Technology Reports (Special Articles) Biometrics Security FIDO Authentication
Special Articles on Solving Password Problems with FIDO Authentication

NTT DOCOMO's Passwordless Authentication Utilizing FIDO Standards

Product Department Tomohiko Ozaki Hiroki Uesaka
Yukiko Makino Yukiko Tomiyama Koichi Moriyama

A serious problem that is rapidly increasing is unauthorized access using passwords stolen by phishing or other types of information theft. Also, it is troublesome for customers to manage passwords because they are often required to make their passwords complex enough to prevent unauthorized access with guessed passwords. To solve such password problems, NTT DOCOMO launched d ACCOUNT®*1 Passwordless Authentication utilizing FIDO®*2 Authentication standards in March 2020. DOCOMO's passwordless authentication allows users to disable their password for d ACCOUNT and offers biometric and/or other methods based on FIDO standards for simpler and stronger authentication instead. Thus, users no longer have to worry about unauthorized access to their d ACCOUNT while maintaining ease of use.

1. Introduction

The role of online authentication is becoming critical for logging into services, making payments for online shopping, and other activities on the Internet. However, many news articles and reports indicate that there is a growing number of unauthorized accesses by third parties. Using clever phishing sites*3 to steal passwords for unauthorized purposes has created a particularly serious problem.

NTT DOCOMO provides an ID called "d ACCOUNT," which is used for a variety of purposes such as accessing DOCOMO services, checking d POINT, online-shopping at dmarket®*4, and more from a smartphone or a PC. d ACCOUNT is offered to

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

anyone and is not limited just to DOCOMO subscribers. DOCOMO started to offer d ACCOUNT Biometric Authentication [1] in May 2015; it utilizes FIDO (Fast IDentity Online), an open standard for passwordless authentication, to enable simpler and stronger online authentication for login to d ACCOUNT or for online payments. It is designed for making d ACCOUNT authentication more convenient, providing easy alternatives to password authentication such as using fingerprints, iris, or any other biometrics that may be implemented on smartphones. We have utilized FIDO Authentication mainly for ease of use; however, password-related security risks will remain as long as users still have the choice of using passwords.

We had a strong intention to make the best use of FIDO Authentication standards in order to improve security for d ACCOUNT from the beginning, when we planned d ACCOUNT Biometrics Authentication, but we first needed to widely deploy d ACCOUNT FIDO authentication compliant devices. Now that such devices have spread sufficiently, we have developed and deployed d ACCOUNT Passwordless Authentication, which allows users to disable password authentication in order to eliminate unauthorized access using stolen passwords. We started to offer it in March of this year as an optional feature that enables transition to FIDO Authentication in all situations.

This article first gives an overview of d ACCOUNT Biometric Authentication, which is utilized as a foundation for d ACCOUNT Passwordless Authentication. It then describes the design and implementations of DOCOMO's passwordless authentication, especially addressing the top five issues needing to be addressed to eliminate passwords in the real world. Finally, it discusses future prospects.

2. Background: Overview of d ACCOUNT Biometric Authentication

DOCOMO deployed d ACCOUNT Biometric Authentication utilizing FIDO standards in May 2015, under the tagline, "Your Security, More Simple," to enable more convenient login and use of services on DOCOMO branded smartphones. For DOCOMO subscribers, we provide an sp-mode®*5 password and Network PIN (both four-digit numbers) in addition to a d ACCOUNT (a.k.a. docomo ID) password, and we have been actively expanding the use of biometrics as a convenient authentication method to consolidate them.

One major reason we chose FIDO standards for introducing biometric authentication was to differentiate our DOCOMO branded devices from other devices. At that time, biometric sensors were not commonly equipped on smartphones, and DOCOMO launched the world's first iris scanner equipped device in May 2015, when d ACCOUNT Biometric Authentication was introduced. The FIDO Authentication model introduces the authenticator architectural concept, i.e., the separation of local verification (checking whether the user is the owner of the authenticator, e.g., a smartphone) from online authentication utilizing public-key cryptography without passing any shared secrets. This separation enables us to make our product portfolio more attractive with various smartphone models equipped with different types of biometric sensors, such as fingerprint sensors and iris scanners while deploying only one FIDO server for d ACCOUNT Biometrics Authentication across all FIDO certified

*2 FIDO®: A trademark or registered trademark of the FIDO Alliance.
*3 Phishing site: A Web site that accurately mimics a corporate Web site or other public site, tricking users into entering their IDs, passwords or other personal information.
*4 dmarket®: A trademark or registered trademark of NTT DOCOMO, INC.
*5 sp-mode®: A trademark or registered trademark of NTT DOCOMO, INC.

devices.

Another major reason for choosing FIDO Authentication is that it provides superior security. FIDO Authentication does not pass any shared secrets such as biometric data or passwords over the network, and it is resistant to phishing attacks. Therefore, we were motivated to make the best use of FIDO standards to improve d ACCOUNT security through eliminating passwords in the future in addition to the ease of use afforded by d ACCOUNT Biometric Authentication from the beginning [1].

We could not eliminate passwords when we deployed d ACCOUNT Biometric Authentication for several reasons, including the lack of coverage of authenticators; only four smartphone models supported FIDO Authentication, and only a limited number of customers had started using biometric authentication. Problems such as unresponsive fingerprint sensors also had to be considered. As a result, it was too early to disable passwords. We thus had to coexist with conventional password authentication for the time being.

2.1 Architecture and FIDO UAF Adoption

When introducing d ACCOUNT Biometric Authentication, we adopted the FIDO UAF 1.0*6 standard, which was published by the FIDO Alliance in December 2014. We added support for FIDO UAF 1.0 to the existing d ACCOUNT authentication server and to the already launched FIDO authenticators with the d ACCOUNT Settings application installed.

The d ACCOUNT Settings application is designed to handle authentication requests from various DOCOMO and partner services through the Web or from native applications. There are over 100 such services using d ACCOUNT authentication. These services and the native applications are linked with the d ACCOUNT Settings application to provide a single-point, integrated interface with the d ACCOUNT authentication server.

By incorporating a FIDO UAF 1.0 client into the d ACCOUNT Settings application and also requiring device manufacturers to implement FIDO Authentication in DOCOMO branded smartphone and tablet devices, we were able to smoothly deploy FIDO Authentication for d ACCOUNT.

2.2 Identity Proofing for d ACCOUNT Biometric Authentication

With d ACCOUNT Biometric Authentication, DOCOMO subscribers must enter their Network PIN when they configure their smartphone or other device equipped with a biometric sensor as their FIDO authenticator. This ensures that the biometric information used for online authentication is really from the person being authenticated for the d ACCOUNT. As such, FIDO Authentication can only be configured after verifying the user's identity, and the result of verifying their identity can be bound to the FIDO authenticator with certainty.

1) Network PIN and Identity Proofing

The Network PIN is a four-digit number that a user enters when they place an order at a DOCOMO shop or with DOCOMO Online.

As a mobile network operator, DOCOMO has been maintaining and operating the business infrastructure required to verify identities when a customer subscribes to our services, in compliance with regulations aimed at preventing improper use of mobile phones in Japan. There are several ways

*6 FIDO UAF 1.0: UAF stands for Universal Authentication Framework and was designed for passwordless authentication. Published in December 2014.

a person's identity can be checked: by checking the form of identification they present in-person at a DOCOMO shop, by sending an item such as a mobile phone to the address on the identification through registered mail, which only the addressee can receive, or by using the Network PIN number issued to the person when they subscribed to a phone line, which required them to present proof of identity at a DOCOMO shop.

To check a person's identity by using the Network PIN number, the number must be entered on a mobile device that is connected to the DOCOMO subscriber line and that has the Subscriber Identity Module (SIM)*7 card for the subscribed line inserted. The SIM card is unique and cannot connect without a valid contract, so that in itself provides strong authentication of ownership of the SIM card for the person's subscribed line, which is known as "SIM authentication." The four-digit PIN entered is not transmitted over the Internet; it is passed only within DOCOMO's local network. In contrast with ordinary passwords, the Network PIN provides strong multi-factor authentication based on SIM authentication and information known only to the subscriber. As such, it is a highly robust, online way of checking identity.

2) d ACCOUNT Biometric Authentication for non-DOCOMO Subscribers

d ACCOUNT can be used by anyone, even if they are not a DOCOMO subscriber (a "carrier-free" customer), but in that case the Network PIN cannot be used for checking identity or authentication. Instead, a screen lock must be enabled on the customer's authentication device, and the d ACCOUNT password must be entered on the device before d ACCOUNT Biometric Authentication is configured under the assumption that the screen lock prevents a third party from having access to the device.

2.3 d ACCOUNT Authentication by Your Smartphone

When d ACCOUNT Biometric Authentication was announced with the tagline "Your Security, More Simple," a concept for the future was also announced with the tagline "Smartphone as Your Key to Life." This concept was to use a smartphone with biometric authentication for safer and more convenient authentication, even for services provided by devices that are not equipped with a biometric sensor.

At the time, there were fewer PCs equipped with biometric sensors than there are today. It was also very inconvenient to enter passwords on TV sets and set-top boxes, each time requiring many cursor operations using a remote control. Since d ACCOUNT "Authentication by Your Smartphone" was launched in January 2017, authentication on other devices such as PCs and set-top boxes can be done easily using a smartphone that supports d ACCOUNT Biometric Authentication without entering a password. Once such devices are preregistered, authentication can be performed by simply selecting an "Authentication by Your Smartphone" button in services or applications presented by those devices.

2.4 Expanding the Portfolio of Authentication Devices

Since d ACCOUNT Biometric Authentication was launched, we have been working to bring "Your Security, More Simple" to more users by quickly expanding the portfolio of FIDO Authentication

*7 SIM: An IC card used to store mobile operator subscriber information, such as the phone number.

compliant devices supporting d ACCOUNT authentication.

We first worked quickly to support iOS[*8]. Since iPhone®[*9] and iPad® devices equipped with Touch ID® were becoming popular, we added support for devices with Touch ID in March 2016 [2]. We also added official support for devices with Face ID® in December 2017.

We have also worked to increase support for Android™[*10] devices. From the beginning, DOCOMO worked actively with device manufacturers to gain their support of the FIDO UAF 1.0 standard. In parallel, since joining the FIDO Alliance [3], DOCOMO has worked to popularize devices supporting FIDO UAF and promote their adoption [4]. We contributed specifications for FIDO UAF 1.1[*11] so that manufacturers could develop Android devices that support FIDO Authentication applications using only the standard features of the new Android OS rather than requiring special OS customizations. We began providing devices supporting this authentication standard in November 2017 [5]. This reduced the burden on device manufacturers and helped ensure a continuous supply of devices supporting d ACCOUNT Biometric Authentication.

As a result, the number of Android and iOS devices supporting d ACCOUNT Biometric Authentication had expanded to 93 as of the end of 2019: 36 Android FIDO UAF 1.0 models, 32 Android FIDO UAF 1.1 models, and 25 iOS models.

3. Issues in Implementing d ACCOUNT Passwordless Authentication

We have achieved the goal of having almost all smartphone and tablet devices offered by DOCOMO support d ACCOUNT Biometric Authentication. With this as a foundation, now is a practical time to start providing an option to disable passwords for d ACCOUNT authentication.

d ACCOUNT Passwordless Authentication provides safer and more convenient online authentication, which prevents unauthorized access through stolen passwords and/or list attacks[*12] by third parties, and liberates users from the complexity of password management. However, there were still several issues with implementing passwordless authentication:

- How to migrate from biometrics+password authentication to passwordless-only authentication,
- What alternatives to offer for biometric authentication,
- How to recover access to d ACCOUNT if user's device is lost, stolen, or broken (the "account recovery issue"),
- How to support a variety of devices, and
- How to support the many services and applications that require d ACCOUNT passwordless-only authentication.

1) How to Migrate from Biometrics+Password Authentication to Passwordless-only Authentication

For security, it is desirable that all users use passwordless authentication, but the scope of migration and how migration is done must be studied carefully. Issues such as the effect on users that are accustomed to using passwords every day and ensuring continuity of user experiences for services must be considered.

2) What Alternatives to Offer for Biometric Authentication

Once a password is disabled, it will no longer

*8 iOS: A trademark or registered trademark of Cisco in the U.S. and other countries. Used under license.

*9 iPhone®: "iPhone," "iPad," "Touch ID" and "Face ID" are are registered trademarks of Apple Inc. However, "iPhone" is a trademark of AIPHONE Co., Ltd. in Japan as it is used under license.

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

*11 FIDO UAF 1.1: An extension to FIDO UAF 1.0 created in December, 2016. It makes use of a key attestation feature to enable device manufacturers to develop and provide FIDO UAF applications without requiring custom implementations for each device.

be possible to use the password as an alternative if the biometric sensor does not work, such as when a finger is injured. As such, an alternative method had to be ensured. According to a survey by DOCOMO, approximately 30% of users will not use biometrics, so it was necessary to prepare alternate ways for these users to use d ACCOUNT without passwords.

3) How to Recover Access to d ACCOUNT (the "Account Recovery Issue")

Once passwords are disabled, it is necessary to provide methods to configure a FIDO authenticator when changing devices or when a device is lost, stolen, or broken. These methods must also be easy to use for users and customer support representatives.

4) How to Support a Variety of Devices

There will be situations in which PCs, set-top boxes, and other devices are not equipped with a biometric sensor, or a second smartphone is used for d ACCOUNT authentication, so options for passwordless authentication on such devices also had to be considered.

5) How to Support the Many Services and Applications that Require d ACCOUNT Passwordless-only Authentication

Before d ACCOUNT Passwordless Authentication was deployed, not all services and applications using d ACCOUNT supported FIDO biometric authentication. There are services that require entering a set of d ACCOUNT ID and password onto a device for CRM (customer relationship management) at DOCOMO shops. There are also services and applications that are not linked to the d ACCOUNT Settings application as the single point for authentication. For these reasons, the side effects of disabling passwords must be considered comprehensively, and the availability of authentication methods must be ensured in such cases.

4. Design, Development, and Deployment

The goal of implementing d ACCOUNT Passwordless Authentication is to strengthen security, so it was designed to resolve the issues described above while maintaining convenience and being easy for users to use.

4.1 Overall Concept and Architecture

d ACCOUNT Passwordless Authentication was implemented on the basis of d ACCOUNT Biometric Authentication, which already utilizes FIDO Authentication standards.

A new option menu was added to the d ACCOUNT Settings application that allows users to disable their password for d ACCOUNT. Users can completely disable the d ACCOUNT password on the server by choosing this option. Also, the implementation of the passwordless authentication eliminated the password input field on each login or authentication screen of all the services and the applications that use d ACCOUNT authentication (**Figure 1**).

Initially, d ACCOUNT Passwordless Authentication is being offered only to DOCOMO subscribers. DOCOMO subscribers are able to use their Network PIN to verify their identity themselves, so the result of the identity proofing process (using Network PIN) is bound to the FIDO authenticator (smartphone, etc.). Once password authentication is disabled, online authentication using the appropriately configured FIDO authenticator is used

*12 Password list attacks: A type of cyber attack that attempts to gain unauthorized access to accounts using a list of illegitimately gained IDs and passwords.

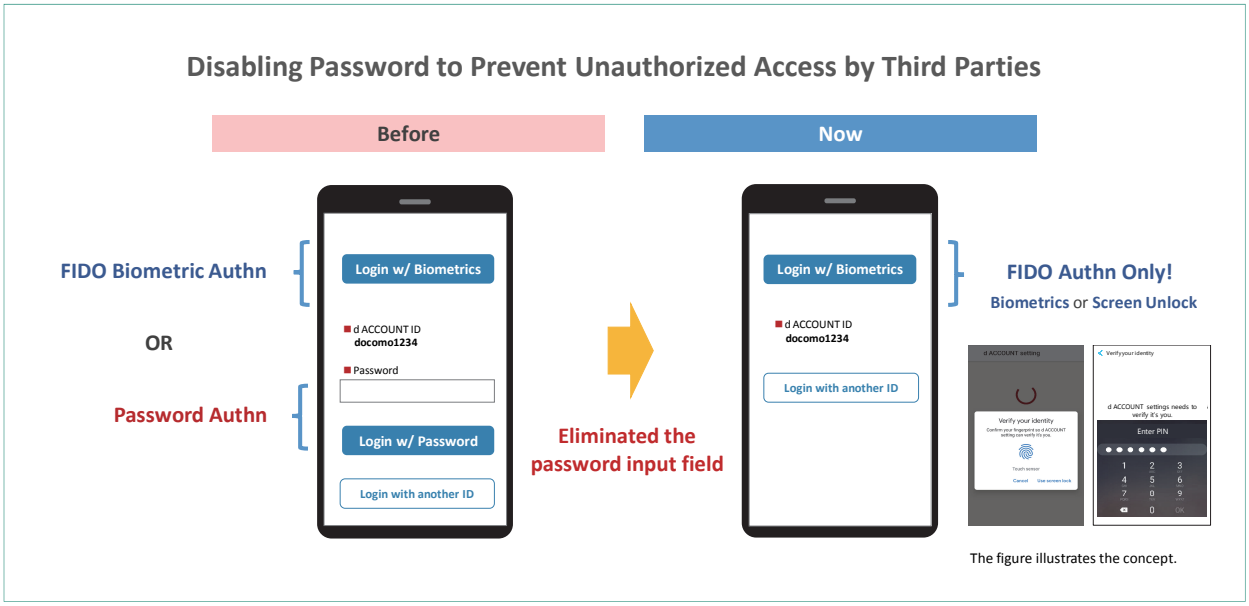

Figure 1 Overview of d ACCOUNT Passwordless Authentication

for passwordless authentication for login and other purposes including online payment and identity verification, thereby solving password-related security problems.

4.2 Configuration for Transition to Passwordless Authentication

Since the goal is to strengthen security, it is desirable that as many users as possible disable their passwords. However, considering the disruption to users accustomed to using passwords, we introduced the menu item to disable their passwords as an opt-in*13 feature.

Migration to d ACCOUNT Passwordless Authentication requires an update to the d ACCOUNT Settings application pre-installed on devices supporting d ACCOUNT Biometric Authentication. Users must turn on the password disabling option themselves from the new "Disabling Password" menu item.

Users that have already configured d ACCOUNT Biometric Authentication only need to perform biometric authentication once, when they turn on the "Disabling Password" option. Users that have not configured biometric authentication can complete the configuration by entering their Network PIN. Thus, users can easily disable their d ACCOUNT password (**Figure 2**).

Note that if necessary, the password disabling option can be returned to the OFF setting in the d ACCOUNT Settings application in the same way as turning it ON.

4.3 Support When Biometric Authentication Cannot Be Used

1) Using Screen Unlock

Some users will not use biometric sensors even if they have a device that supports biometric authentication, and there are cases in which the sensor cannot be used, such as finger injuries. As such,

*13 Opt-in: Use of a feature or setting is optionally permitted by the user.

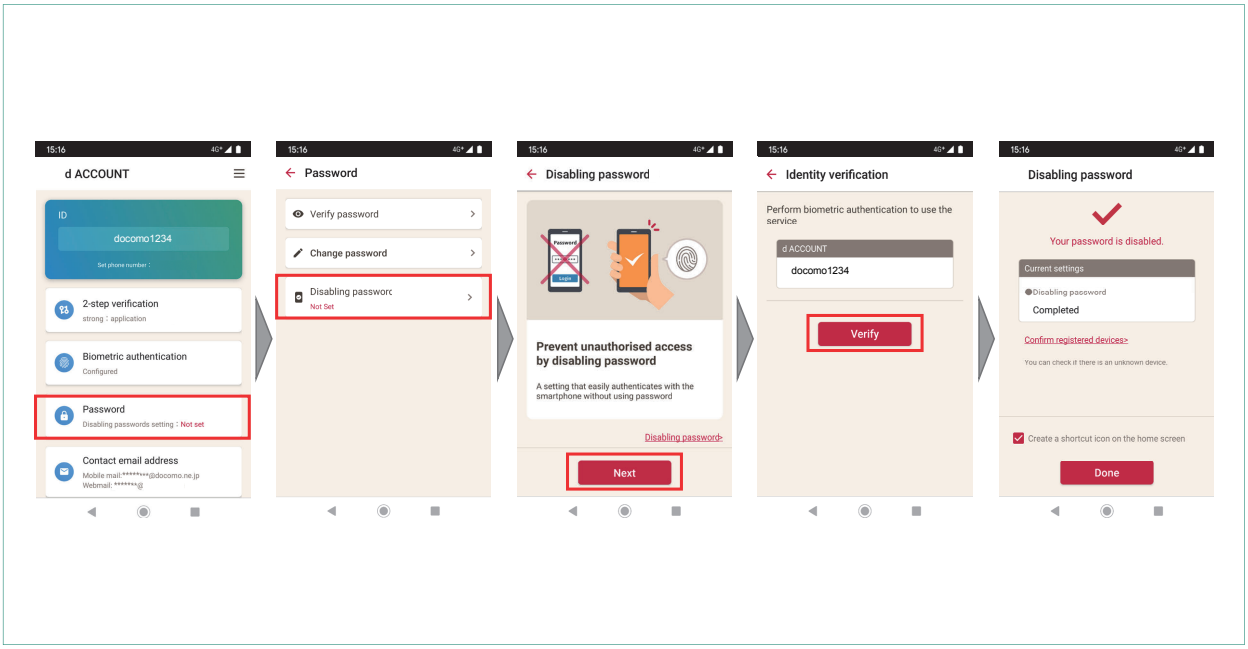

Figure 2 Screen shots of disabling password by d ACCOUNT settings application

it was necessary to consider passwordless authentication implementations that do not use biometrics. The key feature of FIDO Authentication is that the part between the user and authenticator (smartphone, etc.), which verifies the user's identity locally, is completely separated from the part between the authenticator and server, which utilizes public-key cryptography. Therefore, the FIDO authenticator should be able to verify the user's identity not only by using biometric authentication but also by using information that only the owner of the device should know, such as the local PIN used to unlock the screen.

Fortunately, recent smartphone OSs have been implemented securely, using information known only to the user to unlock the screen, and this feature is available for use by applications. Thus, instead of biometric authentication, d ACCOUNT Passwordless Authentication can verify the user's identity for d ACCOUNT login or purchases using the local PIN, passcode, or pattern that is used to unlock the screen.

Note that, as mentioned earlier, d ACCOUNT Passwordless Authentication was initially launched for DOCOMO subscribers, so if such users cannot use biometric authentication, they are able to verify their identity by entering their Network PIN as an alternate method. As the next step, d ACCOUNT Passwordless Authentication using the screen lock feature was added later.

2) Migrating from FIDO UAF to FIDO2*14 [6]

On Android devices, the d ACCOUNT Settings application was updated from FIDO UAF 1.1 to FIDO2 in order to implement authentication with the screen lock feature. For Android version 7.0 and subsequent versions, the FIDO2 implementation became a standard feature, so the local PIN, passcode, or pattern used by the device screen

*14 FIDO2: A set of specifications for supporting the FIDO model on platforms, to promote the broader use of FIDO Authentication. The FIDO Alliance proposed the Client to Authenticator Protocol (CTAP), which it created, and W3C created the Web Authentication API. The initial version of the Web Authentication API formally became a recommendation in March 2019.

lock feature can be used to verify the identity of the user (**Figure 3**). In the future, FIDO2 adoption will enable us to provide d ACCOUNT Passwordless Authentication to users that are not DOCOMO subscribers because FIDO2 has become a standard feature as of Android 7.0.

To enable login to a d ACCOUNT or to verify a user's identity using the Android screen lock feature, the d ACCOUNT Settings application must be updated by migrating from FIDO UAF 1.1 to FIDO2.

This migration is simple, requiring just one additional screen in the d ACCOUNT authentication process. This screen advises that d ACCOUNT authentication using the screen lock in addition to biometric authentication will be enabled, and the user must touch the fingerprint sensor to register the change to FIDO2. Thus, the user does not need to be concerned with changes in the FIDO specifications (**Figure 4**). This feature is scheduled to be available starting in June 2020.

Note that devices supporting FIDO UAF 1.0 that required device manufacturers to implement special customization of the Android OS in order to support the FIDO authenticator requirements are exempt from this FIDO2 migration requirement.

4.4 Recovering Accounts when Devices are Lost and Resetting Accounts

When changing to a new device, the user must reconfigure their d ACCOUNT on the new device. Users that have configured d ACCOUNT Passwordless Authentication have passwords disabled, so their password cannot be used to verify their identity. Nevertheless, they are able to verify their identity using their Network PIN to complete the reconfiguration, similarly to how they configured it initially.

When a device is lost, users can follow the standard DOCOMO procedure for lost devices, which has

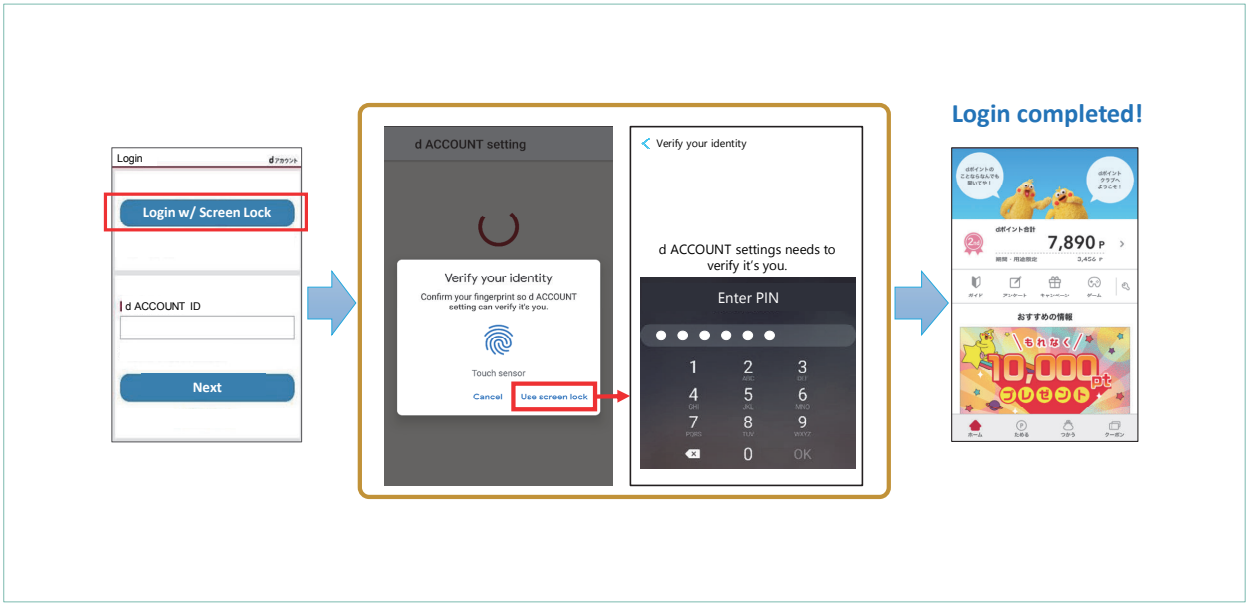

Figure 3 d ACCOUNT Passwordless Authentication with screen unlock feature (example of FIDO2 on Android device)

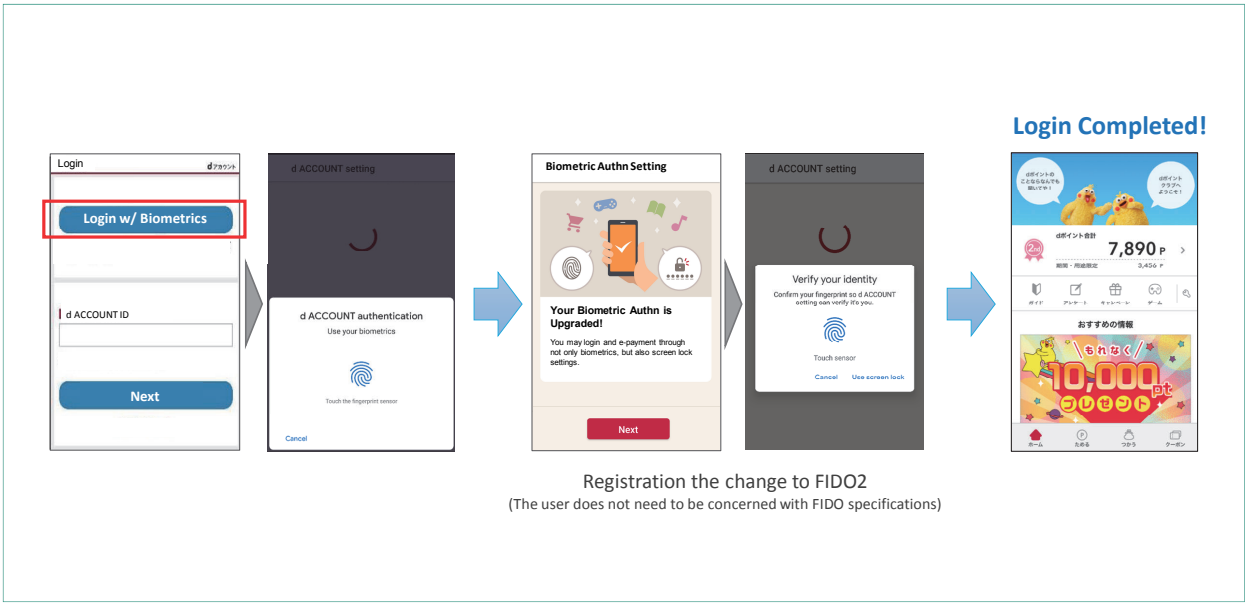

Figure 4 Screen shots of migrating from FIDO UAF 1.1 to FIDO2 (on Android device)

proven effective, even for d ACCOUNT Biometric Authentication. If the user's SIM card is reissued and they obtain a new device, d ACCOUNT Passwordless Authentication can be reconfigured as described above by entering their Network PIN to verify their identity.

Note that if the user cancels their DOCOMO contract, the password disable setting will automatically revert to OFF in the current implementation.

4.5 Supporting a Variety of Devices

With the migration from FIDO UAF to FIDO2, d ACCOUNT Passwordless Authentication is designed and implemented to allow using the device screen lock feature in cases when biometric authentication cannot be performed and also on devices not equipped with a biometric sensor.

In use cases for logging on a device that does not have a biometric sensor, such as PCs, TV sets, and set-top boxes, d ACCOUNT Passwordless Authentication also supports the Authentication by Your Smartphone mechanism described above. By configuring this mechanism beforehand, users can simply select a d ACCOUNT authentication button on a service or application provided by a nearby device such as a PC or set-top box, and the authentication request will be sent to the smartphone configured for d ACCOUNT Passwordless Authentication. The user can then authenticate easily on the smartphone using biometric authentication or the screen lock feature without entering a password (**Figure 5**). The required prior settings also have mechanisms to prevent spoofed authentication requests by third parties.

A d ACCOUNT that is configured for passwordless authentication (password is disabled) can be used for multiple devices. If a user has multiple phone lines, a single d ACCOUNT can be associated with all of them. Thus, a user can configure

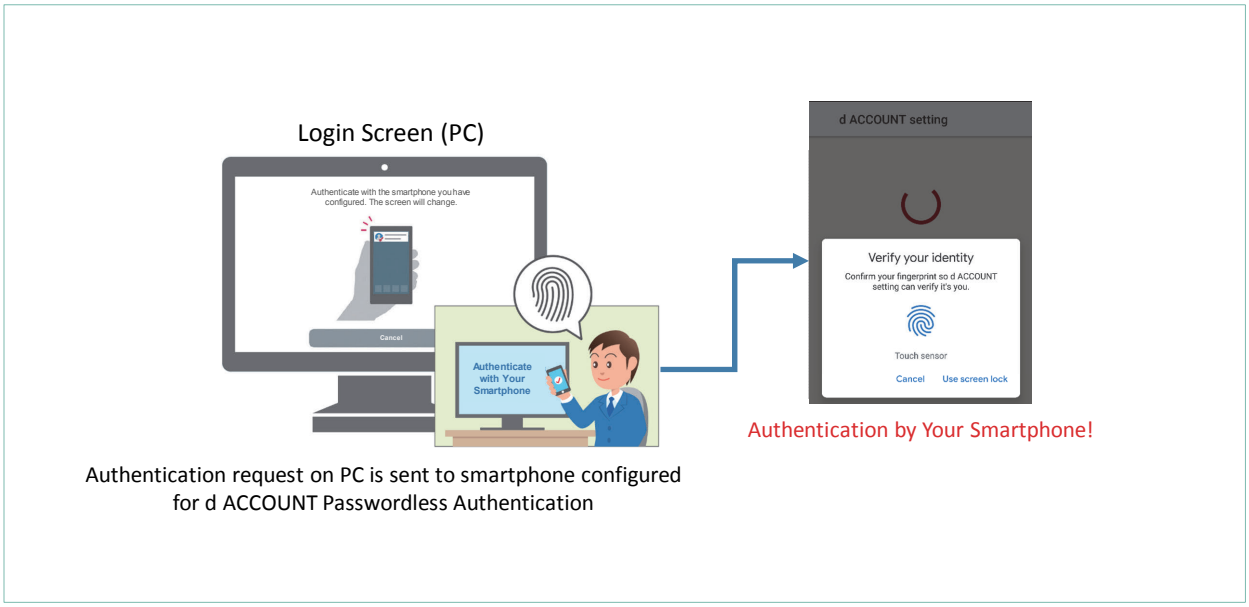

Figure 5 d ACCOUNT Passwordless Authentication by your smartphone

as many multiple FIDO authenticators as they have phone lines, and any of these devices can be used for d ACCOUNT Passwordless Authentication.

4.6 Supporting the Many DOCOMO Services and Applications

When designing d ACCOUNT Passwordless Authentication, we performed a comprehensive check and found that there were certain services and applications that were not ready for d ACCOUNT Biometrics Authentication through the single point of the d ACCOUNT Settings application. We decided to utilize the Authentication by Your Smartphone mechanism to resolve this issue.

That is, we treat services and applications that are not yet directly associated with the d ACCOUNT Settings application in a manner similar to that for devices not equipped with a biometric sensor—even on devices equipped with a biometric sensor. When a d ACCOUNT authentication button is touched in one of these services or applications, an authentication request is sent to the smartphone configured for d ACCOUNT Passwordless Authentication, and the authentication on the smartphone can be done without entering a password.

We have found that there are several scenarios on specific equipment where authentication by entering the d ACCOUNT ID and password is required, and we have resolved these in the same way, using the new Authentication by Your Smartphone mechanism.

5. Future Prospects

The d ACCOUNT Passwordless Authentication that we have begun offering is the first step toward realizing stronger security utilizing the FIDO Authentication standards.

Currently, d ACCOUNT Passwordless Authentication is an optional feature for moving from d ACCOUNT

with passwords to d ACCOUNT without passwords. We expect that in the future we will provide passwordless-only operation as the default even when a new d ACCOUNT is created; and not as an optional feature.

Many DOCOMO services are also provided to users that are not DOCOMO subscribers. These carrier-free users are also using d ACCOUNT in various ways, so we are considering how to support them as well.

We will continue initiatives to provide safer, more convenient d ACCOUNT Passwordless Authentication to even more users, using the various approaches described here.

6. Conclusion

In this article, we introduced d ACCOUNT Passwordless Authentication, which makes the best use of FIDO Authentication standards. We presented an overview of d ACCOUNT Biometric Authentication, which also utilizes FIDO Authentication and is used as a foundation for passwordless authentication. Then, we described its design, implementation, and deployment as a means to solve password problems. We also addressed future prospects.

With the introduction of d ACCOUNT Passwordless Authentication, DOCOMO has demonstrated how we should move from a world using IDs and passwords towards one not using passwords, which have long been taken for granted. By utilizing existing assets, we have begun offering functionality that enables d ACCOUNT to be used safely by a broad range of users, with simpler usability. With the constant news about unauthorized access and fraudulent transactions by third parties, FIDO Authentication is attracting more attention each year. DOCOMO will continue working toward creating a world without passwords, by providing advanced devices and developing services that actively make the best use of FIDO Authentication.

REFERENCES

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

[2] NTT DOCOMO: "Touch ID Support for d ACCOUNT Login and other Online Authentications," (In Japanese). https://www.nttdocomo.co.jp/info/notice/pages/160307_00.html

[3] K. Moriyama et al: "NTT DOCOMO's Contributions to Standardization of Online Authentication at the FIDO Alliance," NTT DOCOMO Technical Journal, Vol.22, No.1, pp.22–34, Jul. 2020.

[4] M. Hata and R. Lindemann: "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/

[5] FIDO Alliance: "First FIDO UAF 1.1 Implementations Ease Deployment of Advanced Biometric Authentication on Android Devices," Dec. 2017. https://fidoalliance.org/first-fido-uaf-1-1-implementations-ease-deployment-advanced-biometric-authentication-android-devices/

[6] W3C: "W3C and FIDO Alliance Finalize Web Standard for Secure, Passwordless Logins," Mar. 2019. https://www.w3.org/2019/03/pressrelease-webauthn-rec.html.en