# Biometrics Achieves Compatibility of Security and Convenience in Mobile Services

NAKATSUKA Yutaka, IKEYA Ryohei, TEZUKA Yukiko, AMANO Shinichi, AOYAGI Toru, IWASA Ayaka


## Abstract

Illegal access to online services using personal authentication IDs and passwords still remains a security threat. This paper introduces the approach of FIDO in using biometrics to provide mobile terminals with secure online authentication that will not be "forgotten, lost or stolen." This strategy, which includes facial recognition, a technology in which the NEC excels, is implemented without transmitting or storing "information required for authentication, such as biometric information," either to or in the server. An advancement of the financial services by using FIDO and API-GW is also achieved.


Keywords

FIDO, NC7000-3A, authentication, approval, ID linkage, biometric authentication, face recognition

## 1. Introduction

The ID and password have traditionally been the most popular mechanisms used in user authentication for online services on the Internet. However, it has been pointed out that these mechanisms have problems in security including those related to illegal access. Particularly with regard to the financial institutions that are prone to the recurring damage incurred by illegal transfers. Aiming at reducing dependency on the password authentication that accompanies such troubles, FIDO (Fast IDentity Online) is attracting attention as a new means of online authentication that makes use of the biometric technology.

Since the foundation of the FIDO Alliance in 2012, the technological specifications of FIDO have been expanded with the aim of standardizing the password-less authentication for online services. It is based on the stance of establishing an authentication standard offering both firm security and ease of use. De facto standards are being developed by the participation of major players in the related fields, such as financial ventures, communication carriers and security vendors[1].

Some financial institutions from outside Japan have already implemented FIDO-based Internet banking services[2]. Japanese financial institutions are also expected to advance utilization of FIDO by considering the safety and convenience of biometric authentication in various consumer-oriented services such as in Internet banking.

This paper introduces the advancement of financial services by utilization of the FIDO biometric authentication technology.

## 2. Background to the Use of Biometric Authentication

It has been reported that about 80% of personal authentications in online services employ IDs and passwords[3]. The number of recognitions of illegal accesses, including impersonations, was 2,051 in FY2016. Once such illegal accesses were successful, 74.6% of the subsequent actions taken were "illegal money transfers in Internet banking." (Source: Status of illegal access actions (National Police Agency, Ministry of International Affairs and Communications, and Ministry of Economy, Trade and Industry)).

According to the Report on the Survey of Online Per-


Fig 1 Merits of biometric authentication.

sonal Authentication Systems issue by IPA, about 70% of users have a basic knowledge on what a safe password is, but only 13% of them actually set safe passwords. With regard to businesses, less than 10% of them offer authentication methods other than IDs and passwords. This deficiency is combined with concerns that authentication using a device presupposes the possession of a dedicated device and that the tightening of the password policy risks reducing the service usage rate.

As a means of solving the security risks lurking in traditional authentications based on knowledge (password, etc.) or possessed item (IC card, key, etc.), attention is being focused on the biometric authentication technology as shown in **Fig. 1**.

## 3. NEC's Approach to Biometric Authentication

At NEC, we have been engaged in R&D and business deployment of biometric authentication for more than four decades (**Fig. 2**). Today we can boast of fingerprint identification and face recognition technologies at the world's top level [4) 5)].

Moreover, the devices providing the service have changed significantly from PCs exclusively to include mobile terminals (smartphones or tablets). It has now become a standard procedure to perform authentication in applications on mobile terminals. As these terminals are now provided with a camera and/or fingerprint sensor as standard, it is quite easy for them to utilize biometric authentications such as the face and voiceprint recognition, and fingerprint identification.

Perceiving the necessity of deploying biometric authentication technology on the server side to mobile terminals based on the technical background described above, we are now able to provide a face recognition

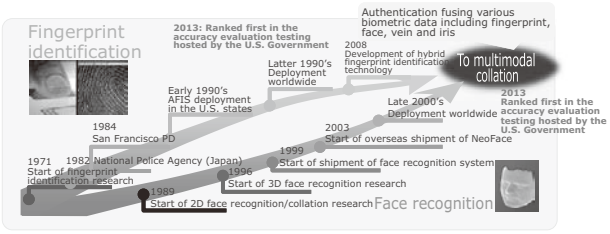


Fig. 2 NEC's approach toward biometric authentication.

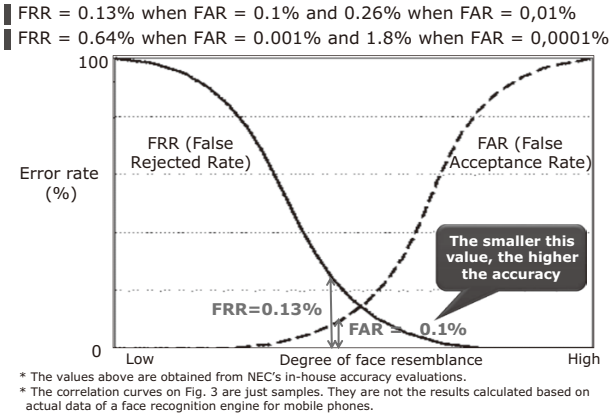


Fig. 3 Estimated accuracy of face recognition for mobile authentication.

engine at the level of the world's highest proven accuracy and performance[5)]. This has thereby been improved even further for use in mobile authentications (**Fig. 3**).

## 4. NEC's Approach to the Authentication of Mobile Customers

At NEC, we employ the NC7000-3A series integrated

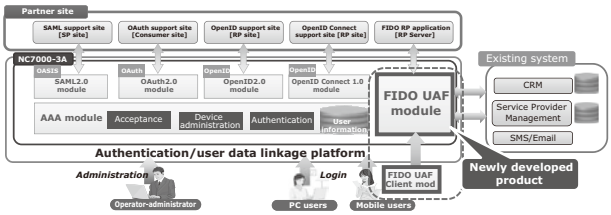


Fig. 4 Overall image of NC7000-3A

authentication platform to provide various authentication services such as the SAML2.0/OAuth2.0/OpenID Connect/OTP (One-Time Password) services for the customers of major carriers.

The NC7000-3A authentication platform has recently been enhanced by the addition of the FIDO biometric authentication in the line-up of its services (**Fig. 4**).

### 4.1 NC7000-3A – An Approach to authentication technology offering both security and convenience –

Traditional mobile terminal services have been enjoyed without imposing burdens on the limited user interface (UI) environment of mobile terminals. This is due to the network access authentication that is provided by the communications carriers as the mechanism for recognizing users without IDs or passwords.

The dissemination of smart phones has increased mobile accesses that do not pass through the networks provided by communications carriers. As the network access authentication of users cannot be applied to this environment the users are required to perform user authentications involving troublesome operations. These include the input of ID or passwords, in order to access the safe use of services.

In order to deal with this situation, NEC introduced an authentication security solution in 2012 that offers both security and convenience by making use of the high-security certificate technology. We have also been promoting advances in this field, by for example providing late in 2016, a unique device authentication function.

### 4.2 Outline of FIDO

Roughly speaking, FIDO includes two kinds of standards; 1) UAF and 2) U2F.

(1) UAF stands for "Universal Authentication Framework" and defines the standard for authentication using a FIDO-compatible device, without using a password.

(2) U2F stands for "Universal Second Factor" and defines the standard for two-factor authentication.

In the following section, we describe our approach toward 1) UAF, which is a biometric authentication.

One of the most significant features of FIDO is that any information tied to an individual, such as biometric information, is not transmitted outside of the terminals. As the biometric information such as face features does not flow on the network, nor is it stored in and/or leaked from the servers of the service providers, the system safety is enhanced considerably.

FIDO makes the above possible by means of the two phases of 1) personal authentication is performed inside each terminal; and 2) only "the result of personal authentication" on the PKI base is transmitted to the server side.

Specifically, after the authentication tool called the "Authenticator" inside the user device performs the personal authentication based on the biometric information, etc., the authenticator attaches the signature to the personal authentication result. This is done by using a secret key and the result is then transmitted to the server side. The server then verifies the signature using a pre-registered public key in order to complete the authentication. A pair of secret and public keys are generated and registered at the time of user registration.

### 4.3 A Usage Example

The login procedure using FIDO is extremely simple for the user. A typical example of the authentication procedure is to press the login button and place a finger on the fingerprint sensor on the smartphone or by showing the user's face towards the camera (**Fig. 5**).

### 4.4 NC7000-3D-FS (FIDO Service)

The 3A-FS is an authentication software product compliant to FIDO UAF 1.0. It features user high convenience and safety thanks to its biometric authentication.

The 3A-FS has a configuration shown in **Fig. 6** and

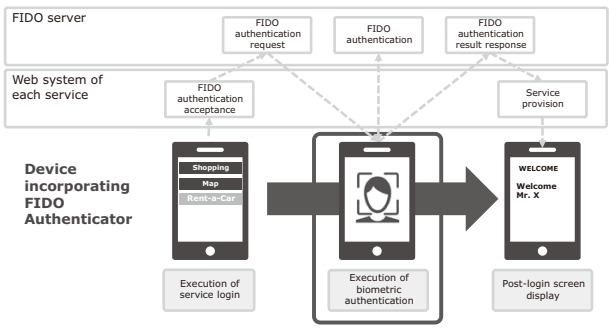


Fig. 5 Example of login using FIDO

provides; 1) FIDO Server, and; 2) FIDO Client/ASM/Authenticator (fingerprint and face recognitions).

The product may be used by server or client alone, and is certified to comply with the FIDO specifications as one of the certified products* of the FIDO Alliance[6].

It is the first Japanese product to have acquired the certifications for both the server and client (NEC survey as of December 2016) and it can provide a one-stop service of FIDO biometric authentication.

In order to implement "multimodal authentication" we are planning to incorporate other technologies such as vein and voice print recognition in this product. These are biometric authentication technologies that identify users by using multiple pieces of biometric information. The product is attracting the attention of financial institutions worldwide as a promising means of personal authentication and it is positioned as one of the solutions expected to offer greater usage flexibility. It is being studied as a next-generation authentication method that offers higher reliability and usability than the ID and password method.

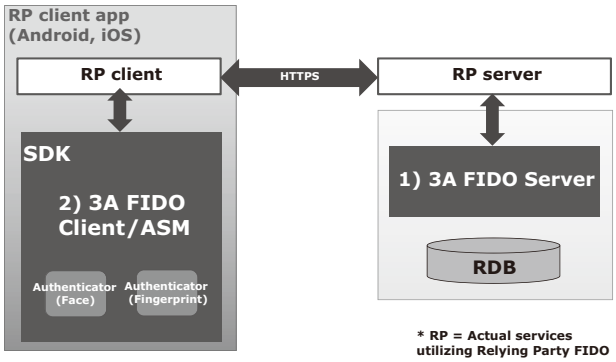


Fig. 6 Configuration of NC7000-3A-FS.

### 4.5 Security Proper to NEC

What is noticeable in recent mobile application developments is that the attacks on terminals are increasing compared to those of servers. With a mechanism that utilizes the terminals to store authentication information and perform encrypted computations, the security inside the terminals is important. The FIDO Authenticator of the 3A-FS incorporates a unique security module based on the information on the terminal side, and this security module is protected by a strong obfuscation function. This design prevents abuse and hacking by malware or external malicious applications.

At NEC, we have long been conducting research into the encryption methods at the security department of our Central Research Laboratories. We are therefore planning to adopt NEC's latest, unique encryption technology as required in order to implement strong authentication of information leak prevention by means of rapid and secret computations.

## 5. Approach to Open API

The Japanese Bankers Association has established the "Study Group on Open API" and opened the bank system connection specifications to FinTech enterprises, etc. (open API). This strategy enables the financial ser-

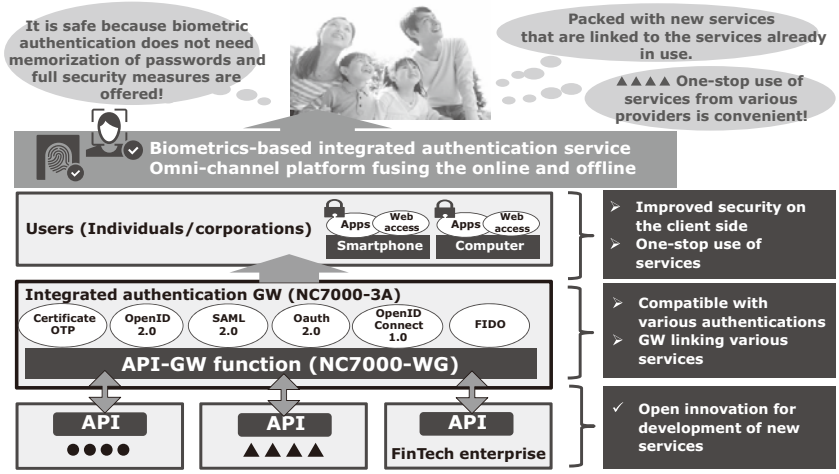


Fig. 7 Platform of the Connected Economy/Open API era

* The Server, Client and Authenticator (fingerprint identification for iOS) have completed certifications as of February 2017. The certifications of other Authenticators (fingerprint identification for Android and face recognition for iOS/Android) are planned for the future.

vices performance to advance based on the linkage of financial institutions and FinTech enterprises, etc.

In order to allow a financial institution to open its services as API and to safely and conveniently connect the users, banks and FinTech enterprises, etc., a mechanism that authenticates them via biometrics and links the authentication information (or security token) is required.

As we have already provided the API-GW in an NC7000 series product called the NC7000-WG our system is capable of quickly approaching the security measures required by the open API. For example, by means of an access control linked with the NC7000-3A, which is the biometric authentication platform.

The combination of the API-GW and integrated authentication platform provides a new platform for the Connected Economy/Open API era (**Fig. 7**).

## 6. Conclusion

In the above, we introduce our approach to biometric authentication for mobile phones. This is being undertaken concurrently with the advancement of financial services by introducing FIDO in financial institutions. We are also advancing the technical development and commercialization of products by combining our unique security technologies. We aim also to deploy our technologies and products in support of IoT security solutions in various fields, including for digital terminals and home appliances connected to the Internet.



## Reference

1) FIDO Alliance
https://fidoalliance.org/
2) Bank of America
http://newsroom.bankofamerica.com/press-releases/consumer-banking/bank-america-introduces-fingerprint-and-touch-id-sign-its-mobile-ban
3) Symantec's consciousness research on the password management in companies and individuals (Japanese)
http://internet.watch.impress.co.jp/docs/news/621665.html
4) NEC Press Release: NEC ranks first in NIST fingerprint matching technology benchmark test, August 21, 2014
http://www.nec.com/en/press/201408/global_20140821_02.html
5) NEC Press Release: NEC's Video Face Recognition Technology Ranks First in NIST Testing, March 16, 2017
http://www.nec.com/en/press/201703/global_20170316_01.html
6) FIDO Certified
https://fidoalliance.org/certification/fido-certified-products/

## Authors' Profiles

**NAKATSUKA Yutaka**
Manager
SDN/NFV Solutions Division

**IKEYA Ryohei**
Assistant Manager
SDN/NFV Solutions Division

**TEZUKA Yukiko**
Assistant Manager
SDN/NFV Solutions Division

**AMANO Shinichi**
Assistant Manager
SDN/NFV Solutions Division

**AOYAGI Toru**
Senior Principal Engineer
Financial Systems Development Division

**IWASA Ayaka**
Manager
Global 1st Systems Department
Transportation and City Infrastructure Division

# Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

**Link to NEC Technical Journal website**

Japanese

English

## Vol.11 No.2 FinTech That Accelerates Digital Transformation



### Papers for Special Issue



### NEC Information




Vol.11 No.2
June 2017

Special Issue TOP