ID Service Providing Instantaneous Availability of User's Desired Financial Services

AOYAGI Toru, TSUJI Yasunari, KAWAKAMI Eisuke, SAITOU Yoshihiro, SHINDO Yoshiko, MURAKAMI Takahiro

Abstract

The amendment of the Act on the Prevention of Transfer of Criminal Proceeds on 30th November 2018 made possible the completion of the online identification of bank account-opening customers that is obligatory for the financial institutions. Personal identification used to be carried out by forwarding non-transferrable postal mails to customer homes which takes quite a time. The online possibility of identification, now allows users to use a desired financial service immediately. To deal with the online account opening facility, NEC provides a Personal Identification Service making use of its world leading face recognition technology (face matching and impersonation prevention) to support the improvement of user experience and the promotion of digital businesses in financial institutions.

Keywords

face recognition, FIDO biometric recognition

1. Introduction

The amendment to the Act on the Prevention of Transfer of Criminal Proceeds on Nov. 30, 2018 permitted the completion of the online identification of account-opening customers. This would be obligatory for the financial

Quick opening of accounts per purpose

Opening of bank accounts has hitherto been troublesome. But the Digital KYC facilitates account opening so that several accounts may be opened according to their various usages. For example, to open an account for saving money for a trip, a joint account for a couple to control their incomes, or an individual account for each child to save academic fees. In this way, one may be able to spend money more meaningfully.

Learn brokerage and immediately open an account

Learning about stocks, investment trusts, bonds, deposits, insurances and FX... Friends recommend me to begin, but I am busy with my everyday work, I also enjoy playing around and, among all, I should learn about them in more details. Even when one does not have much time to spare, the Digital KYC allows you to open a brokerage account whenever you decide so. In the future, the mechanism will be advanced even more in order to encourage the will to learn and challenge in a more sophisticated manner.

Fig. 1 Images of services.

institutions, in addition to identification based on the forwarding of non-transferrable postal mails. With the online account opening, the financial institutions can reduce the costs for dispatching non-transferrable postal mails and also prevent the loss of opportunity for acquiring new users. The users sometimes reject opening their bank accounts in consideration of the time and labor caused by the number of days taken for postal forwarding. In addition to it, once any deficiency is found, users have to try another procedure to open bank accounts. On the other hand the user can easily and swiftly open an account for a purpose such as travel or education or for learning about investment at any time (**Fig. 1**).

NEC implements the online account opening procedure by providing the Personal Identification Service based on its world leading face recognition technology[1] in order to support the digital society.

2. Personal Identification Service

2.1 Outline of the Amendment to the Act of Prevention

The recent amendment to the Act of Prevention of

Transfer of Criminal Proceeds defined the following four methods that permit the completion of online identification (**Fig. 2**). For the main method that is "photography of a customer's face (Article 6, paragraph 1, item v)", NEC supports the real-time account opening of users by means of the matching and impersonation prevention, by making use of NEC's face recognition technology.
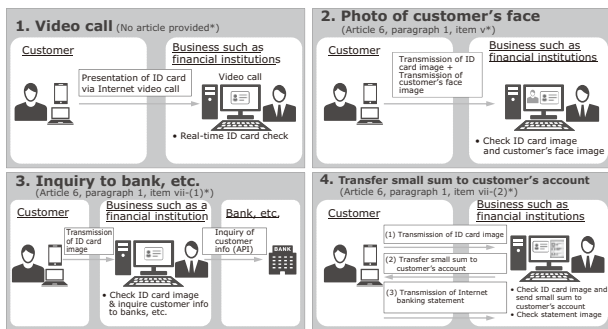

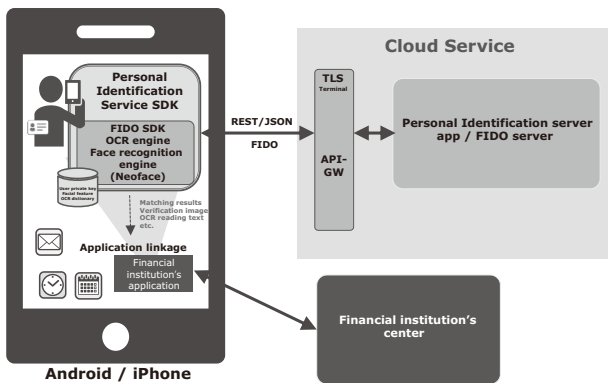Fig. 2 Methods of identification prescribed in the Act of Prevention.

Fig. 3 Overall configuration.

2.2 Outline of Personal Identification Service

The Personal Identification Service is embedded in a direct app such as an internet banking service already provided by a financial institution. As it uses a single app for operations from account opening to the provision of its various services, it is provided as an SDK (Software Development Kit) (**Fig. 3**) to improve user experience and to enable identification management.

The specific processing employs the "ID Selfie" method, with which a "view of the applicant's face" and an "ID document with photo for certifying the ID (driver's license, My Number card, etc.)" are shot together with the selfie or self-portrait photography of a smartphone. They are then checked to confirm if the view of the person in front of the camera matches the photo in the presented document. The ID Selfie method enables secure identification for account opening because face matching is executed while the person in front of the camera is surely presenting the "ID document".

The verification is performed on the FIDO (Fast IDentity Online) protocol which is the de facto standard of biometrics-based online identifications[2].Users register the "face feature quantity template (data registered by extracting feature data of the user's face)" in the secure area in their smartphones at the beginning of the application for their account opening. This template can be used as a means of biometric login in place of the ID/password, for example in matching with the photo on an ID document and matching for impersonation prevention as well as in log-in of a direct service such as Internet banking.

3. The FIDO Approach to Biometric Recognition

Since the foundation of the FIDO Alliance in 2012, various technical specifications have been released to standardize the password free identification of online
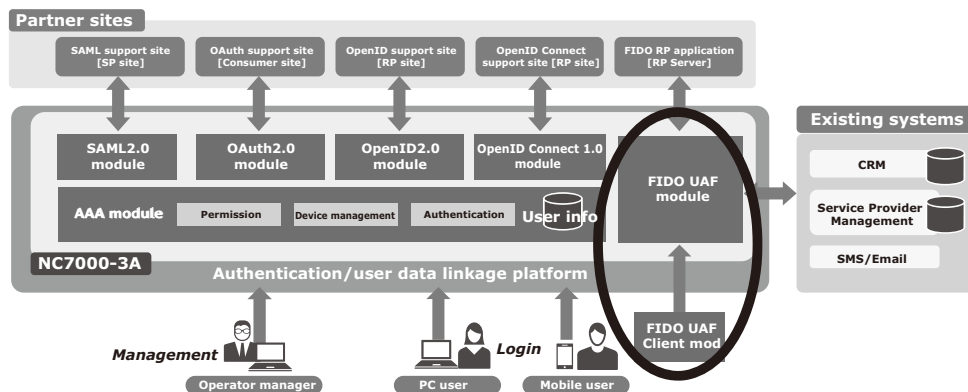

Fig. 4 Configuration of NC7000-3A software.

services from the stance of establishing authentication standards that offer both strong security and easiness of use. Major players in various fields including the financial institutions, communications carriers and security vendors are participating in this project, making its standards the worldwide de facto ones.

One of the features of the FIDO authentication is that the privacy information is not provided to the server side, including the communication path. Another feature is that it adopts the public key encryption technology (hereinafter the key pair generated by it will be referred to as the FIDO authentication key). This does not let the user's feature quantity template and secret key go out of the device so the user can be protected from phishing and MITM or man-in-the-middle attacks.

NEC released FIDO UAF 1.0 compliant software in the NC7000-3A series of integrated authentication platform software in July 2017 (**Fig. 4**).

Roughly speaking, FIDO provides three types of standards including; 1) UAF; 2) U2F; 3) FIDO2 (web authentication).

(1) The UAF stands for Universal Authentication Framework and includes the standards with FIDO-compatible devices without using passwords.

(2) U2F stands for Universal Second Factor and is a standard based on two-factor authentication.

(3) FIDO2 (web authentication) performs FIDO authentication via the web browser, and the latest specifications are made public as the candidates for recommendation at W3C[3]. A user of the CTAP (Client to Authenticator Protocol) is able to send a direct authentication request from a browser or OS to an external authenticator (USB key or smartphone, etc.), thereby making it unnecessary to re-register the FIDO authentication key for every device.

The FIDO products are composed mainly of the FIDO server, FIDO client and FIDO Authenticator (for each biometric authentication based on face, voiceprint, fingerprint, etc.) (**Fig. 5**). NEC develops all of these components in house (FIDO2 products are under prepara-
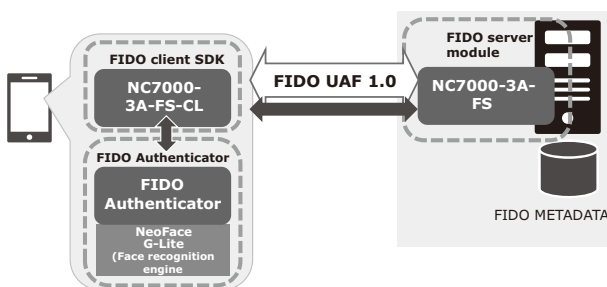
tion) as the Certified Products of the FIDO Alliance that are compliant to the FIDO specifications[4].

4.1 Accuracy of face recognition

The face recognition authenticator is NeoFace-G Lite proven to have the highest accuracy and performance worldwide. This is the lightweight version for use in mobile authentication of the server-side face recognition engine. With a high authentication accuracy similar to the server side (when the false acceptance rate FAR = 0.0001%, the false rejected rate FRR is 0.25%), it serves to prevent impersonations (**Fig. 6**).
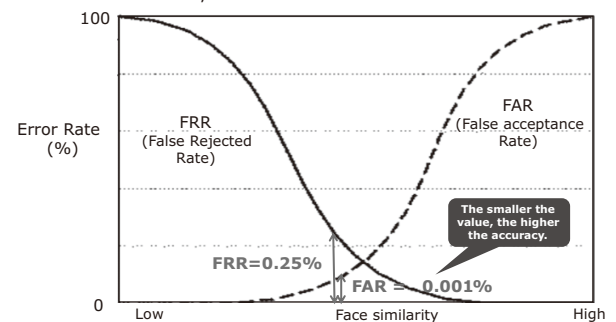
4.2 Impersonation prevention

To prevent the risk of illegal account opening based on impersonation by showing a photo or video of a different person for the purpose of money laundering or terrorist financing, a Face Liveness Detection technology is provided (**Fig. 7**). This function gives instructions on random face movements and verifies if the instructed movement is completed within the specified period. As the testing cannot be cleared unless the real living person is in front of the smartphone camera, impersonation of another person becomes difficult.

- Random selection from smile, face orientation, face tilting, eye wink, etc.
- The number of movements is selected using a suitable parameter, and the same instruction is not given successively.

The verification with NEC's Liveness technology is executed within the smartphone so the operation is very smooth without being affected by the quality of commu-

- When FAR=0.1%, FRR=0.08%. When FAR=0.01%, FRR=0.13%.
- When FAR=0.001%, FRR=0.25%.

Fig. 5 FIDO product configuration (UAF1.0).

Fig. 6 Accuracy of NeoFace-G Lite.
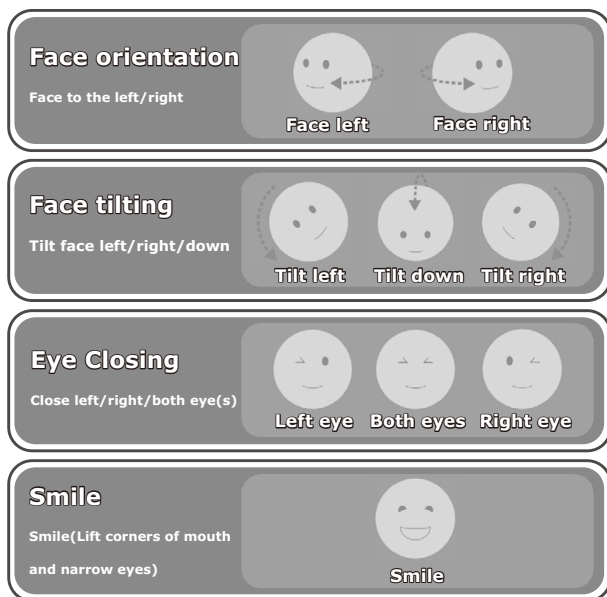
Fig. 7 Examples of Liveness Detection Technology.

Fig. 8 Matching between ID document and camera-shot image.
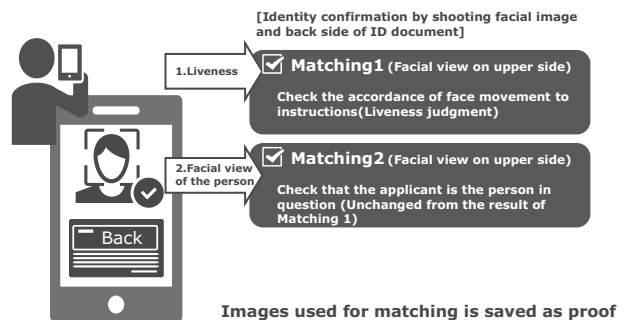
Fig. 9 Matching with the back side of ID document.

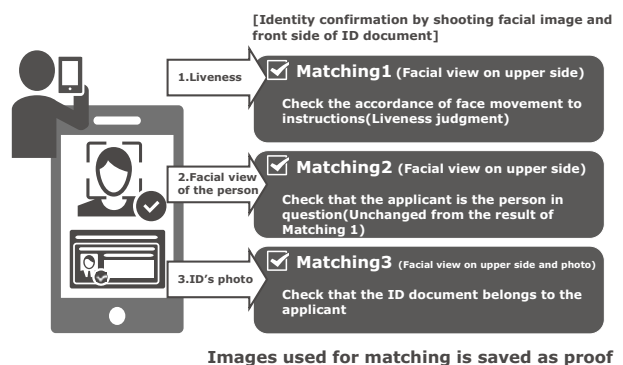Fig. 10 Shooting of ID document thickness.

nication.

The next version is planned to detect impersonation additionally by means of 3D masking based on visible light checking making use of deep learning.

In this way, the severity of the identification at the time of a bank account opening is increased thanks to the high authentication accuracy and impersonation prevention function of the engine for mobile devices.

5. Image of Identification Processing at Account Opening

(1) Matching between ID document and the personal image shot with the camera (Fig. 8):
The applicant's face and his/her ID document (front side) are shot together using the selfie camera of a smartphone to check the identity. Impersonation is prevented by the Liveness technology. When matching is successful, the face feature data template is registered.

(2) Matching the back side of an ID document (Fig. 9)
The applicant's face and his/her ID document (back side) are shot together using the selfie camera of a smartphone. The applicant's face is matched with the face feature data template for authentication.

(3) Shooting of the thickness of ID document (Fig. 10)
The applicant's face and his/her ID document (side view) are shot together using the selfie camera of a smartphone. The applicant's face is matched with the face feature quantity template for authentication. To prevent falsification, the shot movie of the
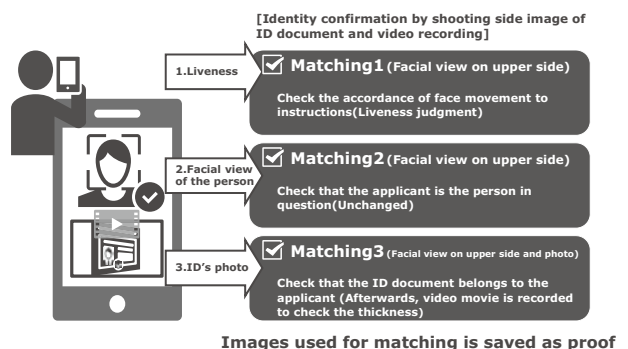
ID document is checked visually in the processing of the financial institution to confirm the features such as the thickness.

(4) OCR of ID document and verification of applied items
Information entered in the ID document (both sides) is subjected to OCR and the applied information required for the account opening, including the name and address, is input automatically.

(5) Service provision after account opening

A financial institution performs an account opening procedure based on the information in the application. At this time, the ID of Internet banking or online trade is tied to the biometric information used at the time of an account opening so the user can immediately receive a service after a biometric login is performed.

6. Application of Personal Identification service

In addition to account opening and large money transfers as prescribed in the Act on Prevention of Transfer of Criminal Proceeds, the Personal Identification Service may be applicable to the following operations (**Fig. 11**).

(1) Identification at cellphone purchase

Application to identity confirmation at the time of cellphone contract, as defined in the Mobile Phone Improper Use Prevention Act.

(2) Identification at ticket purchase or at a sharing site

Application to identify confirmation at the time of ticket purchase as defined in the Ticket Resale Regulation Act, and at the time of used commodity purchase/sale at sharing sites.

(3) Personal Data Store (PDS)/Information bank

These organizations perform rigorous identity checks, manage personal data under the leadership of individual persons, and also provide the data to third parties in place of the individual persons by determining the appropriateness according to the instructions by individuals or based on the conditions specified in advance.

7. Conclusion

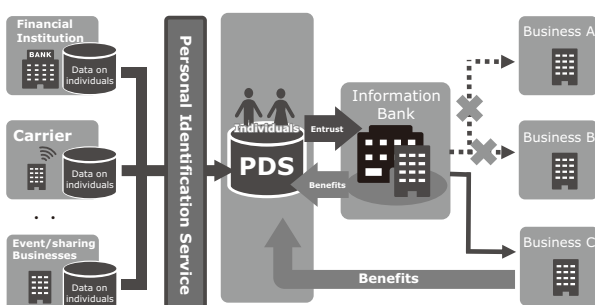This paper introduces the efforts for provision of the Personal Identification Service applying the face recognition technology to prepare for the completion of online account opening.

This service allows the financial institutions to reduce the costs of non-transferrable mails and also prevents the opportunities lost in user acquisitions. For the users, it enables the immediate use of a desired financial service. Its rigorous individual identification is suitable for applications to biometric login for Internet services and in the future, personal data management and Information Banks will be serviced. Now that digitalization and speed increase are effective keys to competitiveness, it is important to be capable of exchanging directly with users via smartphones and websites, analyzing their behavior data and improving services accordingly in order to improve usability. At NEC, we are determined to contribute to the creation of new digital businesses based on Personal Identification Services, as well as on biometric authentication technologies.

---

* FIDO is a trademark of FIDO Alliance.
* Android is a trademark and/or a registered trademark of Google Inc.
* iPhone and iPad are trademarks of Apple Inc. The iPhone trademark is used under license from AIPHONE CO., LTD.
* All other company names and product names that appear in this paper are trademarks or registered trademarks of their respective companies.

Reference

1) NEC Press Release, NEC's Video Face Recognition Technology Ranks First in NIST Testing, 2017.3
https://www.nec.com/en/press/201703/global_20170316_01.html
2) FIDO Alliance
https://fidoalliance.org/
3) Web Authentication:An API for accessing Public Key Credentials Level 2
https://w3c.github.io/webauthn
4) FIDO Certified
https://fidoalliance.org/certification/fido-certified-products/

(Source) Approach to Social Implementation of "Information Bank", Ministry of Internal Affairs and Communications (July 2018), with some additions

Fig. 11 Image of deployment of Personal Identification Service.

Authors' Profiles

AOYAGI Toru
Senior Principal Engineer
Financial Digital Innovation Technology Development Office

TSUJI Yasunari
Project Manager
Financial Digital Innovation Technology Development Office

KAWAKAMI Eisuke
Assistant Manager
Financial Digital Innovation Technology Development Office

SAITOU Yoshihiro
Assistant Manager
Financial Digital Innovation Technology Development Office

SHINDO Yoshiko
Assistant Manager
Financial Digital Innovation Technology Development Office

MURAKAMI Takahiro
Financial Digital Innovation Technology Development Office

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

Vol.13 No.2 Social Value Creation Using Biometrics

Vol.13 No.2
April 2019

Special Issue TOP