NTT DOCOMO

Technical Journal

Vol.22 No.1 | Jul. 2020

NTT docomo

Dawn of the 5G Era

General Manager of 5G Business Office
Tsutomu Taguchi

In Japan, March 2020 marked the launch of commercial services for the fifth-generation mobile communications system (5G). Up to now, the mobile communications system has evolved to the next generation of technology about once every ten years, starting with the first-generation analog system and moving on the second-generation digital system, third-generation IMT-2000, fourth-generation LTE, and today's 5G. During this time, transmission speeds and network capacity have increased dramatically, which has helped to make our daily lives more convenient and, in industry, to increase productivity and foster the creation of added value. In 5G, even higher speeds and greater capacities will enable advanced media such as high-definition video transmission, Virtual Reality (VR), and Mixed Reality (MR) to be used in an exceptionally smooth manner. Furthermore, thanks to other features such as low latency and massive device connectivity, we can expect 5G to be used in the gaming field including esports that requires rapid reactions and in the Internet of Things (IoT) field that uses many and varied sensors.

The introduction of 5G should drive the evolution of the mobile communications infrastructure through these improvements in technical performance. It should also drive the evolution of the business infrastructure by facilitating the creation of new lines of business and the evolution of the social infrastructure by helping to solve pressing social problems and contributing to regional revitalization. The DOCOMO 5G Open Partner Program has been in operation since February 2018 to provide a boost to this evolution through the creation of services and solutions in collaboration with a wide range of companies and organizations, local governments in Japan, and research institutions including universities.

Some of these collaborative activities were presented at DOCOMO Open House 2020 held in Tokyo in January of this year. Many visitors to this event were able to learn about and comment on the achievements made so far by these activities.

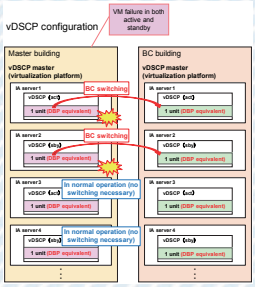
In this way, the 5G era will stimulate the creation of a wide range of services and industries, and we envision that a diverse array of devices in addition to smartphones and tablets will come into widespread use. For example, the use of Head-Mounted Displays (HMDs) to view VR video services via 5G smartphones or the use of future HMDs capable of 5G communications will enable users to have truly immersive and intuitive experiences in a mobile environment. In addition, the linking of high-definition cameras, wearable devices, sensors, and other types of devices should free us from the limitations of smartphone/tablet-based User Interfaces and User Experiences (UI/UX) and lead us into an era of truly novel experiences. Device vendors will find it easy to participate in a 5G ecosystem where a wide range of business opportunities will take form.

To meet customer needs that look to become increasingly diversified and sophisticated from here on, it will be vitally important to give birth to added value through cutting-edge ICT of the era and to determine how such added value should be used. Today, we anticipate future service and product designs that will make effective use of 5G as an important infrastructure supporting the next ten years and that will enable our customers to experience this added value.

NTT DOCOMO
Technical Journal
Vol.22 No.1 Jul. 2020

[Contents]

(P.10)



(P.35)

Technology Reports

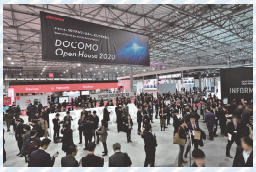
Subscriber Database Virtualization Supporting NTT DOCOMO Services 35

D-SCP | Virtualization | Reliability

Standardization

2019 ITU Radiocommunication Assembly 2019 (RA-19), World Radiocommunication Conference (WRC-19) Report 45

ITU | WRC | 5G

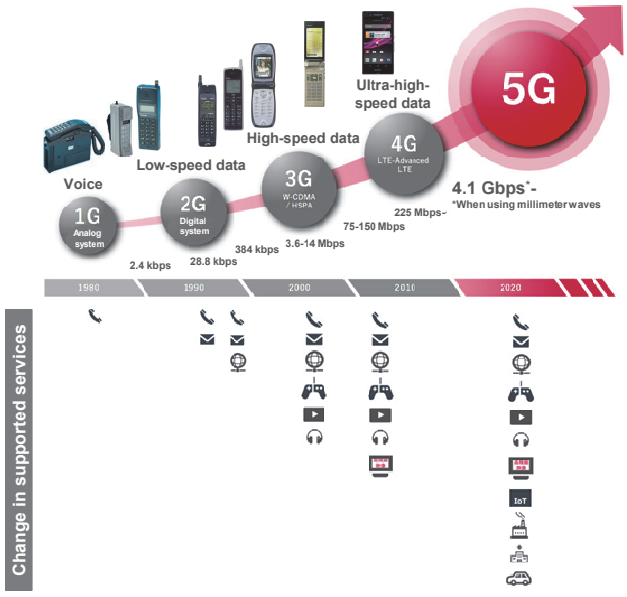


(P.52)

Event Reports

DOCOMO Open House 2020
—Dawn of the 5G Era and the Future Beyond— 52

5G | Open House | Exhibition Report



Technology Reports Overview of 5G Commercial Service (P.4)
Evolution of mobile communications system

Technology Reports
5G | High Speed & Large Capacity/Low Latency/Massive Connectivity | Service Commercialization

Overview of 5G Commercial Service

R&D Strategy Department Yu Kojo Taisei Kato
Takahiro Kawada Suguru Okuyama Aki Ohashi

NTT DOCOMO launched its 5G commercial service in March 2020. Featuring advanced communication specifications of high speed and large capacity, low latency, and massive connectivity, there are high expectations that 5G will provide a means of solving social problems, and from the industrial world, that it will be a force for creating new industries. This article describes 5G technical features and presents a system overview.

1. Introduction

NTT DOCOMO launched its fifth-generation mobile communications system (5G) in March 2020. Up to now, NTT DOCOMO has been unrolling its network in increasingly advanced versions, from its third-generation mobile communications system (3G) to its fourth-generation mobile communications system (4G), and within 4G, from LTE to LTE-Advanced, as data traffic increased with the spread of video content. We can expect this trend toward higher volumes of data traffic to continue into the future as large-capacity plans become popular and content like video and other services becomes enriched.

In addition, the 5G features of high speed and large capacity, low latency, and massive connectivity when combined with AI should make it possible to solve heretofore difficult social problems and create new industries thereby generating even higher expectations of mobile communications (**Figure 1**).

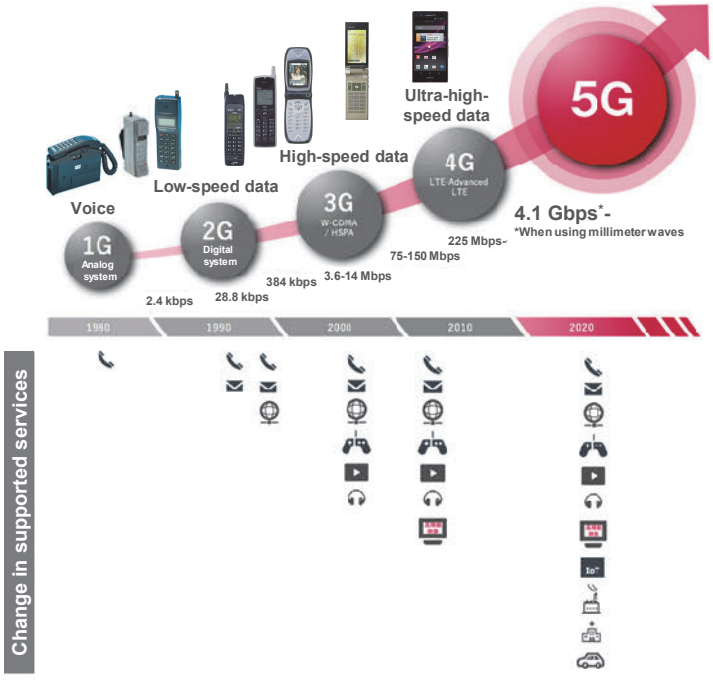


Figure 1 Evolution of mobile communications system

Prior to launching its 5G commercial service, NTT DOCOMO began basic 5G studies in 2010 and commenced high-frequency-band trials in 2014. Then, after contributing to early formulation of 3GPP standards for 5G in collaboration with major global mobile enterprises, NTT DOCOMO launched its 5G pre-commercial service in September 2019 creating many solutions together with co-creation partners.

Going forward, NTT DOCOMO plans to construct and roll out 5G service areas successively starting with major train stations/airports and stadiums in urban and regional areas as well as various types of facilities with partner collaboration in mind.

In this article, we describe 5G technical features, present a system overview, and take a look at supported services and terminals.

Special articles in future issues will take up the radio systems and core network technologies making up 5G, 5G base stations and other types of equipment and terminals, and associated platform technologies.

2. 5G Technical Overview

2.1 Three Technical Features

NTT DOCOMO aims to leverage the 5G features of high speed and large capacity, low latency, and massive connectivity to create a new world that no one has experienced before while making

our lives more convenient and comfortable. Each of these technical features is summarized below.

1) High Speed and Large Capacity

The 5G system will provide much higher broadband data transmission compared with the existing system. It will realize high-definition video including Virtual Reality (VR)*1 and Augmented Reality (AR)*2 experiences while enabling users to enjoy high-presence video and services as a familiar part of life.

The maximum receive speed will be 3.4 Gbps achieved through the use of various technical advances such as high-order Multiple Input Multiple Output (MIMO)*3 technology and the combining of many frequency bands. This value corresponds to the maximum receive speed at the time of the 5G commercial service launch as shown in **Table 1**, but NTT DOCOMO will continuously improve transmission speed through a variety of technical approaches including higher spectral efficiency.

2) Low Latency

In 5G, low latency will enable high-real-time control. For example, it can contribute to even higher levels of automation by determining current running conditions of plant facilities and machines and controlling and operating them in real time.

Also in 5G, the radio transmission unit has been shortened to one-half to one-eighth that of 4G depending on the frequency band, and the timing for confirming delivery has been positioned immediately after data transmission. These technologies combined are expected to achieve low latency in the radio interval compared with 4G. In addition, the adoption of Multi-access Edge Computing (MEC)*4 is expected to achieve low latency on an end-to-end basis.

Table 1 Maximum transmission speeds

	Launch Period	Speed		
LTE commercial service	December 2010	Receive		75 Mbps
		Transmit		25 Mbps
5G pre-commercial service	September 2019	Sub-6 GHz	Receive	2.4 Gbps
			Transmit	107 Mbps
		Millimeter wave	Receive	3.2 Gbps
			Transmit	202 Mbps
5G commercial service	March 2020	Sub-6 GHz	Receive	3.4 Gbps
			Transmit	182 Mbps
	June 2020 or later (plan)	Millimeter wave	Receive	4.1 Gbps
			Transmit	480 Mbps

*Transmission speeds are maximum receive/transmit values as listed in technical standards.

*1 VR: Technology for producing "virtual reality" using a computer.

*2 AR: Technology for superposing digital information on real-world video in such a way that it appears to the user to be an actual part of that scene.

*3 MIMO: A spatial multiplexing method where signals are transmitted using multiple transmitting antennas and received using multiple receiving antennas for increased transmission speed and transmission capacity.

*4 MEC: A system that installs servers at locations near users. Standard servers are typically placed on the Internet, but MEC servers are installed within the carrier network to reduce latency. This scheme greatly improves response speeds.

3) Massive Connectivity

In 5G, simultaneous connection of smartphones and a wide variety of things such as sensors and electronic devices will become possible thereby furthering the penetration of IoT and enhancing the use of information helpful to life (for example, 5G will enable the collection of inventory data in automatic vending machines or meter data on electricity, water, and gas usage without human intervention for use in analysis and later use).

At present, two systems—LTE-M*5 and Narrow Band (NB)-IoT*6—are in widespread use for achieving massive connectivity.

2.2 Major 5G Radio Technologies

1) Technologies for Achieving High-speed and Large-capacity Transmission

These technologies include high-frequency/ultra-broadband transmission*7 and antenna techniques typified by Massive MIMO*8 as described below.

(a) High-frequency/ultra-broadband transmission

LTE has been using frequency bands up to 6 GHz, but 5G looks to supplement those frequency bands with high frequency bands up to 100 GHz to achieve ultra-broadband capabilities. In particular, the high-frequency bands that include the 28 GHz band used by NTT DOCOMO's 5G pre-commercial service feature signal propagation characteristics*9 different than those of existing frequency bands, so new specifications appropriate for using high frequency bands have been specified and a basic bandwidth of 400 MHz has been set.

In addition, NTT DOCOMO is achieving high speeds and large capacities not only by using new frequency bands marked for 5G but also by using various combinations of existing 4G frequency bands simultaneously in radio transmissions.

(b) Massive MIMO

Massive MIMO is a technology that uses many antenna elements to control the shape of transmit/receive beams (beam forming) and configure an optimal area according to the environment. It can be used to expand an area by combining individual antenna elements and concentrating energy in one direction and to achieve a high-capacity system by simultaneously generating multiple beams to increase the number of simultaneously connected users.

2) Technologies for Achieving Low Latency

New Radio (NR), a newly introduced radio access technology, achieves even shorter delays in the radio interval by shortening the smallest unit of radio transmission. However, to achieve low latency in the provision of services, it will be necessary to shorten total delay including delay in core equipment and transmissions, so it will be important to shorten delay in both the radio interval and fixed-line interval. Specifically, end-to-end low latency can be achieved by combining 5G with MEC that deploys computing resources at locations close to terminals. The docomo Open Innovation Cloud™*10 that NTT DOCOMO provides as one form of MEC will be used to promote the creation of 5G services and solutions that make the most of low-latency technologies.

*5 LTE-M: An LTE communication specification for terminals that communicate at low speed using narrow bandwidth, for IoT devices (sensors, etc.).

*6 NB-IoT: An LTE communication specification for terminals that communicate at even lower speed and narrow bandwidth than LTE-M, for IoT devices (sensors, etc.).

*7 Ultra broadband: Bandwidth of 100 MHz or greater. In Japan, 400 MHz of bandwidth has been assigned in the 28 GHz band for 5G radio communications.

*8 Massive MIMO: A generic term for MIMO transmission technologies using very large numbers of antennas. MIMO is a signal technology that improves communications quality and spectral efficiency by using multiple transmitter and receiver antennas to transmit signals at the same time and same frequency.

3) Technologies for Achieving Massive Connectivity

These are IoT technologies that fall under the enhanced LTE (eLTE)*11 standard as part of the continuous evolution of LTE/LTE-Advanced. Here, the use of technologies such as LTE-M and NB-IoT introduced to simplify signal processing can achieve massive connectivity of IoT terminals (environmental sensors, meters, etc.) installed in a certain area where each terminal transmits small amounts of data with low frequency.

These technologies are specified in 3GPP Rel. 13 – 15. The IoT system in 5G NR is now under discussion for specification in Rel. 17. This system is expected to achieve low costs and low power consumption required of IoT by making use of NR features.

3. System Overview

3.1 Concept of 5G Deployment

NTT DOCOMO is moving forward with the deployment of 5G by combining NR, which achieves dramatic improvement in transmission speed and capacity performance using a wide range of frequency bands, and eLTE, which enables basic area coverage and services such as broadcast.

3.2 5G System Configuration

NTT DOCOMO has achieved its 5G service through a non-standalone*12 format in which terminals connect to the mobile network through both the NR and eLTE radio access systems. Specifically, it has leveraged the know-how obtained in deploying an Advanced Centralized Radio Access Network (Advanced C-RAN)*13 in LTE to provide high-speed communications through Dual Connectivity (DC)*14, which uses two radio access systems in an area in which both NR and eLTE can be used. A system configuration diagram of the 5G service is shown in **Figure 2**.

3.3 Multi-vendor Connections between Base Station Equipment

Up to now, specifications for interconnecting

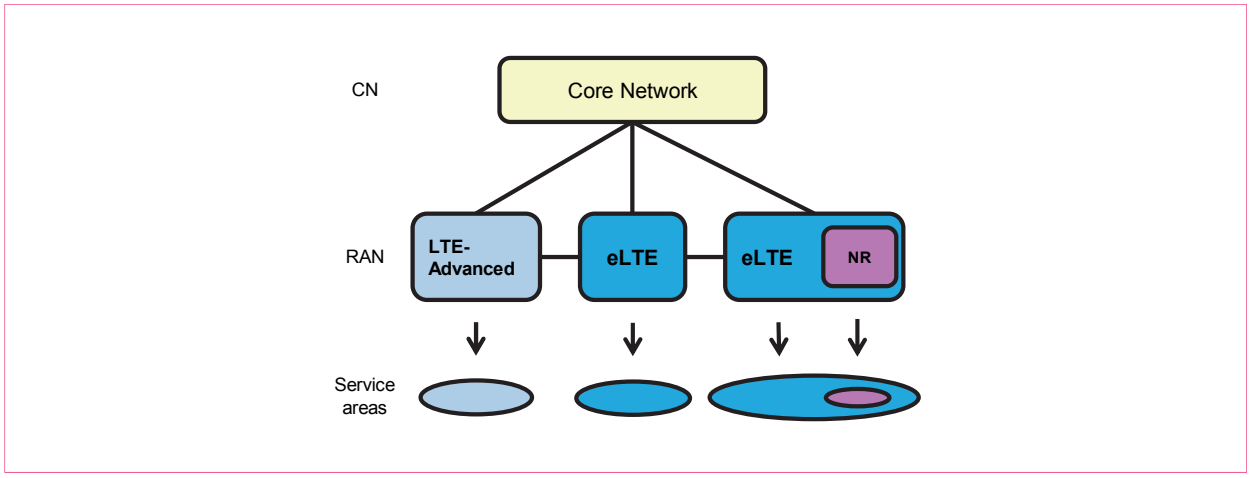


Figure 2 System configuration diagram

*9 Signal propagation characteristics: Refers to characteristics such as propagation losses, power and delay profiles, and angular profiles.

*10 docomo Open Innovation Cloud: A trademark or registered trademark of NTT DOCOMO.

*11 eLTE: An LTE communication specification conforming to 3GPP Rel. 15 or later.

*12 Non-standalone: An operation format that provides services through a combination of NR and an LTE area—in this format, a service area cannot be provided by NR alone.

*13 Advanced C-RAN: A new centralized radio access network (C-RAN) architecture proposed by NTT DOCOMO. Being controlled by the same base station, a radio access network makes a linkage between a macro cell (which covers a wide area) and a small cell (which covers a local area) by applying carrier aggregation.

base station equipment (signal send/receive rules) differed from vendor to vendor without sufficient consideration given to international standards. This situation made it difficult to interconnect base station equipment of different vendors so the usual approach was to interconnect base stations from the same vendor. However, in the 5G launch period, in which expansion of the 5G area would take place while using the existing 4G network, this approach would limit the vendors of 5G base station equipment that can be selected to vendors of 4G base station equipment. To solve this problem, the Open Radio Access Network (O-RAN) Alliance that NTT DOCOMO has been participating in promoted the international standardization of interoperability specifications between base stations thereby unifying interoperability specifications across 4G and 5G base station equipment and enabling multi-vendor connections.

These interoperability specifications have made it possible to deploy newly developed 5G base stations without having to rely on 4G base-station vendors and to achieve a speedy 5G rollout while using existing 4G assets.

4. Overview of 5G Commercial Services/Solutions and Terminals

In the 5G commercial service, NTT DOCOMO is providing a variety of services and solutions that exploit the 5G features of high-speed/large-capacity transmission including spectator support services such as multi-angle (multipoint) viewing and high-presence public viewing. The plan is to provide more new 5G services and solutions for the Olympic and Paralympic Games Tokyo 2021 and other events.

For the 5G commercial service, compatible terminals will perform NR communications using a 100 MHz bandwidth in the "sub-6" 3.7-GHz/4.5-GHz frequency bands and a 400 MHz bandwidth in the "millimeter-wave*15" 28 GHz frequency band. Using wide frequency bandwidths not available in past systems makes it possible to achieve the 5G feature of high-speed/large-capacity transmission. However, this also means high frequency bands in addition to wide frequency bandwidths, so there will be a need for radio terminals equipped with advanced antenna technologies that will enable high-frequency and ultra-broadband transmission not provided in past systems.

5. Conclusion

This article described an overview of NTT DOCOMO's 5G commercial service. NTT DOCOMO is committed to technology development with the aim of using 5G to create a new world with totally new experiences and to make all of our lives more convenient and comfortable.

REFERENCES

[1] T. Shimojo, et al.: "Future Core Network for the 5G Era," NTT DOCOMO Technical Journal, Vol.17, No.4, pp.50–59, Apr. 2016.

[2] A. Harada, et al.: "5G Trials with Major Global Vendors," NTT DOCOMO Technical Journal, Vol.17, No.4, pp.60–69, Apr. 2016.

[3] S. Abeta, et al.: "Radio Access Network in 5G Era," NTT DOCOMO Technical Journal, 25th Anniversary, pp.16–24, Dec. 2018.

*14 DC: A technology that connects multiple base stations and performs transmission and reception using multiple component carriers supported by those base stations.

*15 Millimeter waves: Radio signals in the frequency band from 30 GHz to 300 GHz as well as the 28 GHz band targeted by 5G that are customarily called "millimeter waves."

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.

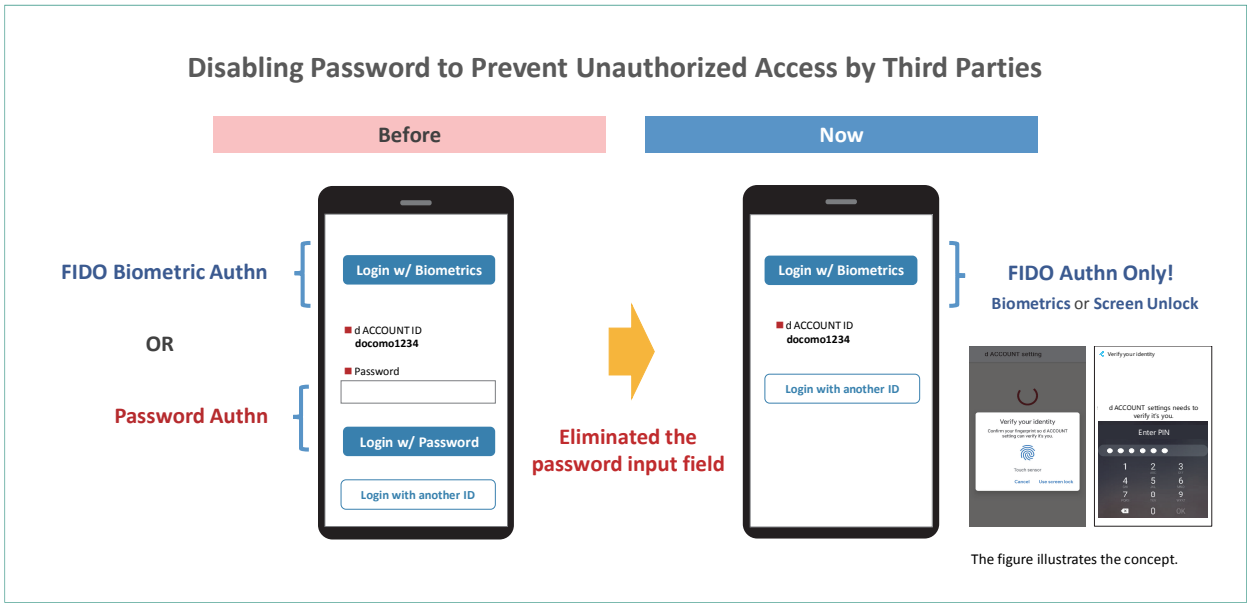


Figure 1 Overview of d ACCOUNT Passwordless Authentication

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.

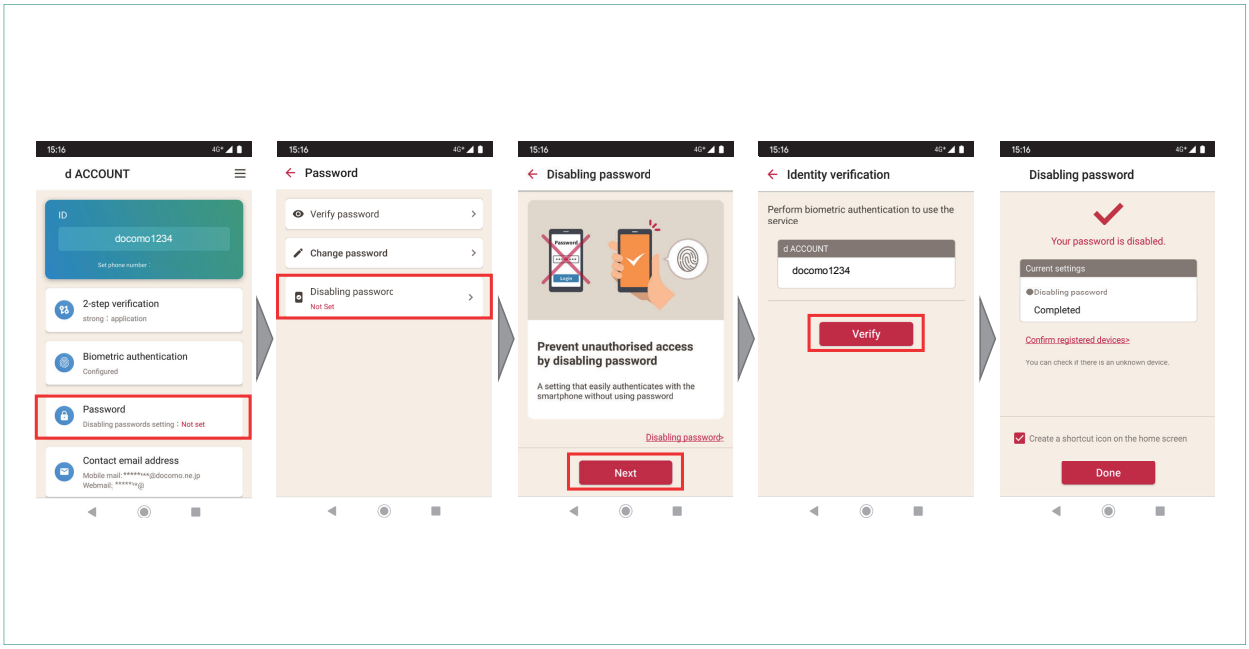


Figure 2 Screen shots of disabling password by d ACCOUNT settings application

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

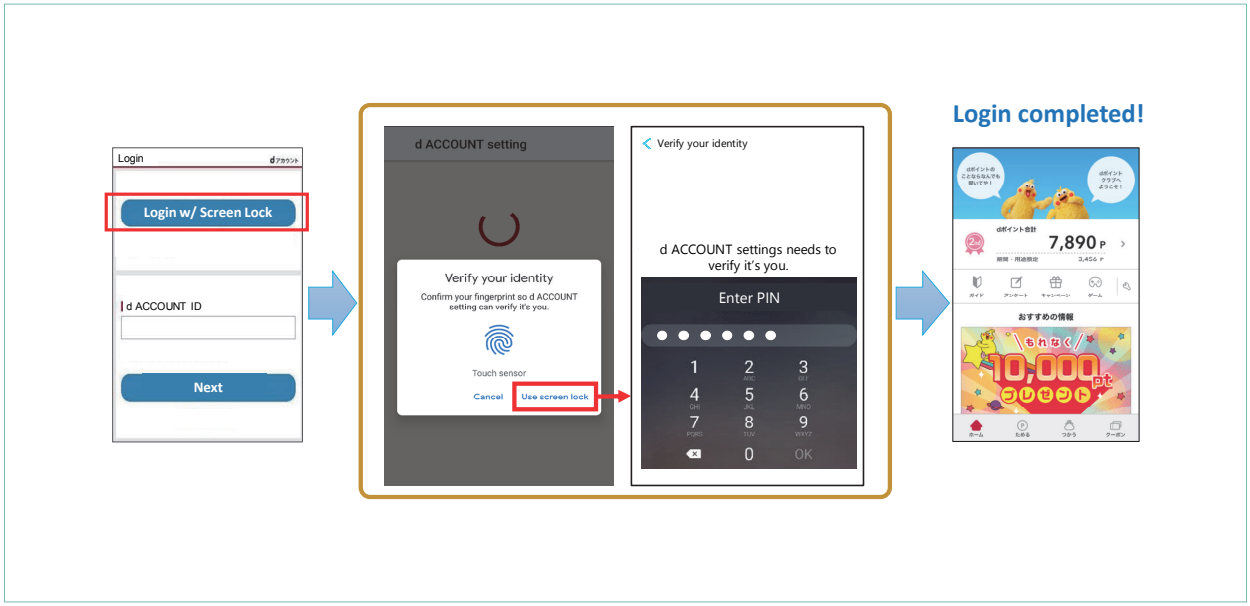


Figure 3 d ACCOUNT Passwordless Authentication with screen unlock feature (example of FIDO2 on Android device)

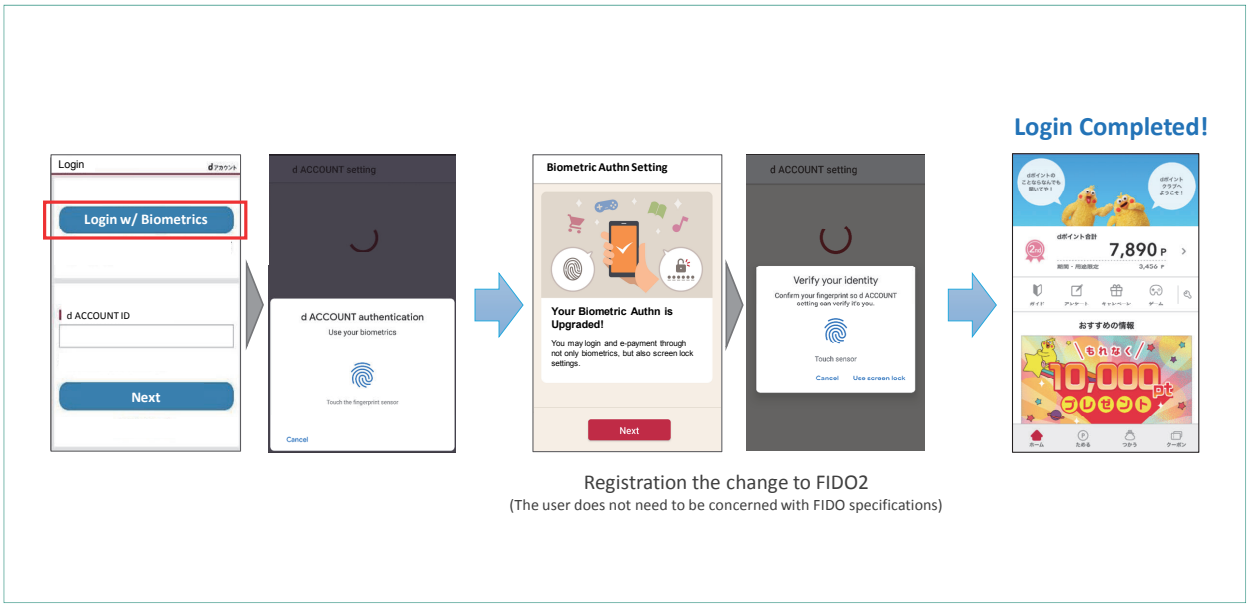


Figure 4 Screen shots of migrating from FIDO UAF 1.1 to FIDO2 (on Android device)

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

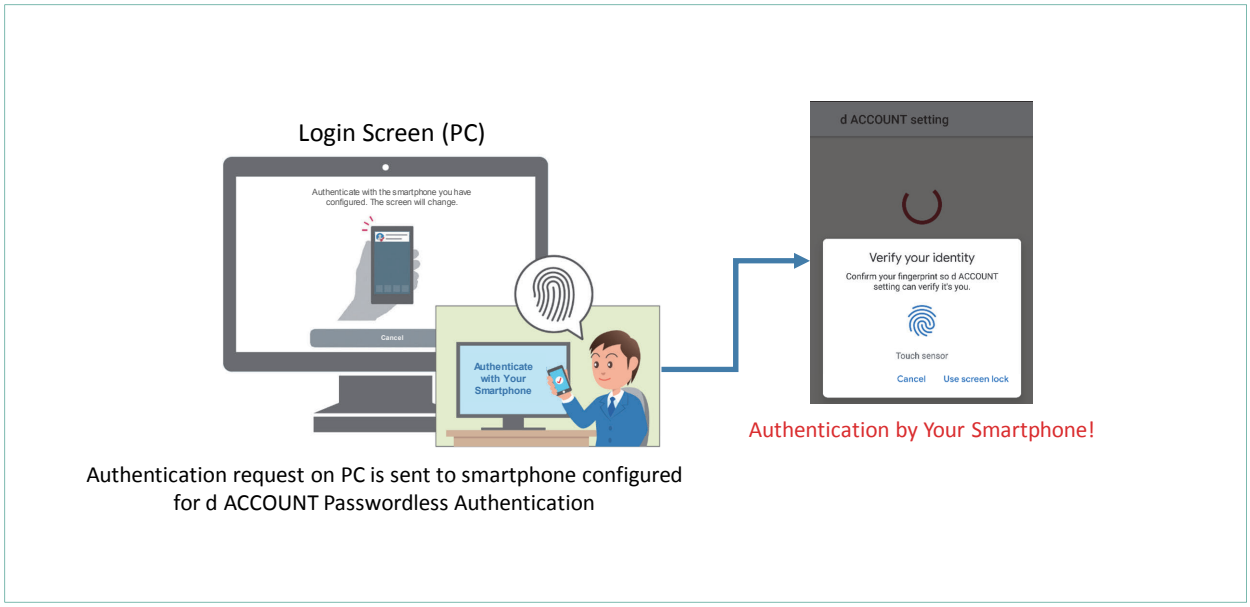


Figure 5 d ACCOUNT Passwordless Authentication by your smartphone

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

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

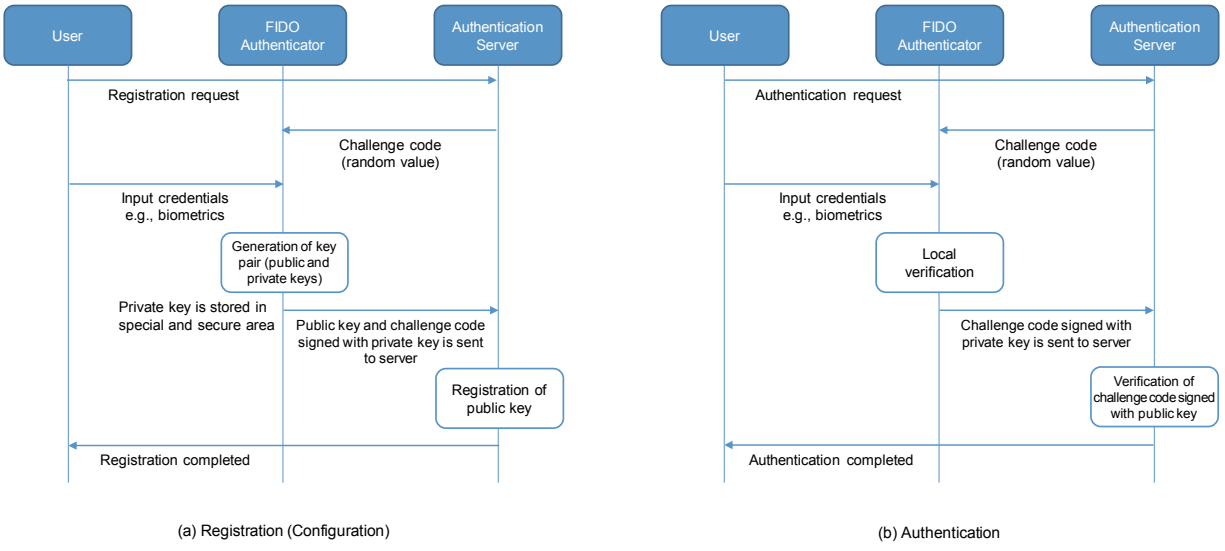


Figure 2 Sequence of FIDO Authentication – "Secrets" Never Passed over the Internet

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.

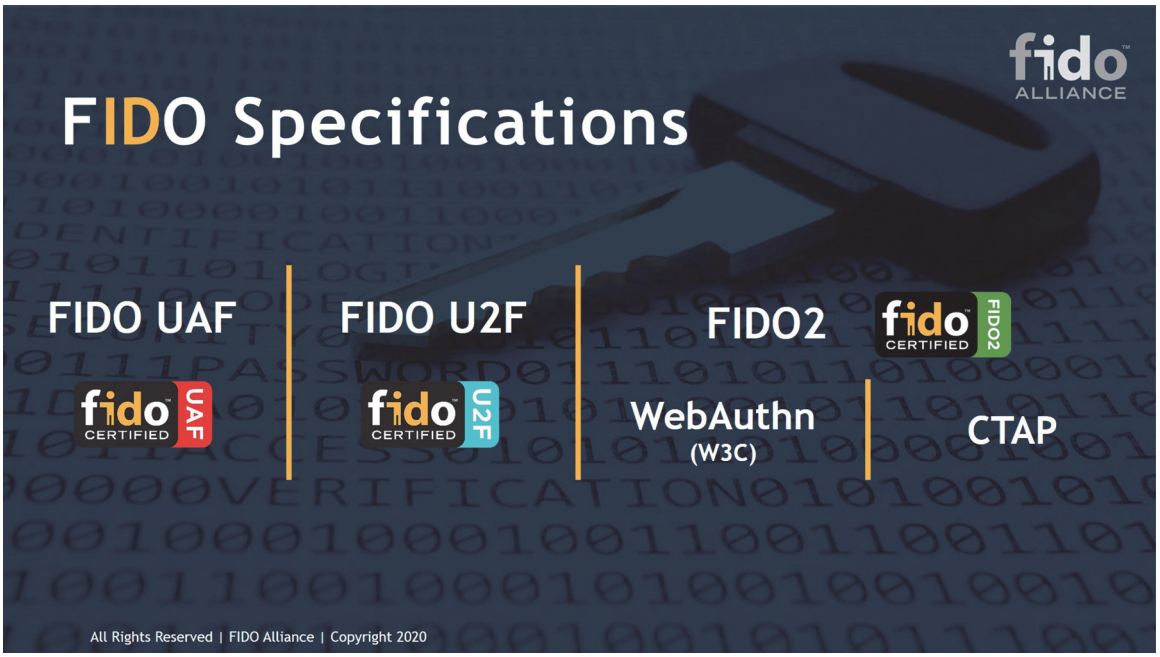


Figure 4 FIDO Specifications

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/

Technology Reports

D-SCP Virtualization Reliability

Subscriber Database Virtualization Supporting NTT DOCOMO Services

Core Network Development Department Shin Nishida Takuya Tsutsumi Kazuki Takayama† Yuji Fujimori

NTT DOCOMO supports the provision of diverse types of services in its core network by a service control equipment group. Here, the control of user (subscriber) information that must be carefully managed is handled by equipment called F-SCP (call-control function) and D-SCP (database function). Now, with D-SCP equipment reaching its EoL, we have applied network virtualization that NTT DOCOMO has been energetically promoting in recent years to this service control equipment group and have deployed successor equipment (vDSCP) with improved reliability and economy as benefits of virtualization.

1. Introduction

At NTT DOCOMO, the equipment that provides Home Location Register (HLR)*1 and Home Subscriber Server (HSS)*2 functions for managing user subscriber information and location information and performing location registration and call sending/receiving control in the mobile communications network is called a Service Control Point (SCP) group. Within this group, the call-control section and subscriber database function are achieved by equipment called Front end SCP (F-SCP)*3 and Database SCP (D-SCP)*4, respectively [1] [2].

Now that D-SCP hardware that has been operating commercially is reaching its End of Life (EoL)*5, it has become necessary to develop successor equipment.

With regard to network virtualization [3], NTT DOCOMO

† Currently Packet Network Division, DOCOMO Technology, Inc.

*1 HLR: A logical node defined by the 3GPP with functions for managing subscriber information and call processing.

*2 HSS: A subscriber information database on a 3GPP mobile network that manages authentication and location information.

*3 F-SCP: A unit of subscriber service control in charge of call control.

deployed virtualized Evolved Packet Core (vEPC)*6 in March 2016 and has since been applying network virtualization to core network*7 equipment. This application of virtualization to core network equipment is about 40% complete as of the end of fiscal year 2019 and continues to this day.

Virtualization provides a number of benefits. In addition to improving the reliability of communication services and the economics of network facilities, virtualization makes it easier to achieve connections during times of congestion and enables early provision of services. (**Figure 1** (1) – (4)). We developed D-SCP successor equipment in line with this policy of applying network virtualization.

This article describes revised equipment configuration and functional allotment in virtualized D-SCP (vDSCP)*8, the successor equipment to D-SCP, the benefits of network virtualization as applied to that equipment, and the mechanisms used for improving reliability and economy.

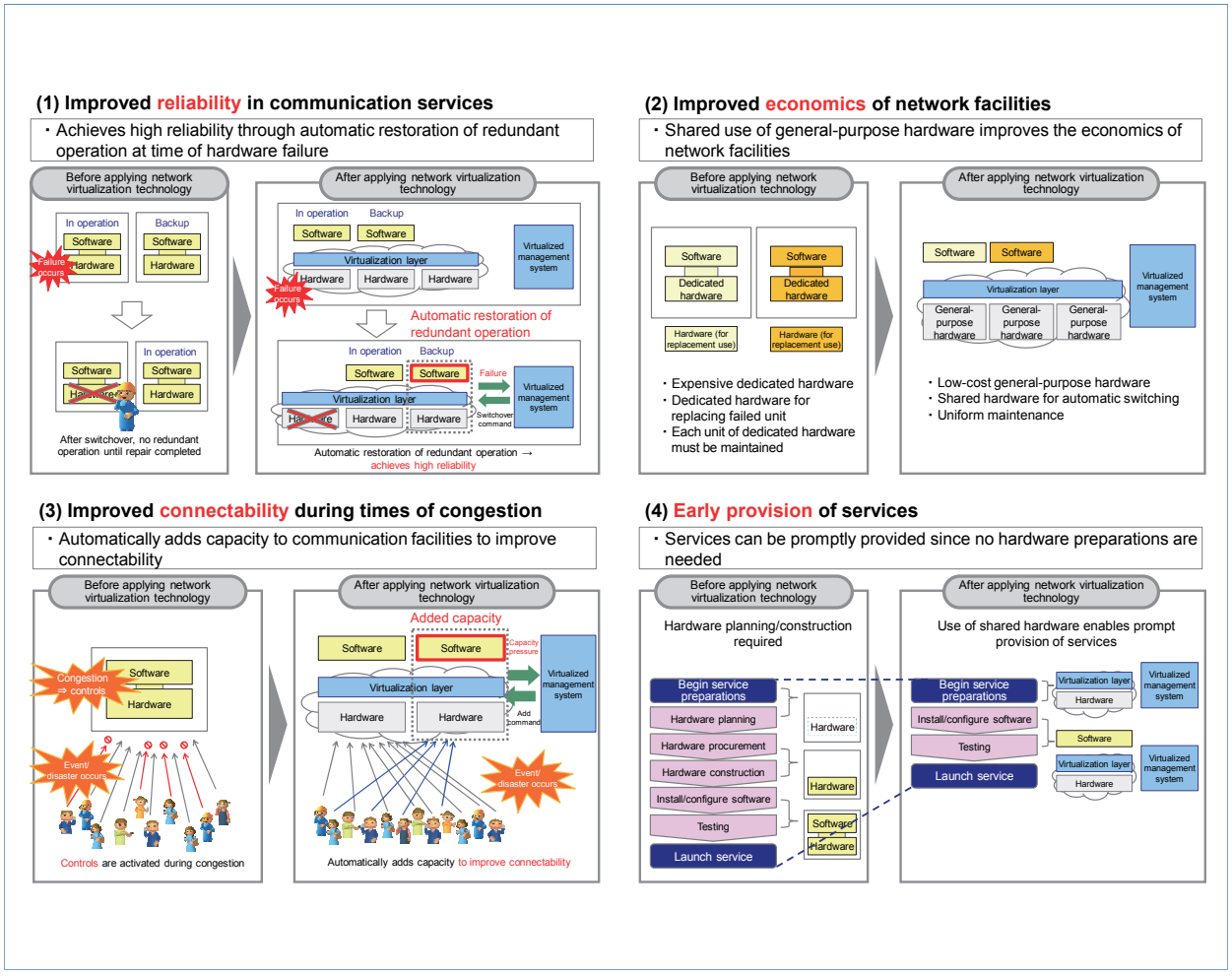


Figure 1 Benefits of network virtualization

*4 D-SCP: A unit of subscriber service control in charge of database functions.

*5 EoL: A term that refers to the end of sales, software support, and updates/revisions for certain products or services.

*6 vEPC: Communications software specified by 3GPP for LTE and other access technologies and provided to enable the EPC IP-based core network to function as a virtual machine (VM).

*7 Core network: A network consisting of switches, subscriber-information management equipment, and other devices. Mobile terminals communicate with the core network via the radio access network.

*8 vDSCP: D-SCP running on a virtualization platform. In this article, this name is also used to refer generically to vSSCP/vDSCP as a VNF.

2. Issues in Applying Virtualization to D-SCP

Given that virtualization is independent of the target hardware, it is relatively easy to support virtualization for stateless functions having no subscriber information on that hardware. At NTT DOCOMO, although control of subscriber information is achieved by F-SCP/D-SCP, F-SCP is a stateless function untied to subscriber information while D-SCP achieves control of subscriber information as a stateful function that holds states on hardware. Consequently, it is not sufficient to simply switch to another D-SCP at the time of a failure—it is also necessary to hand over the subscriber information being held (**Figure 2**).

Subscriber information is extremely important in a mobile communications network, so rapid restoration at the time of a failure is essential. However, in the event of a failure in a D-SCP applying

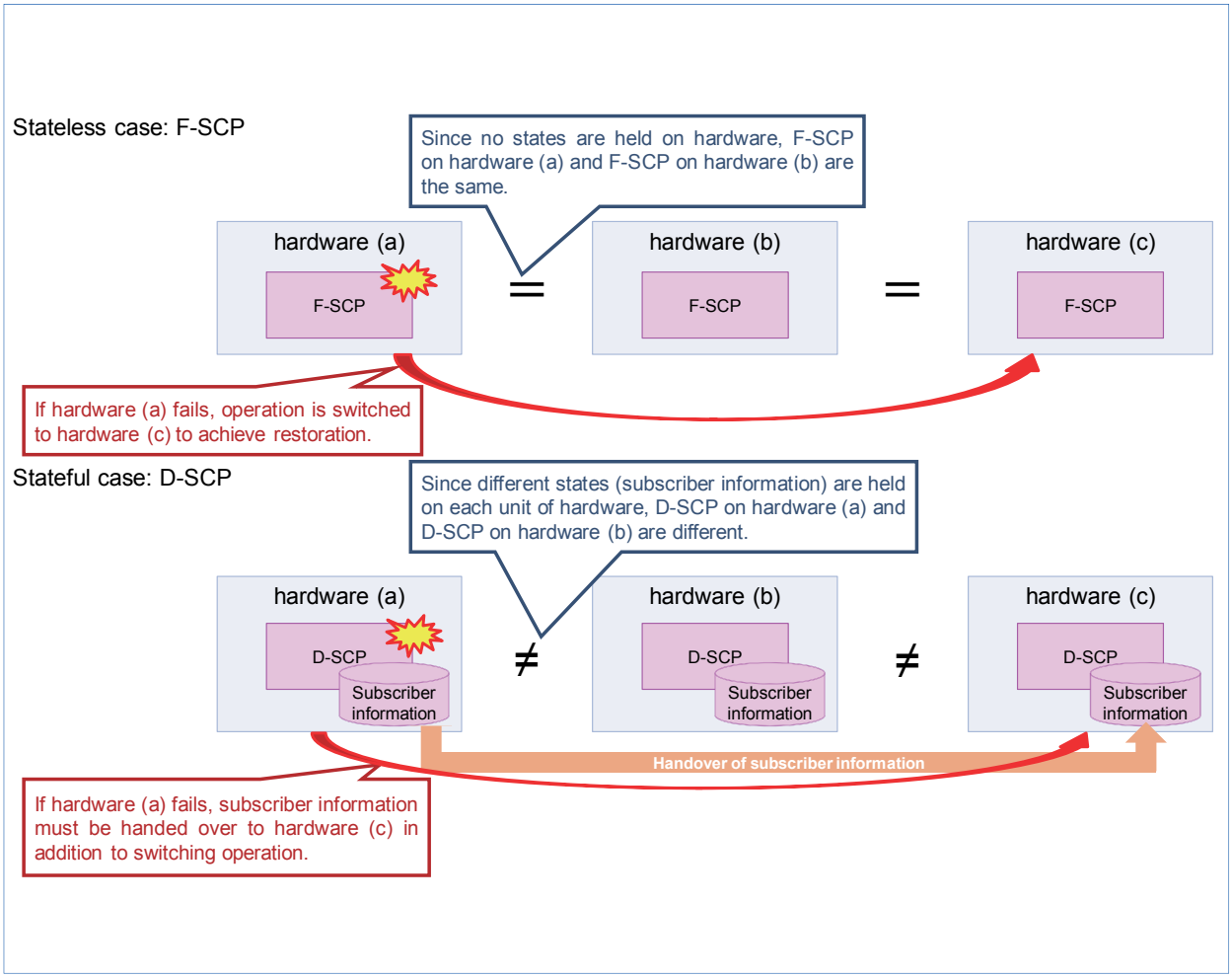


Figure 2 Operation overview at time of a hardware failure

virtualization, processing to synchronize a massive amount of subscriber information is required, but this presents a problem as some time is needed to complete this processing before restoration.

NTT DOCOMO has resolved this issue by implementing some functions on dedicated equipment.

3. Equipment Configuration

The hardware configuration of D-SCP and that of the vDSCP subscriber database after the virtualization upgrade are shown in **Figure 3**. Here, vDSCP is achieved by two Virtual Machines (VMs): Storage/System Manager (SM)*9 and DataBase (DB)*10.

(1) SM-VM in vDSCP corresponds to some of the File Server (FS)*11 functions for holding data related to D-SCP system maintenance operations and equipment control (system maintenance functions, restart control, etc.). The Virtual Network Function (VNF)*12 configured by SM-VM is called virtual SM for SCP (vSSCP)*13 that performs system and storage management.

(2) DB-VM in vDSCP includes the D-SCP Data Base Processor (DBP)*14 function as well as some FS functions (system maintenance functions, Backup Center (BC) switching control). The VNF configured by DB-VM is called narrowly defined vDSCP that performs call control, backup control, BC switching control, etc.

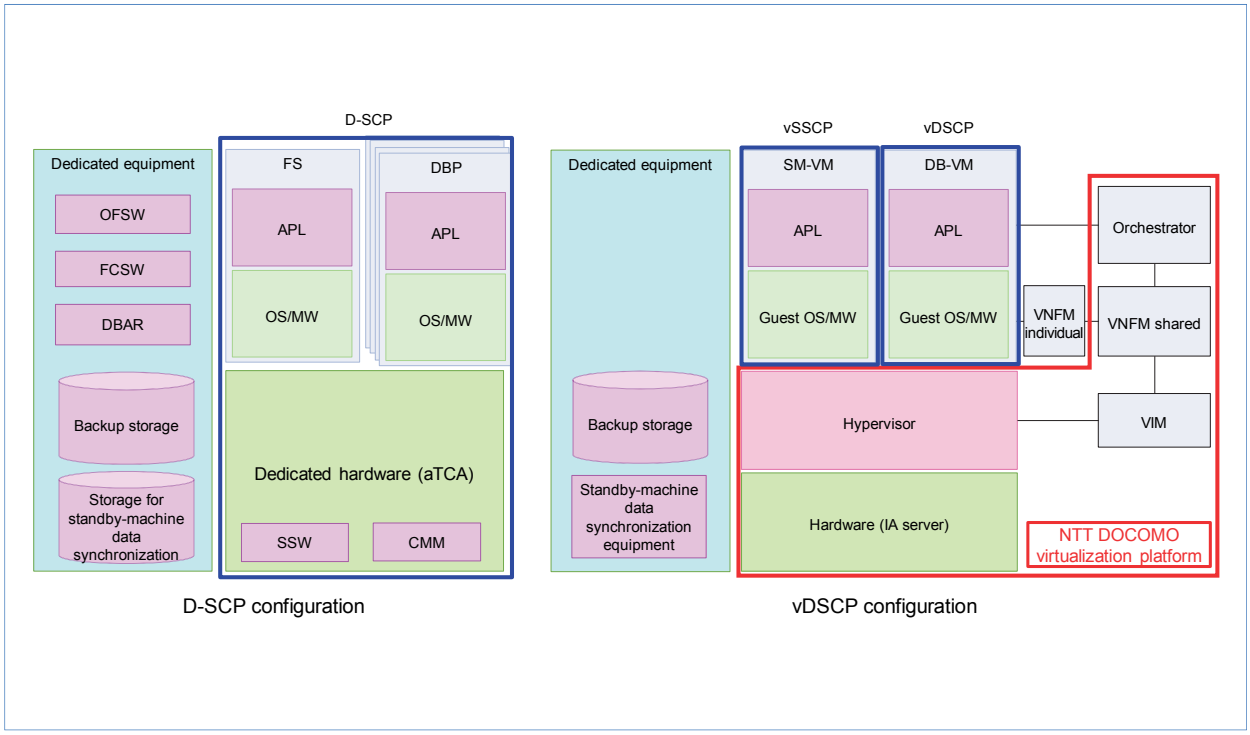


Figure 3 D-SCP and vDSCP hardware configuration

*9 SM: Functions that manage RAID and storage router capacity.
*10 DB: In this article, functions that perform call control, backup control, backup center switching, and relocation control.
*11 FS: Functions that hold data for system maintenance/operation and equipment management and that perform backups to RAID.
*12 VNF: A constituent element of an application running on the virtualization platform.
*13 vSSCP: The equipment that performs vDSCP system management and storage management.
*14 DBP: Database function for subscriber information.

Some of the dedicated hardware and dedicated equipment have been implemented as software-based applications and some have been migrated to the virtualized network side such as the virtual Layer 3 SWitch (vL3SW)*15. In this way, the internal Shelf SWitch (SSW)*16 of dedicated hardware and the Fiber Channel SWitch (FCSW)*17 and Data Base Access Router (DBAR)*18 of dedicated equipment have been virtualized and the Chassis Management Module (CMM)*19 of dedicated hardware and OpenFlow SWitch (OFSW)*20 of dedicated equipment have been discontinued.

As a result, operation of dedicated hardware becomes unnecessary, the shared use of general-purpose products such as IA servers*21 and vL3SW with other virtualized equipment becomes possible as did the lump procurement of such products, and expenditure on facility procurement and maintenance becomes more efficient thereby improving the economics of network facilities.

4. Functional Allotment between vSSCP (SM-VM) and vDSCP (DB-VM)

If the SM-VM supervising section can be made non-subordinate to the DB-VM database section, a configuration in which the number of SM-VMs and DB-VMs can be changed as needed becomes possible thereby inhibiting an SM-VM failure from affecting services. Furthermore, by having SM-VM perform system management without having to be aware of any differences in the DB-VM internal configuration, SM-VM development work in response to the future addition of new types of DB-VM can be minimized. The above configuration is superior in terms of both fault tolerance and extendibility, and for this reason, we adopted a scheme that separates SM-VM and DB-VM as independent vSSCP and vDSCP VNFs (= units) and allocates functions accordingly.

5. Application of Dedicated Equipment

The functions provided by D-SCP dedicated equipment (backup storage, storage for standby-machine data synchronization (HS3*22)) are also installed in vDSCP dedicated equipment (backup storage, standby-machine data synchronization equipment*23) without using functions on the virtualization platform while taking into account the capacity needed for the data being handled and the application using that data.

5.1 Backup Storage

At present, virtual storage provided by the virtualization platform does not support a multi-attach function that mounts a single volume by multiple VMs. For this reason, the system used up to now for data sharing between active/standby VMs in virtualized core network equipment has been to implement on VNF a data synchronization application called Distributed Replicated Block Device (DRBD)*24 and to synchronize data between the volumes in the active and standby systems. However, when using DRBD, there are cases in which total synchronization is necessary between the active and standby volumes such as at the time of a failure. In such a situation, a considerable amount of time is needed to complete this synchronization processing

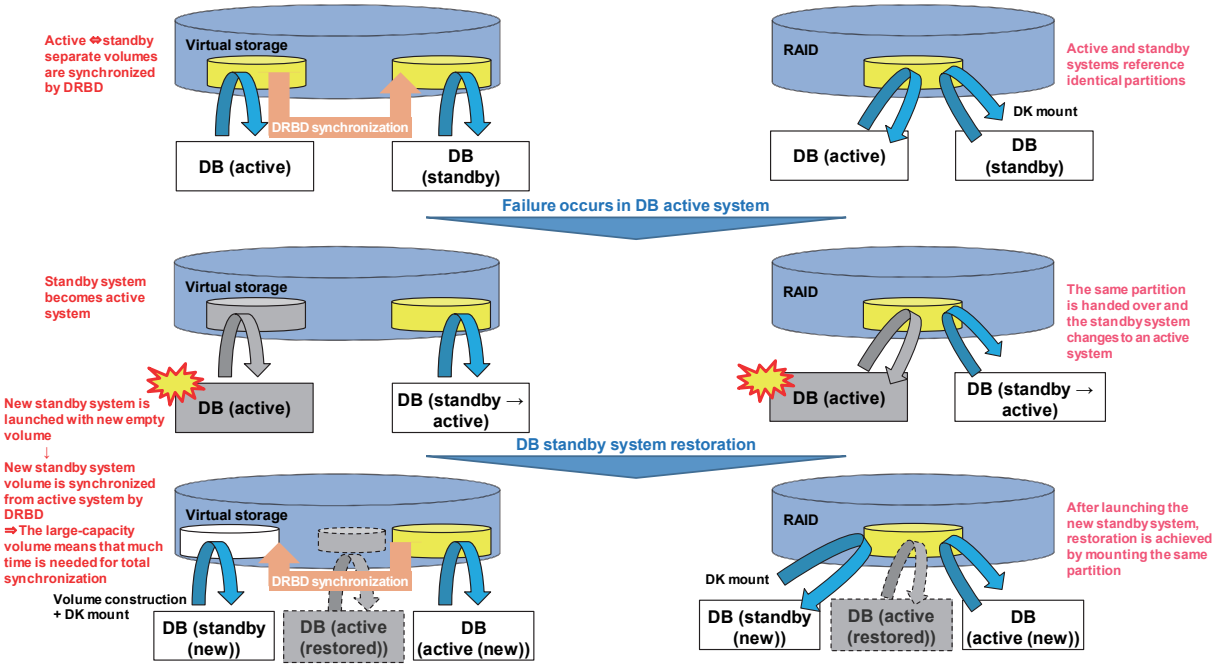
*15 vL3SW: A virtual switch for making L3 connections with service network equipment.
*16 SSW: An internal switch blade between FS and DBP in aTCA, an industry standard for operator-oriented next-generation communication equipment.
*17 FCSW: A switch between backup storage and DBP.
*18 DBAR: A router used for making connections with external associated equipment.
*19 CMM: Performs intra-chassis management in aTCA.
*20 OFSW: A switch having a function for directing an F-SCP seeking data access to the DBP accommodating the target subscriber data.

resulting in a single-system operation state during that period (**Figure 4** (a)). As a consequence, the large amounts and importance of subscriber information handled by vDSCP make using DRBD a risk, so we adopted dedicated storage equipment in vDSCP.

Here, dedicated storage is connected to a network accommodating a virtualization platform and database construction is achieved by mounting identical partitions via this network from both the active and standby DB-VMs, the same as the D-SCP system. Now, if a failure occurs in the active system, the same region is taken over by the standby system. The partition mounted in the current active system can then be mounted in the former active system to restore it thereby eliminating any synchronization time. This enables immediate launching while minimizing the single-system operation period (Fig. 4 (b)).

5.2 Standby-machine Data Synchronization Equipment

Similar to D-SCP, vDSCP installs one master unit that operates during normal times and two BC



(a) DRBD synchronization system

(b) vDSCP adopted system (equivalent to existing D-SCP)

Figure 4 Operation comparison between DRBD synchronization system and vDSCP adopted system

*21 IA server: A server equipped with an Intel microprocessor or an Intel compatible processor. Its internal structure is very similar to that of an ordinary personal computer, and it is less expensive than servers based on other types of microprocessors.

*22 HS3: External storage equipment used to store backup data within a unit and to perform replication with backup centers. Can also be used to store backup data from multiple units through replication with D-SCPs.

*23 Standby-machine data synchronization equipment: Equipment that performs data replication between remotely installed storage equipment.

*24 DRBD: Middleware for mirroring disk partitions among multiple Linux servers. DRBD is a trademark or registered trademark of LINBIT Information Technologies GmbH in Australia, United States, and other countries.

units in separate office buildings and features a function for switching to these BCs in the event of a master-unit fault that could hinder service continuity. To achieve this function, it is necessary to synchronize (replicate) subscriber-information backup data stored in backup storage between different office buildings, but virtual storage on the virtualization platform does not provide a synchronization function between volumes at different office buildings.

For this reason, it was decided to deploy dedicated standby-machine data synchronization equipment in vDSCP the same as that for backup storage. This equipment features a device having a data compression function for use in data transfers, which enables efficient inter-building synchronization without affecting VM call processing performance in comparison with a method that deploys no dedicated equipment and achieves synchronization by a VM application.

The vDSCP master/BC configuration and the backup file flow using the standby-machine data synchronization equipment are shown in **Figure 5**.

6. Benefits of Deployment

6.1 Minimization of Affected Users at Time of Failure

For a vDSCP that manages subscriber information, reducing as much as possible the effect of

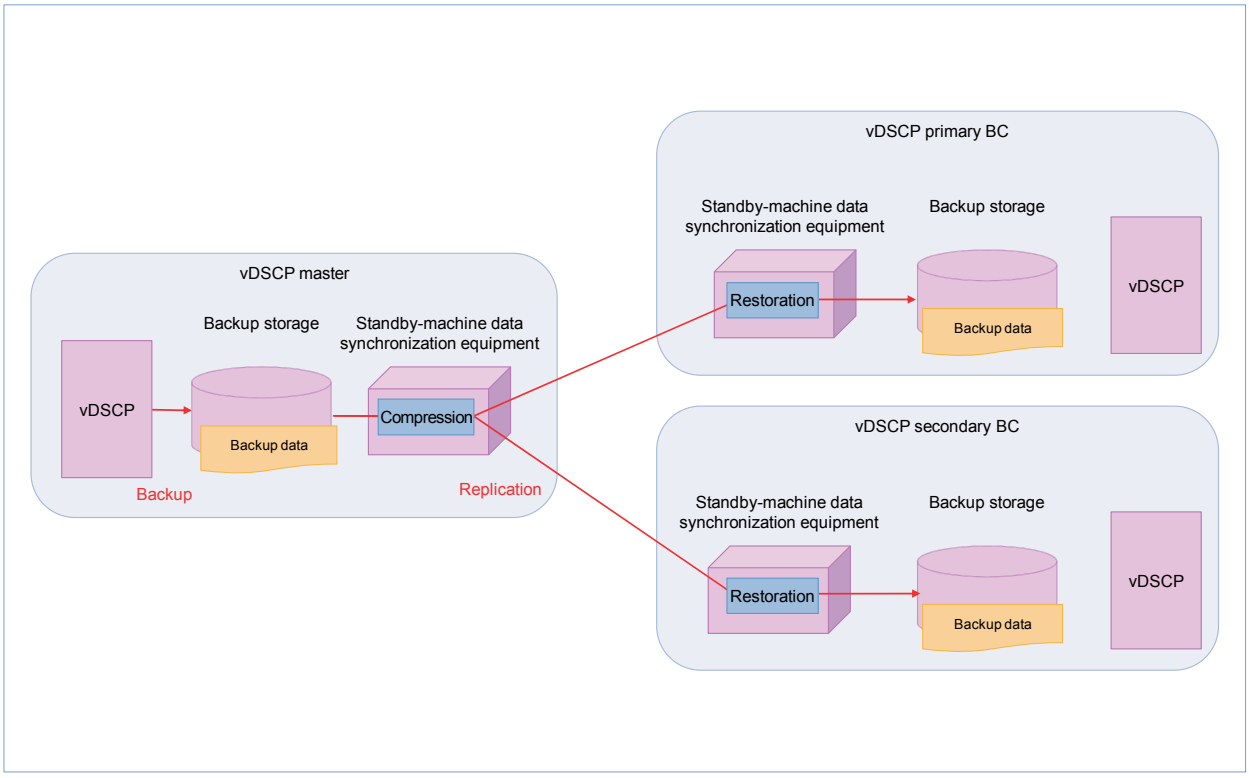


Figure 5 vDSCP master/BC configuration and backup file flow

a failure on users is a high-priority issue. From here on, as the use of IoT devices that demand reliability spreads throughout the social infrastructure and living environments, we can expect vDSCP to become all the more important to society, so we studied schemes for minimizing the effects of failures on users.

Conventional D-SCP is database equipment accommodating subscriber information. If we treat DBP with a database function on hardware as a single entity, the number of DBPs in a unit specifies the number of accommodated users per unit. Here, the FS function manages and controls multiple DBPs. The grouping of one FS and multiple DBs constitutes one D-SCP unit.

Now, in vDSCP, we migrated the FS function to DB-VM and adopted a scheme that handles SM-VM and DB-VM as independent VNFs (= units). As a result, user data corresponding to one DBP is handled as a single VNF enabling that VNF to be defined as one unit (**Figure 6**).

In D-SCP, a failure at the unit level given the configuration of a D-SCP unit described above necessitates BC switching on a unit basis.

In vDSCP, on the other hand, distributed deployment of VMs corresponding to DBPs on IA servers means that BC switching can be performed between individual VMs in the event of a failure on a VM unit. This enables the number of affected users at the time of a failure to be minimized (**Figure 7**). Additionally, since database capacity can be increased or decreased in a unit-by-unit manner, facility construction in response to an increase in demand can be handled in a flexible manner thereby reducing expenses.

6.2 Faster Restoration after Failure

1) Operation in D-SCP at Time of Failure

In D-SCP, the occurrence of a double failure in the active system (act) and standby system (sby)

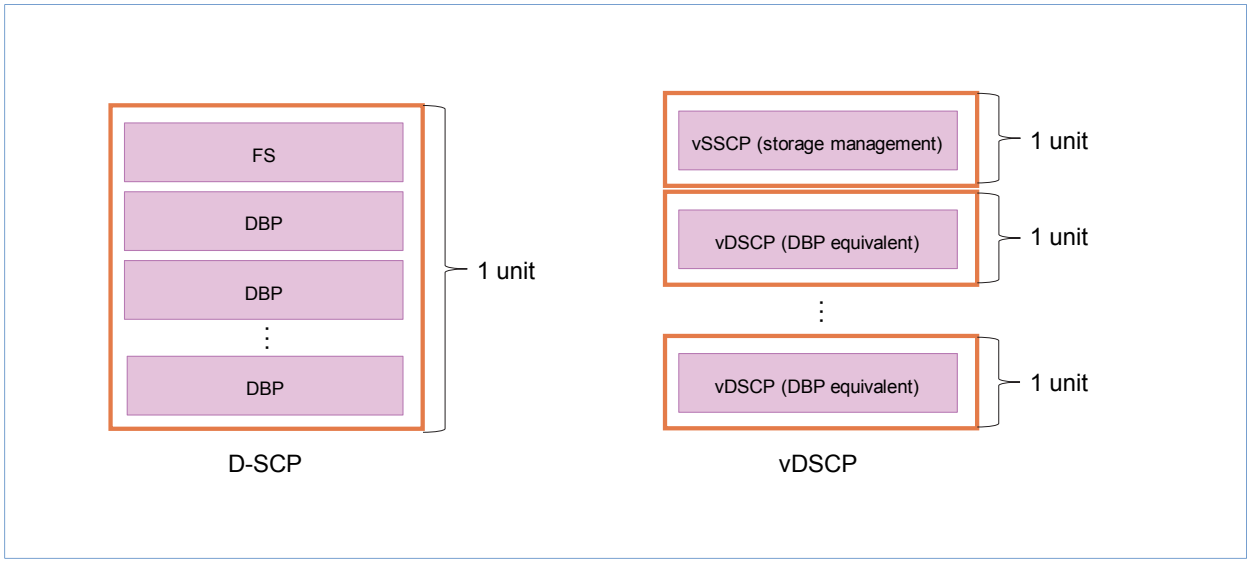


Figure 6 Comparison of unit configurations between D-SCP and vDSCP

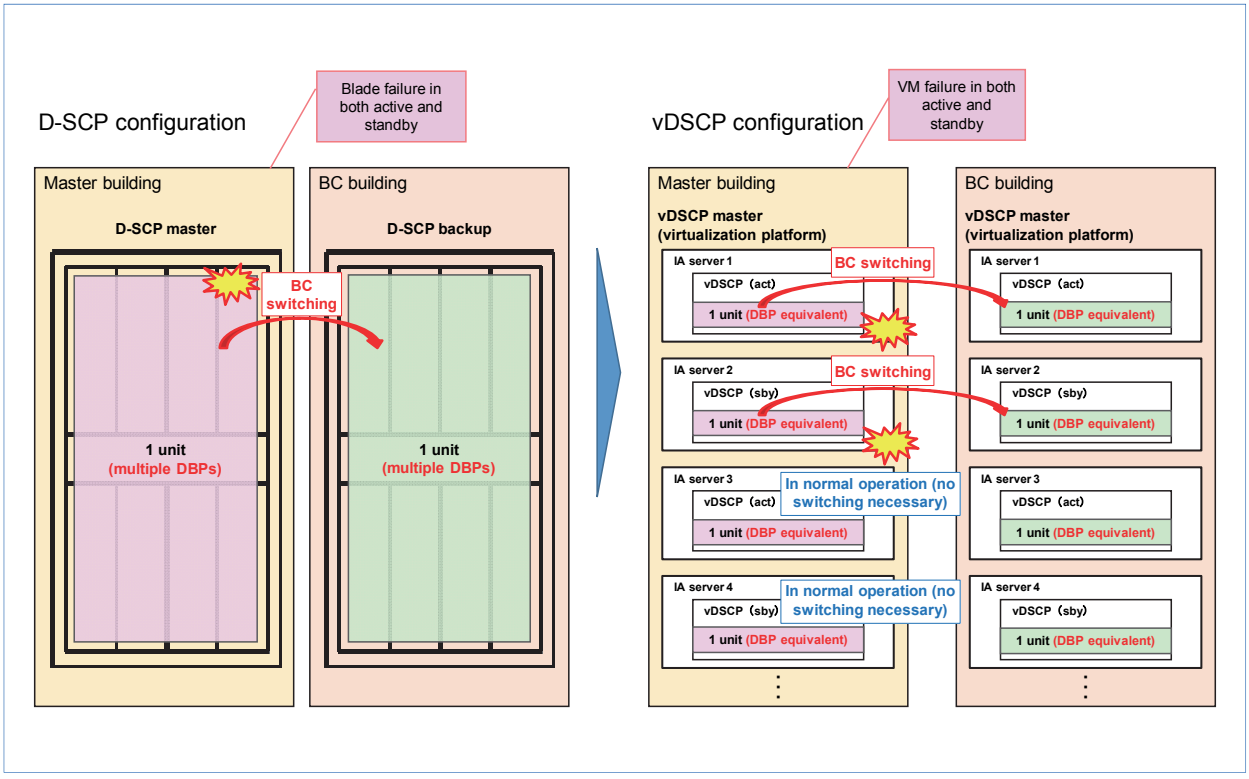


Figure 7 Overview of failure reaction at time of BC switching

of a processor accommodating a database (DBP) would be handled by a function called "relocation" that reallocates users to other DBPs within the same equipment. This function reallocates database information at the time of a failure with the aim of improving equipment reliability. Additionally, if a failure occurs in which service cannot be restored even with relocation, the D-SCP would be switched to a BC as described above and operated as an alternative unit to the equipment in which the failure occurred. This two-stage failure-reaction function in D-SCP minimizes the number of affected users.

During the relocation or BC-switching process, associated call processing that requires database access will be affected, so it is important from the viewpoint of improving reliability that the time required for such operations and the number of affected users be minimized.

A D-SCP adopts a system in which BC is made to stand by in a hot standby state (always running). As a result, the time required for BC switching is much shorter than the switching time incurred by relocation, but since BC switching here would be performed for an entire unit consisting of multiple DBPs, the number of affected users would be larger than that by relocation.

2) vDSCP Effect

In vDSCP, on the other hand, by reconfiguring the user-accommodation unit as described above,

BC switching can reduce the number of affected users the same as that at the time of D-SCP relocation in units of DBPs. We therefore evaluated vDSCP from the viewpoints of restoration time and the availability of alternative procedures and adopted a BC switching function that reduces the number of switched users per unit to that of a DB-VM (equivalent to a DBP) while making full use of the D-SCP feature of short BC switching time. In this way, the number of affected users can be greatly reduced compared with that of D-SCP while having a restoration time the same as that of D-SCP.

In addition, there is a function in the virtualization platform system that deals with a failure in a VM or hardware on the virtualization platform by performing VM restoration called "healing" on separate hardware kept in standby. Before virtualization, it was necessary to send maintenance personnel into the field to replace defective hardware, but this virtualized healing function enables restoration to be achieved in a relatively short time. Here, shortening the time from single-system operation to restoration of dual-system operation decreases the probability of a dual-system failure and improves system availability, all of which has the effect of improving reliability.

7. Conclusion

This article described the equipment configuration and functional allotment of vDSCP that applies virtualization to the database function section and the improvements achieved in reliability and economy through virtualization.

NTT DOCOMO is planning to migrate the service control equipment group in a stepwise manner as each type of equipment approaches its EoL period. Since D-SCP equipment that will reach EoL first has the important role of managing user information, we will take all possible measures to prevent a drop in quality by separating the development and introduction of vDSCP virtualized equipment and the development period for the subscriber-data migration function from D-SCP to vDSCP.

Going forward, we plan to study the application of network virtualization to other equipment in addition to the service control equipment group.

REFERENCES

[1] K. Otsuka et al.: "Enhanced Service Control Equipment Supporting Diverse NTT DOCOMO Services," NTT DOCOMO Technical Journal, Vol.14, No.4, pp.37–42.

[2] T. Kagi et al.: ""F-SCP" Service Control Equipment Providing Higher Reliability Services," NTT DOCOMO Technical Journal, Vol.17, No.1, pp.31–36.

[3] NTT DOCOMO Press Release: "DOCOMO Develops First NFV Technology for Multi-vendor EPC Software —Commercial service on DOCOMO's mobile network to start this March—," Feb. 2016. https://www.nttdocomo.co.jp/english/info/media_center/pr/2016/0219_00.html

2019 ITU Radiocommunication Assembly 2019 (RA-19), World Radiocommunication Conference (WRC-19) Report

Network Department Yuuki Itoh Nobuki Sakamoto
Radio Access Network Development Department Hiroyuki Atarashi

The Radiocommunication Assembly and the World Radiocommunication Conference of the International Telecommunication Union were held in Sharm El Sheikh, Egypt, from October 21 to 25, 2019, and from October 28 to November 11, respectively. This article mainly describes the matters related to International Mobile Telecommunications (IMT), discussed at these events. In particular, the article describes in detail the state of discussions on Agenda 1.13 at the World Radiocommunication Conference, which newly identifies frequencies for IMT in the 24.25 to 86 GHz frequency range with the usage of 5G in mind.

1. Introduction

The International Telecommunication Union (ITU) is a specialized agency of the United Nations. Its main mission is to set international standards and regulations on telecommunications and radio communications. As part of its activities, the organization holds the Radiocommunication Assemblies (RA) and the World Radiocommunication Conference (WRC), important meetings held every three to four years and attended by many persons involved in the telecommunications administrations of ITU member states (193 countries in total).

Held in Sharm El Sheikh, Egypt, from October to November 2019, the Radiocommunication Assembly (hereinafter "RA-19") was attended by approximately 500 people from the administrations, etc. of 88 countries, while the World Radiocommunication Conference (hereinafter "WRC-19") was attended by approximately 3,300 people from the administrations, etc. of 166 countries. Both RA and WRC were held for the first time in four years since 2015, and were held for the first time outside Geneva, the location of the ITU Headquarters, since

being held in Istanbul, Turkey, in 2000.

This article describes on the content of deliberations on International Mobile Telecommunications (IMT) at RA-19 and WRC-19, and their outcomes.

2. RA-19 Deliberations Content and Their Outcomes

The ITU Radiocommunication Sector (ITU-R) studies various types of technology and standardizes technical specifications related to international frequency usage, creates documentation about these, and functions to coordinate international frequency usage, etc. The RA is held as a general meeting concerning the overall activities of the ITU-R, approves documentation for ITU-R Resolutions, Questions and Recommendations, and appoints the chairpersons and vice chairpersons of Study Groups within the ITU-R.

2.1 Deliberations on ITU-R Resolutions, Questions and Recommendations

For resolutions that stipulate procedures, etc. for the various tasks of the ITU-R, 28 items were approved in RA-19 (2 new resolutions, 23 revisions of existing resolutions, and 3 suppressions of existing resolutions). Of these, revisions of Resolution ITU-R 1 stipulating the working method of the overall ITU-R and Resolution ITU-R 2 stipulating the working method of the Conference Preparatory Meeting (CPM)*1 were discussed vigorously during the session and were approved in light of the issues, etc. that had arisen in the past four years of ITU-R activities.

204 questions were submitted, and their assignments to Study Groups for the study cycle until 2023 were approved. Regarding IMT, a general term for international mobile telecommunication systems at the ITU, these include revision of a question [1] to continue studying for further advancement, and formulation of a new question [2] to study requirements that IMT must support with usage in specific industrial areas or enterprise applications in mind.

For recommendations, as items requiring approval in RA, discussions were held on recommendations referred to in the ITU Radio Regulations, and recommendations requiring further deliberations in RA considering the state of deliberations in Study Groups. As recommendations related to IMT, a proposed amendment to Recommendation ITU-R M.1036 was deliberated. This recommendation stipulates how to use frequencies identified for IMT in the ITU Radio Regulations. As a result, the deliberation reached a consensus and approved items that had not been concluded in Study Groups (such as the handling of IMT deployment with frequencies not identified for IMT) [3].

2.2 Appointment of Chairpersons and Vice Chairpersons to ITU-R Study Groups

For Study Group (SG) 3 (radiowave propagation), SG5 (terrestrial services), SG6 (broadcasting services), and SG7 (science services), currently serving chairpersons were re-appointed for a second term. For SG1 (spectrum management) and SG4 (satellite services), new chairpersons were appointed. Dr. Yukihiro Nishida (NHK) of Japan was re-appointed as the chairperson of SG6.

Study Group vice chairpersons were also appointed. Mr. Takahiro Kono (SKY Perfect JSAT) was newly appointed as vice chairperson of SG4,

*1 CPM: The Conference Preparatory Meeting. A meeting that develops reports which summarize ITU-R SG study results and other WRC-related discussions for preparation of WRC.

and Dr. Hiroyuki Atarashi (an author of this article) was re-appointed as vice chairperson of SG5.

3. WRC-19 Deliberations Content and Their Outcomes

To revise the ITU Radio Regulations, a wide range of items for deliberation (agendas) about various radio systems are set at WRC, and these agendas are deliberated based on the outcomes of studies at ITU-R over the last three to four years. At WRC-19, approximately 30 agendas were deliberated.

3.1 Agenda 1.13 (Agenda on Additional Identification of Frequency Bands for IMT)

1) Overview

Regarding frequencies used by mobile phones, harmonized international use enables procurement of devices for base stations and terminals and the enjoyment of benefits such as international roaming*2. The ITU defines the name IMT as a generic term for international mobile telecommunication systems. Also, the ITU identifies the frequency bands for IMT in the ITU Radio Regulations, and makes efforts to ensure that the use of IMT system frequencies is as common as possible in all countries of the world.

In addition, with the introduction of 5G being promoted in a range of countries around the world, one of the objectives of 5G usage is to realize high-speed communications exceeding 4G. This requires securing frequencies with wider bandwidth. For this reason, 12 candidate frequency bands from 24.25 to 86 GHz were selected at WRC-15 held in 2015. These frequencies are higher than those identified for IMT in the ITU Radio Regulations up to that point, and were deliberated as WRC-19 Agenda Item 1.13.

2) Results of Deliberations

As a result of deliberations at WRC-19, the frequency bands 24.25 to 27.5 GHz, 37 to 43.5 GHz, and 66 to 71 GHz were identified globally as frequencies for IMT for Region 1 (Europe, Russia, Africa, Arab countries), Region 2 (North and South American countries), and Region 3 (Asian and Pacific countries), as shown in **Figure 1** and **Table 1**. The 45.5 to 47 GHz and 47.2 to 48.2 GHz frequency bands were also identified as IMT frequencies for some regions or countries. For Japan, the 47.2

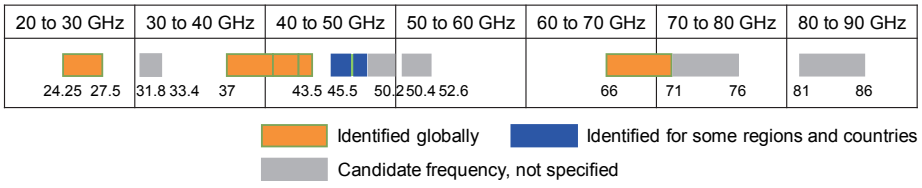


Figure 1 Candidate frequencies and frequencies identified for IMT in WRC-19 Agenda Item 1.13

*2 Roaming: A mechanism that enables users to use services similar to their subscribed carriers within the service areas of alliance partner telecommunication carriers, but outside the service areas of their subscribed telecommunication carriers.

Table 1 Details of frequencies identified for IMT at WRC-19

	Region 1 (Europe, Russia, Arabia, Africa) 122 countries	Region 2 (North and South America) 35 countries	Region 3 (Asia, Pacific) 36 countries
24.25 to 27.5 GHz	Identified globally		
37 to 43.5 GHz	Identified globally		
45.5 to 47 GHz	Identified for 50 countries (Europe (some countries), Russia, Arabia, Africa)	Identified for 1 country (Brazil)	Identified for 2 countries (Iran, Korea)
47.2 to 48.2 GHz	Identified for 62 countries (Europe (some countries), Russia, Arabia, Africa)	Identified for all regions	Identified for 7 countries (Australia, Korea, India, Iran, Japan, Malaysia, Singapore)
66 to 71 GHz	Identified globally		

to 48.2 GHz frequency band was identified for IMT. Adding these frequency bands together, a total of 17.25 GHz of bandwidth was identified for IMT at WRC-19, a significant increase on the total bandwidth of approximately 1.9 GHz of frequencies previously identified by the ITU Radio Regulations.

3) Issues Deliberated

Conditions for frequency sharing with existing radio systems were a major issue in identifying frequencies for IMT. In deliberations on 24.25 to 27.5 GHz and 37 to 43.5 GHz, conditions to prevent radio interference from IMT to nearby Earth exploration satellite services (passive) operating at frequencies 23.6 to 24 GHz and 36 to 37 GHz were discussed. As specific conditions, it was shown that the intensity of unwanted emissions[*3] of IMT radio stations (base stations and terminals) at the reception frequency of Earth exploration satellite were limited, but resulted in a major debate because there were significant differences between the required limits on the intensity of unwanted emissions between the regions and countries making proposals due to differences in prerequisites for technical studies, etc. In addition, conditions for preventing radio interference to inter-satellite services and fixed satellite services operating within 24.25 to 27.5 GHz and 42.5 to 43.5 GHz were also discussed. Specifically, proposals such as provisions for IMT base station output power restrictions, transmission directionality and mechanical tilting[*4] for outdoor IMT base station were discussed.

About the issues regarding frequency sharing conditions with the Earth exploration satellite services (passive), inter-satellite services, and fixed-satellite services, it was assumed that agreement would be difficult through deliberations at the meeting. Therefore, in the latter half of the WRC-19 meeting, considerations were continued on agreeable compromises through the holding of many small, informal meetings with small numbers of people mainly representative of various regions and representatives of countries making specific proposals. Finally, these compromises were submitted to the WRC-19 plenary session and agreement was reached.

*3 Unwanted emissions: Unneeded radio emissions outside the desired band that can cause interference on neighboring frequencies.

*4 Tilting: Inclination of an antenna's main beam direction in the vertical plane. There are mechanical tilt systems that physically tilt the antenna and electrical tilt systems that control the amplitude and phase of antenna array elements to tilt the main beam.

3.2 Other IMT-related Agendas

As 1,427 to 1,518 MHz were identified as frequencies for IMT at WRC-15, considerations were addressed in Agenda 9.1, Issue 9.1.2 regarding compatibility between the 1,452 to 1,492 MHz broadcasting satellite services (voice) and IMT for Regions 1 and 3. Mobile communication systems have been operating in this frequency band in Japan since before WRC-15, and Japan has taken actions to prevent restrictions on future domestic operations. This issue also entailed a difficult debate until the final week of WRC-19, but ultimately a solution that struck a balance between broadcast satellite services (voice) and IMT regulations was reached.

Regarding frequencies from 27.5 to 29.5 GHz, studies on the technical and operational characteristics of Earth Stations In Motion (ESIM)*5 operated as fixed satellite services and their frequency sharing with other radio systems were handled as Agenda 1.5. Some of these frequencies are already allocated for 5G in Japan. The discussions focused on how to prevent the effects of radio interference on existing systems deployed on the ground when ESIMs onboard aircraft (hereinafter "aeronautical ESIMs") transmit to satellites. There was a major debate between Europe, etc. who are considering the deployment of ESIMs in the 27.5 to 29.5 GHz frequency range and Japan, Korea and the United States who are considering these frequencies for the use of 5G. Ultimately, restrictions on the Power Flux Density (PFD)*6 on the ground surface of aeronautical ESIMs were stipulated for operations. Also, it was agreed that the ITU-R Radiocommunication Bureau would strictly inspect aeronautical ESIMs and liability provisions for PFD compliance with restrictions outside borders, to be specified in a WRC resolution.

3.3 Agendas to be Deliberated at WRC-23

At each WRC, agendas for deliberation at the future WRC are decided. Therefore, agendas for WRC-23 to be held in four years were deliberated and agreed upon at WRC-19. **Figure 2** shows the frequency bands of agendas related to IMT.

Continuing from WRC-19 Agenda 1.13, a number of countries and regions made proposals to establish new agendas to study further identification of frequencies for IMT. In the proposed 3.3 to 24 GHz frequency range, as a result of coordination among members representing various regions, agreement was reached to study the frequency bands shown in Fig. 2 as WRC-23 Agenda 1.2.

Also, regarding the 4,800 to 4,990 MHz frequency band identified for some countries as frequencies for IMT in WRC-15, discussions were held to review the handling of PFD limit values for IMT radio stations to protect radio stations for aeronautical mobile services but did not reach a conclusion, although agreement was reached to continue deliberations as WRC-23 Agenda 1.1.

In addition, agreement was reached for Japan's proposal to establish a new agenda to study the use of IMT base stations installed on High Altitude Platform Stations (HAPS)*7 with 2.7 GHz and below specified for IMT after narrowing down target frequencies and regions, as WRC-23 Agenda 1.4.

Furthermore, agreements were reached to study primary allocation*8 for mobile services in the 3,600 to 3,800 MHz band in Region 1 (Agenda 1.3), and frequency usage of existing services and future handling in the 470 to 694 MHz band in Region 1 (Agenda 1.5). These agendas may also become

*5 ESIM: A name for earth stations in motion that communicate with satellite stations operating under the fixed-satellite service.

*6 PFD: The power intensity of a radio wave passing through a unit area.

*7 HAPS: A general term for a system that provides communication services from the sky by mounting communication equipment on an unmanned vehicle such as an aircraft that stays in a fixed location in the stratosphere at an altitude of approximately 20 km.

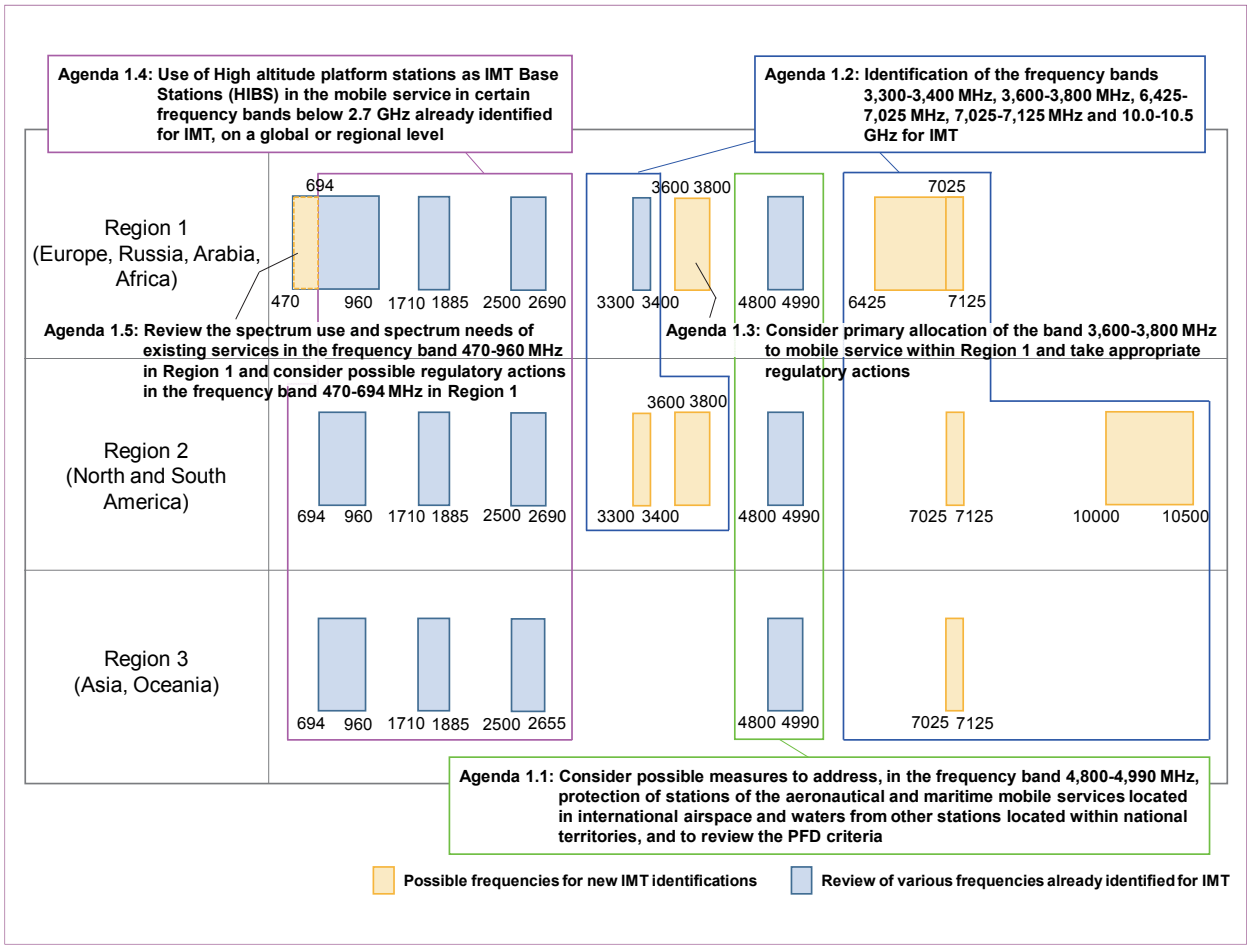


Figure 2 Frequency bands of IMT-related agendas at WRC-23

relevant to discussion on identification of frequencies for IMT, depending on future discussions.

4. Conclusion

This article has described an overview of the outcomes of deliberations at RA-19 and WRC-19. In deliberations on Agenda 1.13 at WRC-19, agreement was reached to identify very wide bandwidth of frequencies for IMT. This is a considerably significant result for further IMT development going forward compared to the results of past WRCs. In contrast, as there are large conceptual differences for the conditions for frequency sharing with existing radio systems in each region and country, much time and effort were also spent on consensus building in deliberations at WRC-19.

Additional identification of frequencies for IMT will also be studied at WRC-23, and it's likely that frequency sharing conditions for existing systems operating on any frequency band will be discussed intensely. At the end of the WRC-19 conference period, informal meetings were held by representatives, etc. from each region and compromises were

*8 Primary allocation: Allocation of frequencies to a primary service in the ITU Radio Regulations. Services to which frequencies are allocated are classified as primary or secondary services. Primary services are services that can be protected from harmful interference from other primary services or secondary services. Conversely, secondary services cannot cause harmful interference to the operation of primary services, nor claim protection from primary service interference.

found, so it's possible that similar methods of coordination will be adopted for difficult cases at WRC-23. To respond appropriately to such discussions, it will be necessary to unify the views of all regions in advance and for representatives of each region to be recognized. Thus, presence at ITU-R Study Group meetings and preparatory meetings in each region will be even more important. NTT DOCOMO will continue to proactively participate in these meetings.

REFERENCES

[1] Question ITU-R 229-5/5: "Further development of the terrestrial component of IMT," Nov. 2019.
[2] Question ITU-R 262/5: "Usage of the terrestrial component of IMT systems for specific applications," Nov. 2019.
[3] Recommendation ITU-R M.1036-6: "Frequency arrangements for implementation of the terrestrial component of International Mobile Telecommunications (IMT) in the bands identified for IMT in the Radio Regulations," Oct. 2019.

Event Reports

5G Open House Exhibition Report

DOCOMO Open House 2020 —Dawn of the 5G Era and the Future Beyond—

R&D Strategy Department Masahiro Tamaoki

For two days, January 23 and 24, 2020, "DOCOMO Open House 2020 —Dawn of the 5G Era and the Future Beyond" wad held at Tokyo Big Sight. This article introduces the scene at this event, and describes its main exhibits in detail.

1. Introduction

For two days, January 23 and 24, 2020, NTT DOCOMO held "DOCOMO Open House 2020 —Dawn of the 5G Era and the Future Beyond" at Tokyo Big Sight (**Photo 1**).

NTT DOCOMO looks beyond 2020 and works together with its business partners (hereafter referred to as "partners") to exceed customer expectations and provide customers with surprise and excitement, and aims for co-creation of new value with its partners. This event had been positioned as a place to convey advanced technologies and capabilities to the world based on examples of collaborative innovation with partners in various fields, but this time, NTT DOCOMO has gone further and made efforts to give visitors a taste of the future it draws from the user's perspective. At the venue, we and our partners who are promoting collaborative creation introduced the latest technologies for 5G, AI and IoT, etc. and business solutions using these (**Photo 2**). The exhibition also featured various lectures and programs, and we introduced the "DOCOMO 202X CONCEPT" that embodies the lifestyles of future imagined by NTT DOCOMO. This successful event attracted attention because it was the first year of provision of 5G commercial services. The number of visitors was approximately 24,000, an increase of approximately 10,000 compared to last year.

This article describes details of the main exhibits at the event.

Photo 1 The scene at DOCOMO Open House

Photo 2 Business creation

2. Event Overview

The event featured 286 exhibits classified into the 10 categories of AI, Device / UI / UX, Digital Marketing, IoT, Business Creation, Global, 5G Vision, 5G Lifestyle, 5G Business, and 5G Future & Technology (**Photo 3**). At the exhibits, visitors were informed of NTT DOCOMO's vision of the future through hands-on experiences of operating actual machines and demonstrations.

In lectures, President and CEO Kazuhiro Yoshizawa gave the keynote lecture on the first day introducing NTT DOCOMO's targeted future and medium-term strategies for the 5G era, entitled "5G, The coming of a richer future" (**Photo 4**). On the second day, Hiroshi Nakamura, Executive Vice President, gave a lecture entitled "Opening the 5G Era and Realizing a Sustainable Society", in which he talked about a society realized by the convergence of the real world with cyberspace in the future where 5G, communication technology of the following generation, and AI are widely used (**Photo 5**).

Photo 3 5G Vision

Photo 4 The keynote lecture by President and CEO Kazuhiro Yoshizawa

Photo 5 Special lecture by Executive Vice President Hiroshi Nakamura

As well as NTT DOCOMO, lectures on various themes were also given by Naomi Tomita (hapi-robo st, Inc., Huis Ten Bosch Co., Ltd.), Rony Abovits (Magic Leap, Inc.), Daisuke Ohata (former Rugby Japan team member, Kobe Steel Rugby Team Kobelco Steelers Ambassador), etc.

3. DOCOMO 202X CONCEPT

This pavilion focused on some of the exhibits at the venue and expressed the lifestyles of future imaged by NTT DOCOMO in six scenes as HOME, MOBILITY, CAFE, LIBRARY, HALL and ARENA. As hands-on experience exhibits with technical explanations kept to a minimum, these exhibits introduced user experiences of the future that can be obtained by combining these various scenes.

For example, HOME exhibited a scene in which AI grasps the body condition of a resident when he or she wakes up in the morning, and switches the indoor environment to more comfortably suit the mood or state of the resident. Combinations of the following exhibits enable the scenes.

(1) A monitoring solution for the elderly: In consideration of privacy, this solution enables acquisition of the residence health status, position and posture without the use of a video camera.

(2) Smart home, future house project: AI-based solutions for providing users with recommendations and controlling IoT devices by various IoT sensors collecting the resident's data.

Another scene demonstrated smartphone charging that starts automatically using "long-distance wireless charging*1" technology when entering a café, and "Osaifu-Keitai touchless" technology that links Ultra Wide Band (UWB)*2 with various radio

*1 Wireless charging: Transmission of power without an electrical connection. Power transmission can be accomplished by an electromagnetic scheme, by optical means, or by sound waves, etc.

*2 UWB: A wireless communications system with a signal bandwidth that exceeds 500 MHz.

standards so that the smartphone can complete the payment from the user's pocket just by the user standing in front of the cash register.

The daily life scenes shown in this pavilion are not merely pipedreams but represent a future that can be realized based on the technologies of NTT DOCOMO and its partners (**Photo 6**, **7**).

4. VMocap - 3D Digitalization of Human Movement Using Cameras

At this booth with a circular stage, a marker-less motion capture technology that works in wide-space and multi-person environments was demonstrated and attracted the attention of many visitors (**Photo 8**, **9**, **Figure 1**).

This technology was developed jointly with the Nakamura and Yamamoto laboratory of the Graduate School of Information Science and Technology, the University of Tokyo. The demonstration was realized by applying the "VMocap" technology developed by the laboratory, which enables motion capture only from camera images.

Generally, special equipment or suits are required to perform motion capture, which limits measurement locations and usage scenes. However,

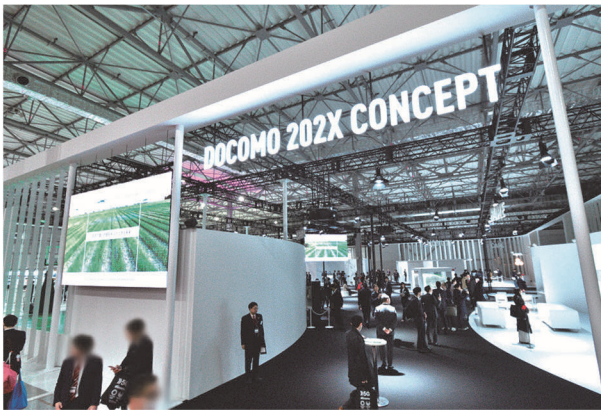


Photo 6 The DOCOMO 202X CONCEPT entrance

Photo 7 DOCOMO 202X CONCEPT sports viewing

Photo 8 The scene at the demonstration

Photo 9 The scene at the venue

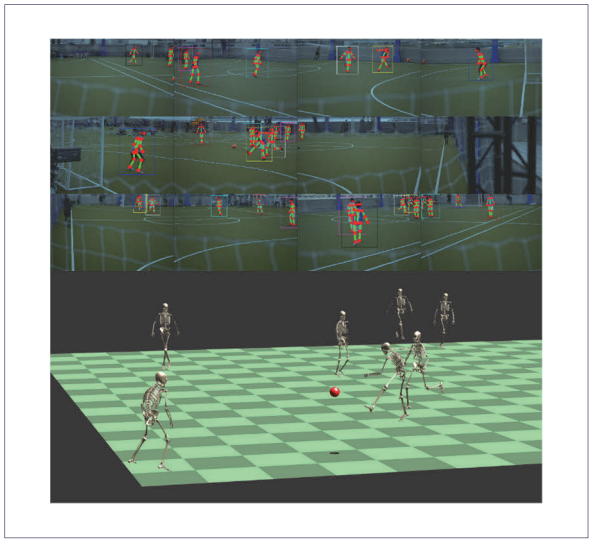


Figure 1 Sample output of the video motion capture

this technology realizes multi-person marker-less motion capture in a wide space by automatically selecting and switching optimum images for analysis from multiple cameras. In addition, even in the situation where human bodies overlap on the image, the technology predicts the human movement robustly by utilizing the human skeletal model, continuity of the motion and the latest image recognition technology. Even in a scene where multiple players move around dynamically such as a game of futsal, the technology can obtain high-accuracy and smooth motion and bone movement (**Figure 2**).

In the future, this technology will be applied to sports such as soccer, baseball, gymnastics, figure skating, etc., and utilized for training, tactical analysis, prevention of injury and motion archiving. In addition, it will also be used to create 3D animations in the entertainment field and evaluate exercises in the nursing and rehabilitation fields.

5. Future Lifestyles Achieved with AR Clouds

Regarding Augmented Reality (AR)*3/Mixed Reality (MR)*4, which will bring innovative communications, we used "AR cloud" technology to present a demonstration exhibition that conjured the lifestyles of the future.

The AR cloud is technology that provides a common AR/MR experience across different devices such as AR glasses, Virtual Reality (VR)*5 goggles and tablets, etc. by using self-localization technology that collects data about the spatial structure in the exhibition booth in advance, builds a digital twin*6 that is a copy of the real space, and aligns the real space with the digital twin using a feature

*3 AR: Technology for superimposing digital information on real-world video in such a way that it appears to the user to be an actual part of that scene.

*4 MR: Technology for superimposing digital information on video taken of the real world and presenting the result to the user. In contrast to AR, MR makes information appear as if it's actually there in the real world from any viewpoint.

*5 VR: Technology that gives the user the illusion of being in a virtual world. In recent years, this illusion is mainly achieved using HMD

point map*7.

The exhibition featured two simulated areas: an outdoor cityscape inspired by an old town, and an indoor living room (**Figure 3**). Visitors experienced a wide range of content fusing the cyber and the physical on three devices, Magic Leap 1*8, Mirage Solo and iPad*9, such as being provided with coupons for nearby (simulated) stores, etc. according to their location, multiple paper cranes flying out from noren curtains, bus arrival times estimated with consideration of traffic congestion displayed on a bus stop, text messages displayed above the heads

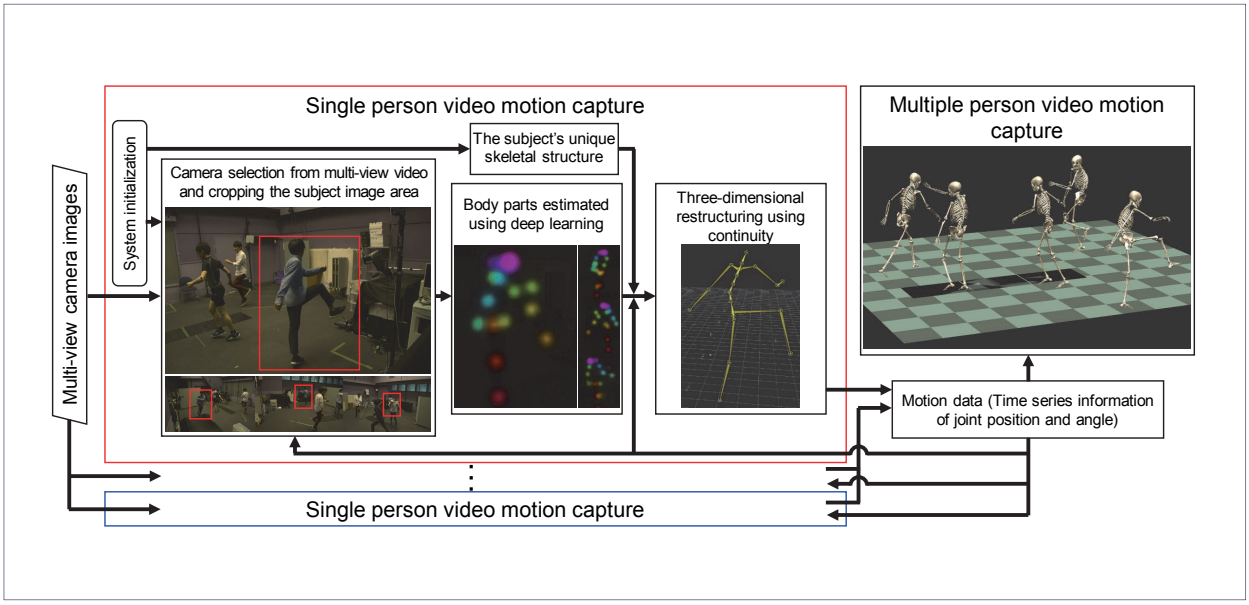


Figure 2 Flowchart of VMocap

Figure 3 Overview of the exhibition booth

*6 Digital twin: A real-time reproduction in the digital world of the position, shape, and various sensor information of various objects in the real world.

*7 Feature point map: A collection of image feature points from which camera images have been extracted, which are required to align (self-position recognition) real space with digital twins.

*8 Magic Leap 1: "MAGIC LEAP", MAGIC LEAP 1, the Magic Leap logo and all other trademarks are trademarks of Magic Leap, Inc.

of people by tracking their movements, virtual pets, and living rooms turning into beautiful sandy beaches in an instant (**Photo 10**, **Figure 4**).

Many visitors wanted to experience Magic Leap 1, and we heard much positive feedback about the world of the AR cloud experienced with these cutting-edge spatial computing devices.

6. Flexible 5G Area Formation with Transparent Dynamic Metasurface

To flexibly develop areas with the millimeter wave band used for 5G and later generations, a prototype of a "Transparent Dynamic Metasurface"*10 developed by NTT DOCOMO and AGC Inc. (hereinafter referred to as "AGC") was exhibited, and demonstration experiments were introduced by video. Last year, NTT DOCOMO exhibited a metamaterial*11 reflector that allows the direction and beam shape of reflected waves to be designed at the same event, but there were some issues. While the metamaterial reflector is effective for expanding an area, it needs to be designed to suit the installation location, the back of the reflector is out of line of sight which degrades communication quality, and the device can also affect the scenery. To address these issues, NTT DOCOMO proposed a new principal and designed a device, while AGC studied the material and microfabrication technologies and manufactured it. We presented this new transparent dynamic metasurface at the exhibition.

This transparent dynamic metasurface achieves a large substrate surface area and dynamic control of the transparency/reflection ratio while maintaining transparency, by tiny micron-level (μm) movement of the glass plate layered on the transparent metasurface to widely vary the metasurface transparency/reflectivity characteristics (**Photo 11**).

At the venue, we also exhibited a video of a

Photo 10 Customers enjoying the demonstration

Figure 4 Contents actually displayed on an iPad

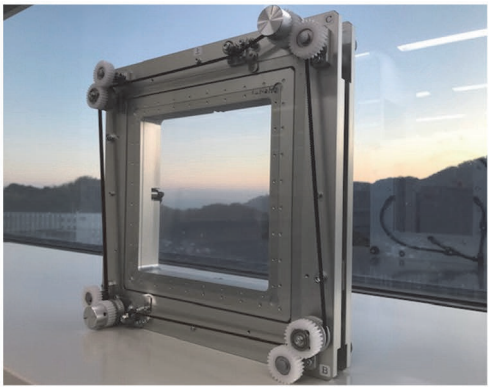


Photo 11 The transparent dynamic metasurface exhibited

*9 iPad: Apple, the Apple logo and iPad are trademarks of Apple Inc. registered in the United States and other countries. TM and ©2020 Apple Inc. All rights reserved.

*10 Metasurface: An artificial surface technology with two-dimensional periodic arrangement of structures that is a type of artificial medium (metamaterial) that achieves an arbitrary dielectric constant and magnetic permeability by periodically arranging structures that are smaller than the wavelength.

*11 Metamaterial: An artificial material that causes electromagnetic waves to behave in ways that they do not in natural materials.

January 2020 demonstration of nearly loss-free transmission/reflection control of radio waves with a bandwidth of 400 MHz or more in the 28 GHz band, and showed that it's possible to flexibly construct 5G areas with the transparent dynamic metasurface more meticulously by dynamically controlling wave propagation without adversely affecting scenery (**Figure 5**, **Photo 12**).

7. Conclusion

This article introduced the scene at "DOCOMO

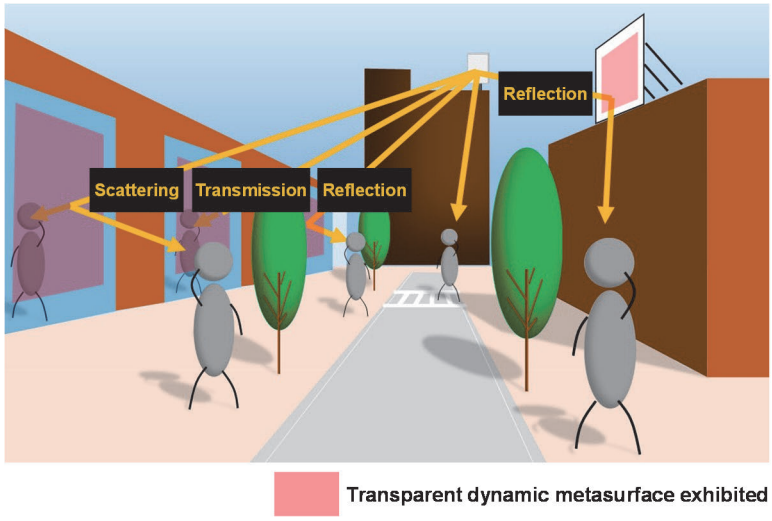


Figure 5 Future use case image

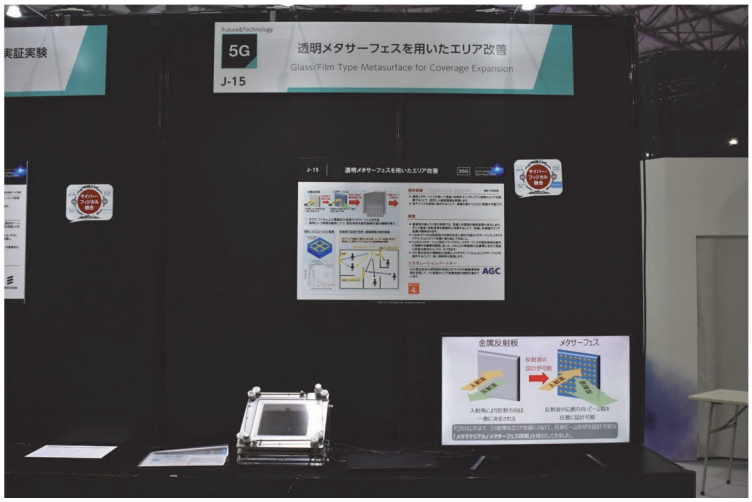


Photo 12 An exhibit

Open House 2020 —Dawn of the 5G Era and the Future Beyond—" held on January 23 and 24, 2020, and described some of its exhibits.

NTT DOCOMO has launched full-scale 5G commercial services and is creating fun and surprising services to innovate customer lifestyles and communications of the future while aiming for the growth of Japan and the prosperity of society, and is making efforts to solve social issues.

NTT DOCOMO
Technical Journal Vol.22 No.1

Editorship and Publication
NTT DOCOMO Technical Journal is a quarterly journal edited by NTT DOCOMO, INC. and published by The Telecommunications Association.

Editorial Correspondence
NTT DOCOMO Technical Journal Editorial Office
R&D Strategy Department
NTT DOCOMO, INC.
Sanno Park Tower
2-11-1, Nagata-cho, Chiyoda-ku, Tokyo 100-6150, Japan
e-mail: dtj@nttdocomo.com