval by the Board, DOCOMO was appointed as chair to drive FIDO adoption.

Initially, there were few examples of FIDO Authentication deployment, and we were working on several fronts: maintaining the prospects for FIDO2, which was being developed at the time; resolving issues that were unrelated to the differences among the various FIDO specifications despite being based on the same FIDO Authentication model; and striving to further expand the potential of FIDO UAF and U2F. A part of this work as the D@S WG chair was to promote reporting on a deployment case study in Korea in the form of a white paper [7]. Later, we also actively worked for the adoption of FIDO Authentication by major banks in Japan. We also summarized the basic concept of FIDO UAF 1.1 as mentioned earlier, and we wrote and published a white paper [8], working with partner companies that are also FIDO Alliance Board members.

Through these activities, we have reached the stage where it is more effective to conduct activities in multiple deployment WGs specialized for consumers, for enterprises, and for government agencies. DOCOMO is now responsible for focusing on efforts in the Consumer Deployment WG.

- Account Recovery

One theme we have been working on recently for accelerating FIDO adoption is referred to as Account Recovery. This is the problem of how a user can enroll a new device to serve as an authenticator for their account if they have lost their authenticator and have no "shared secrets."

To address this problem, DOCOMO has utilized as an example its own business infrastructure for verifying identities when users need to reconfigure their FIDO authenticator due to losing a device. We have long maintained the identity proofing infrastructure needed as a mobile network operator to comply with regulations on preventing improper use of mobile phones ever since d ACCOUNT Biometric Authentication was first introduced. We are also utilizing this infrastructure for d ACCOUNT Passwordless Authentication. It is also very important for DOCOMO to provide an Account Recovery mechanism for users regardless of whether they are a subscriber, so we are working to develop a mechanism that can be commonly applied, not only to telecommunications, but also to a whole range of industries and the FIDO ecosystem.

Through its leadership in the Consumer Deployment WG, DOCOMO has contributed to creating a white paper on Account Recovery and will continue to lead in these efforts.

2) Security and Privacy Requirements WG

The Security and Privacy Requirements WG began as the Security Requirements WG due to a proposal by a Board member from the credit card industry and is now organized as the Security and Privacy Requirements WG after the addition of a security specialist from a platform chipset vendor as co-chair.

Since DOCOMO started providing d ACCOUNT Biometrics Authentication utilizing FIDO Authentication, we have defined security requirements for

DOCOMO branded smartphones (Android) to protect privacy information. This is done using a special and secure area within the device, such as a TEE (Trusted Execution Environment), to store biometric information and private keys and to perform comparison operations with the biometric information. These requirements include transmission of the biometric sensor data to the special and secure area.

Due to our efforts, when the FIDO Alliance was preparing formal requirements for strengthening the certification program with respect to security and privacy protection, we were able to provide useful feedback. This led to deeper discussion with other authorities and contributors within the FIDO Alliance and solidified the essential security requirements for the current six-level certified authenticator security level program.

From July 2018 to March 2020, DOCOMO served as co-chair for facilitating this work.

3) FIDO Japan WG

In 2015, FIDO Alliance member companies doing business in Japan gathered together and began activities promoting FIDO Authentication within the FIDO Alliance as well as outside of the alliance and organized an official FIDO Tokyo Seminar as one of their efforts. The following year, in December, the FIDO Alliance announced the launch of the FIDO Japan WG as the third Regional WG with 11 initial member companies. Its mission was to effectively implement the goal of the FIDO Alliance in Japan. Its formally stated mission is to "develop and promote the FIDO Authentication model as a simpler and stronger alternative to passwords." Currently, 48 companies participate in the FIDO Japan WG, making it the largest and one of the most active WGs in the FIDO Alliance.

Since the inception of the WG, DOCOMO has been the chair and has contributed to the spread and increased presence of FIDO Authentication in Japan. Through the tremendous cooperation of FIDO Alliance member companies within and outside Japan, and of many other parties with business locations in Japan, we have been able to conduct these activities within the global alliance, as a contribution from Japan to the world.

The activities of the Japan WG and its achievements have been reported in press releases, announcements, and many articles published by media and journalists through annual FIDO Tokyo Seminars, annual press briefings, and other press conferences. More than 300 participants have attended the annual seminars in each of the past three years, and recent Japanese news articles have mentioned FIDO Authentication as a solution to password problems.

We would like to express our deep gratitude at this time to all those who have contributed to the FIDO Japan WG.

3.2 Contributions Using FIDO Authentication

In addition to contributions through activities with the FIDO Alliance, DOCOMO is actively utilizing FIDO Authentication, from devices through services, and is giving feedback from that experience as a contribution to the FIDO Alliance and to the FIDO ecosystem.

1) Adopting Various Biometric Sensors

One impetus for adopting FIDO Authentication at DOCOMO has been to provide more attractive devices to our customers. At the time of adoption,

our customers were using multiple passwords such as an sp-mode password and a DOCOMO applications password in addition to the d ACCOUNT password ("docomo ID" at the time), and we were considering use of biometric authentication as a more convenient means of authentication. In planning our Summer 2015 device portfolio, which included the first-ever smartphone with iris recognition (the ARROWS NX F-04G, manufactured by Fujitsu Ltd.), we utilized the fact that FIDO Authentication does not depend on the type of biometric sensor used to verify the user, enabling manufacturers to use sensors suitable for each device model. When devices were equipped with biometric sensors, we made every effort to define requirements for performance, security, and privacy protection, to ensure they were implemented, and to ensure business continuity as a mobile network operator.

We subsequently received proposals from multiple device manufacturers to equip smartphones with multiple iris and fingerprint sensors. We reviewed the FIDO UAF specifications and interpreted them in a way that enabled us to develop a new d ACCOUNT Settings application and provide authentication functions using either iris or fingerprint recognition, without requiring customers to be concerned with multiple biometric sensors.

2) Utilizing Open Standards

We utilize FIDO Authentication, open standard specifications that anyone may implement, and we accept various other authenticator implementations if they are FIDO Certified. Even though we shipped 36 models of DOCOMO branded smartphones (Android) conforming to FIDO UAF 1.0 (predecessor to FIDO UAF 1.1), and there were five different authenticator implementations by seven device manufacturers, we were able to confirm their interoperability through the FIDO certification program, and we experienced no service provision issues or problems. Of course, we also later ensured interoperability with FIDO UAF 1.1, the same as for FIDO UAF 1.0, and we did not expect to have any issues or problems when we planned to migrate to FIDO2, either.

3) Utilization of Good Compatibility with ID Federation

FIDO Authentication is designed to work with ID federation technologies such as OpenID® Connect*7. Since DOCOMO designs and provides d ACCOUNT, which is based on OpenID Connect, we are able to support our partner companies with d ACCOUNT Biometric Authentication by using OpenID Connect based ID federation technologies for logging in to services provided by these partner companies.

4) Making the Best Use of Authentication Model without "Shared Secrets"

From the beginning, DOCOMO has had a strong intention to make the best use of FIDO Authentication, which does not rely on shared secrets and has been proven to be phishing resistant [2]. As such, d ACCOUNT Passwordless Authentication makes the best use of FIDO Authentication; thus, we have solved the remaining password problems from the security perspective. This is described in more detail in another special article in this issue [3].

4. Expanding FIDO Adoption Within and Outside Japan

When d ACCOUNT Biometric Authentication was first launched, it was the first such launch in the world by a mobile network operator and also the first with FIDO authenticators from multiple

*7 OpenID® Connect: A protocol for the ID federation set by the OpenID Foundation. OpenID is a trademark or registered trademark of the OpenID Foundation.

manufacturers and devices with iris recognition.

4.1 FIDO Adoption in Japan

Since major banks in Japan began providing login features using biometric authentication with FIDO Authentication in October 2017, everyday use of FIDO Authentication has increased rapidly, by financial institutions, mobile network operators, Internet service providers, and in various business domains.

Specific examples of use or provision of FIDO UAF in order of launch include NTT DATA (internal mobile applications), Mizuho Bank, SoftBank, MUFG Bank, Aflac Life Insurance Japan, NTT Communications (an SSO service*8), Tepco Systems (internal system), and Japan Post Bank. Furthermore, there are several cases of FIDO2 adoption, including Yahoo Japan (Yahoo! JAPAN ID), International System Research (an SSO service), LINE Pay, and KDDI. If FIDO U2F use cases are also included, there are many more cases of FIDO Authentication within enterprises across Japan. These include several of the first implementations of FIDO2 in industry, further demonstrating Japan's leadership in FIDO adoption.

4.2 FIDO Adoption Outside Japan

Since DOCOMO began offering FIDO Authentication for our customers in Japan, the Bank of America also began offering a service using FIDO UAF. Both DOCOMO and Bank of America are Board member companies in the FIDO Alliance and have supported both Android and iOS*9 devices from the earliest stages. In Korea as in Japan, both Samsung and BC Card, co-chairs of the FIDO Korea WG, have also shown leadership, using FIDO Authentication widely since the early stages.

1) North America

It is widely known that Google has used Titan Security Keys, which are based on FIDO Authentication, to prevent unauthorized logins within the company.

As a FIDO Alliance member, Intuit Inc. recently reported the results of migrating from an SMS OTP (one-time password)*10 to FIDO Authentication [10]. They found that migrating to FIDO Authentication reduced the time required to login by up to 20% and improved authentication success rates.

The U.S. General Services Administration, which supports federal agencies, has also added support for FIDO Authentication on its SSO service website for federal employees, using Windows Hello*11 with security keys.

These examples demonstrate how use of FIDO Authentication is expanding in North America.

2) Europe

In Europe, the General Data Protection Regulation (GDPR)*12 mandates that biometric data is private information of the highest level, so FIDO Authentication is promising in that it stores biometric data in a safe area within the authenticator. In the financial settlements domain, the recently enacted European Payment Services Directive II (PSD2)*13 mandates the use of two-factor authentication, and FIDO Authentication well suited for this purpose.

On another front, there has been news that the NHS, the National Health Service, in the UK, has released open source software for developers to enable applications to use FIDO biometric authentication for login.

*8 SSO service: A service that links IDs beforehand to enable login for multiple IDs by logging in with one particular ID.

*9 iOS: A trademark or registered trademark of Apple Inc., registered in the U.S. and other countries. Used under license from Cisco Systems, Inc.

*10 SMS OTP: A one-time password distributed using the Short Messaging Service (SMS).

*11 Windows Hello: A trademark or registered trademark of Microsoft Corp. in the U.S. and other countries.

As such, the prospects for use of FIDO Authentication are promising in Europe.

3) Asia-Pacific

The Asia-Pacific region is leading the world in the use of FIDO Authentication, with broad deployment in Korea and Taiwan as well as in Japan [10].

In Korea, FIDO Authentication is widely used by banks and other financial institutions, and FIDO Authentication can be used in various other scenarios with government ID that supports K-FIDO [7]. In Taiwan, the MOICA citizenship certificate, which is based on the Public Key Infrastructure (PKI)*14, supports FIDO Authentication in the form of TAIWAN FidO [11].

The FIDO Alliance is working with the Asia PKI Consortium (APKIC) as a liaison partner to demonstrate the use of FIDO Authentication for national identity systems based on the PKI infrastructure in the Asia-Pacific region.

5. Conclusion

This article has described FIDO Authentication and the FIDO Alliance and has introduced DOCOMO's contributions to promoting FIDO Authentication in Japan and throughout the world.

Initiatives utilizing FIDO Authentication at DOCOMO began with a meeting in June 2014 at Nok Nok Labs in Silicon Valley. They are one of the six founding companies of the FIDO Alliance. DOCOMO began providing d ACCOUNT Biometrics Authentication and FIDO Authentication servers using the Nok Nok Labs' implementation in May 2015. Since then, the servers have operated continuously without a single fault.

Finding ways to solve the problems related to the use of passwords is one of the main issues to be addressed in this era of digital transformation*15. DOCOMO believes that world-class corporations driven by the global ecosystem can find solutions to the various problems and resolve this issue.

The FIDO Alliance advocates the use of an authentication model not dependent on "shared secrets." It brings together various companies, major OS and platform providers such as Google and Microsoft, and also those specializing in authentication and security technologies, like Nok Nok Labs. It overcomes barriers among industry domains, regardless of enterprise size, to achieve "Diversity and Inclusion." DOCOMO is very pleased to be able to play key roles in this effort. DOCOMO will continue to expand the reach of its d ACCOUNT Passwordless Authentication to more users while making it easier to use and more secure, thereby contributing to the expansion of the FIDO Authentication ecosystem.

REFERENCES

[1] FIDO Alliance website. https://fidoalliance.org/

[2] K. Moriyama: "Toward a Passwordless World: Initiatives and Future Prospects at NTT DOCOMO for d ACCOUNT Biometric Authentication Using the FIDO Standards," TTA Telecommunications, Vol.80, No.840, pp.13–19, Jan. 2017.

[3] T. Ozaki et al.: "NTT DOCOMO's Passwordless Authentication Utilizing FIDO Standards," NTT DOCOMO Technical Journal, Vol.22, No.1, pp.10–21, Jul. 2020.

[4] FIDO Alliance: "NTT DOCOMO introduces passwordless authentication for d ACCOUNT," Oct. 2019. https://fidoalliance.org/ntt-docomo-introduces-passwordless-authentication-for-d-account/

[5] W3C Recommendation: "Web Authentication: An API for accessing Public Key Credentials Level 1," Mar. 2019. https://www.w3.org/TR/webauthn/

*12 GDPR: Protective regulation regarding the handling of personal information within EU member countries and the European economic region. Also applies to the collection and transport of personal information.

*13 PSD2: Directive for implementing safe electronic transactions within the EU region. Includes new settlement services on the Internet and mobile devices.

*14 PKI: Infrastructure that uses public key cryptography to guarantee safe communication.

*15 Digital transformation: Changes brought by the use of digital technology, promoting business activities and bringing benefits to all aspects of human life.

[6] Y. Matsuura, K. Tanaka, S. Fujimura, K. Moriyama: "Activities at W3C Technical Plenary and Advisory Committee Meetings Week (TPAC) 2019 in FUKUOKA," NTT Technical Review, Vol.18, No.3, pp.75–78, Mar. 2020.

[7] FIDO Alliance: "FIDO Alliance White Paper: Korean FIDO Deployment Case Study Accredited Certification System for Safe Usage of Accredited Certificate using FIDO in Smartphone in Korea (K-FIDO)," Sep. 2017.
https://fidoalliance.org/white-paper-korean-fido-deployment-case-study-accredited-certification-system-for-safe-usage-of-accredited-certificate-using-fido-in-smartphone-in-korea-k-fido/

[8] FIDO Alliance: "FIDO Alliance White Paper: Hardware-backed Keystore Authenticators (HKA) on Android 8.0 or Later Mobile Devices," Jun. 2018.
https://fidoalliance.org/white-paper-hardware-backed-keystore-authenticators-hka-on-android-8-0-or-later-mobile-devices/

[9] FIDO Alliance: "The Right Mix: Intuit's Journey with FIDO Authentication," Oct. 2019.
https://fidoalliance.org/the-right-mix-intuits-journey-with-fido-authentication/

[10] FIDO Alliance: "New Certifications, Deployments Further Illustrate Strong FIDO Momentum throughout Asia," Dec. 2018.
https://fidoalliance.org/new-certifications-deployments-further-illustrate-strong-fido-momentum-throughout-asia/

[11] TAIWAN FidO website.
https://fido.moi.gov.tw/