Biometric Authentication Technologies of Client Terminals in Pursuit of Security and Convenience

● Hiroshi Yokozawa ● Takashi Shinzaki ● Akira Yonenaga ● Atsushi Wada

An environment is now in place that can offer services utilizing information and communications technology (ICT) in various scenes of daily life, and a wide range of operations and commercial transactions are becoming cloud-based. In this situation, biometric authentication is becoming widespread as a reliable and simple means of user authentication. Fujitsu started providing biometric authentication devices for PCs in 1999. Subsequently, we have worked on the development of biometric authentication technologies for notebook PCs and smartphones, pursuing convenience as well as security. This paper presents Fujitsu's activities related to biometric authentication technologies, centering on the integration of a slimmed-down palm vein sensor in tablets and the successful integration of iris authentication in a smartphone for the first time in the world.

1. Introduction

Nowadays, with the increased use of information technology for social systems and the development of network services, a variety of operations and commercial transactions are becoming cloud-based, and an environment that allows the use of services utilizing information and communications technology (ICT) in daily life is in place. In this situation, biometric authentication technology is becoming widespread as a reliable and simple means of user authentication. Moreover, client terminals directly operated by users are becoming increasingly diverse, with devices such as smartphones and tablets now being commonly used besides conventional devices such as PCs and mobile phones. This is generating demand for the implementation of easy-to-use and highly accurate biometric authentication technologies on various types of terminals.

This paper presents Fujitsu's activities related to biometric authentication technologies until now. Next, it presents palm vein sensors developed for tablets and iris authentication technology developed for smartphones.

2. Fujitsu's activities until now

Fujitsu has developed biometric authentication technologies that use physical features information as functions to prevent spoofing while maintaining the convenience of PCs and smart devices (**Figure 1**). For example, we began offering, as PC peripherals, fingerprint authentication devices (FS-200P, FS-200U) combining a capacitance-type fingerprint sensor with an authentication algorithm using the connected-minutiae-relation method in December 1999. Then we began equipping notebook PCs with plane-type fingerprint sensors in October 2000, and from 2004, we started applying the adaptive connected-minutiae-relation method, which is an improved authentication algorithm, along with the use of smaller and lower cost sweep-type sensors. The use of sweep-type sensors greatly expanded the number of devices that support fingerprint authentication.

Further, to improve the availability of biometric authentication, which is a priority for corporate customers, we launched notebook PCs equipped with a palm vein sensor in May 2011. Then, in July 2013, we equipped thin notebook PCs with even more compact palm vein sensors and also successfully mounted them on tablets. These various products are being used by organizations that require a high level of security such

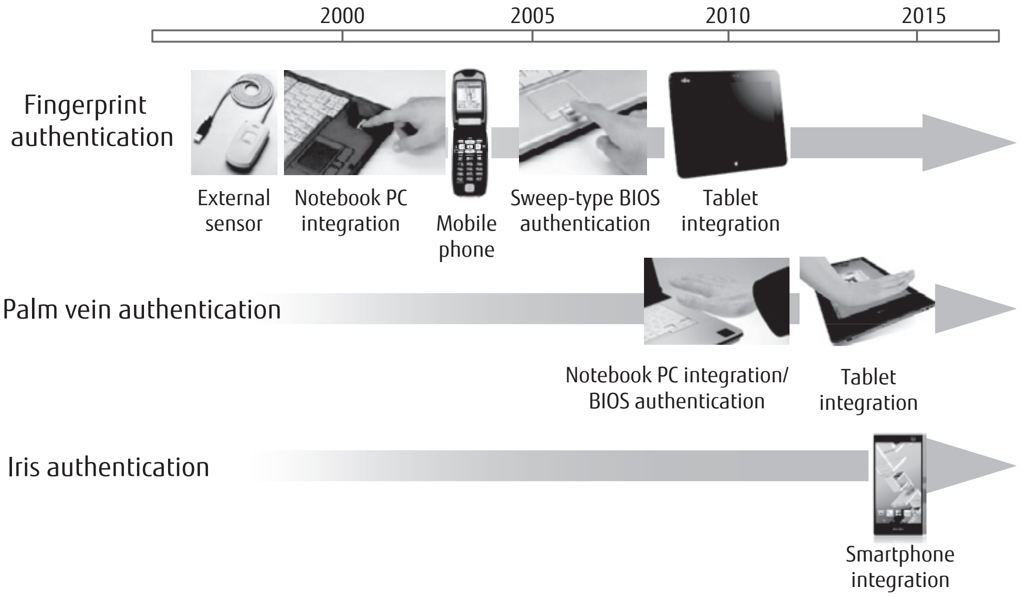


Figure 1
Integration of biometric authentication technologies to terminals.

as financial institutions.

For fingerprint authentication and palm vein authentication on notebook PCs, a pre-boot authentication function that performs biometric authentication on startup of the basic input/output system (BIOS) is also implemented.

For corporate PCs that are required to offer such biometric authentication capabilities, a biometric authentication appliance server (Secure Login Box) was commercialized in August 2002 for the purpose of making the implementation of authentication security systems a simple and hassle-free process. This solution makes it possible to perform Windows login and application login through biometric authentication by centrally managing biometric information and passwords on the server.

Then, in July 2003, fingerprint authentication started being implemented on mobile phones as a way to improve user experience. Until now, Fujitsu has promoted the integration of the various security features of mobile phones with fingerprint authentication.

Starting in 2013, we have been working on providing iris authentication on smartphones to further improve security and the user experience. Iris authentication is highly convenient in that it allows authentication just be looking at the screen. Further work was done to integrate iris authentication with the password manager and offer also FIDO[note)] compliance (**Figure 2**), resulting in the launch of the world's first smartphone featuring iris authentication in May 2015.

3. Tablet-integrated palm vein sensor

The palm vein sensor developed by Fujitsu in 2011 had a height of 11.2 mm and thus could fit only in thick notebook PCs. In response to user demand for inclusion of palm vein sensors in thin notebook PCs and tablets, in 2013, Fujitsu developed a more compact palm vein sensor with dimensions of 25.0 mm wide, 25.0 mm deep, and 6.0 mm high, which was achieved by pursuing thinner optical systems for lighting and image capture.

The mounting position of the palm vein sensor in tablets was studied from the viewpoint of usability and development cost. In terms of development cost, installing the palm vein sensor on the rear side of the tablet would reduce development cost because this position would necessitate only designing a new cover for existing models. Moreover, this would allow commercialization without having to increase terminal size, a merit for users. To verify usability for users, prototypes equipped with a palm vein sensor on the rear side were

note) Acronym for Fast IDentity Online. An authentication method that sends the result of authentication in the terminal to the cloud.

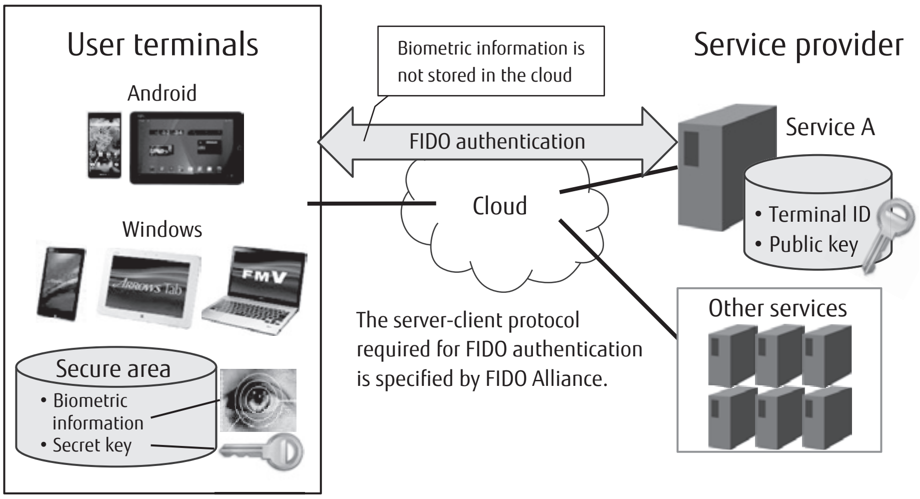


Figure 2
FIDO compliance for iris authentication.

created and tested.

Actual use of these prototypes revealed that getting users to pass their hand over the sensor without being able to see the imaging position of the palm vein sensor on the rear side of the tablet was extremely difficult. As a result, it was decided to install the sensor next to the screen (**Figure 3**) focusing on usability, although this would mean a larger terminal size and require extra development cost.

The inclusion of this palm vein sensor resulted in a product that achieved both portability and security, and led to adoption by financial institutions, etc.

4. Smartphone-integrated iris authentication sensor

Easy use of iris authentication by smartphone users requires that users be able to hold the smartphone in a natural way during authentication. The distance from the user's eyes to the sensor of the smartphone is an important factor in this regard. Conventionally, the smartphone needed to be brought near the user's face in order to achieve sufficient authentication accuracy. To solve this problem, a high-resolution infrared camera and high-power infrared LED were developed, allowing authentication with a practical eye-sensor distance range of 25 to 35 cm.

Moreover, for convenient use of iris authentication by users, we developed also reliable registration technology for dependable iris image capture, and split-second authentication technology for instant authentication. These technologies make possible the optimal design of the mounting position, spacing, and angle of the infrared camera and infrared LED within the restricted space of smartphones to ensure reliable image capture of the iris (**Figure 4**).

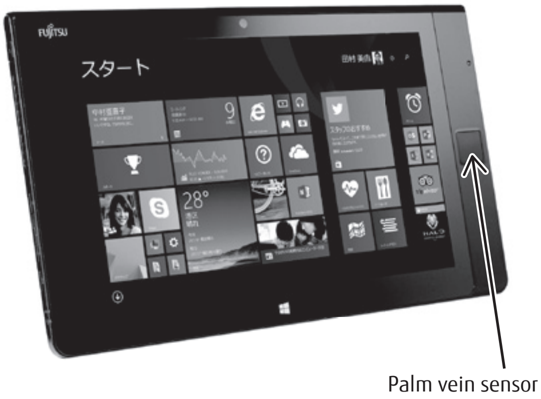


Figure 3
Integration of palm vein sensor to tablet.

Furthermore, as this would be the first time for users to perform iris authentication on a smartphone, it was important that the operation procedure be clearly relayed. As it is difficult for users to visualize a procedure based on words alone, we decided to show the actual procedure through an animation. To further ensure easy and accurate registration, we decided to provide users with illustrations clearly showing the

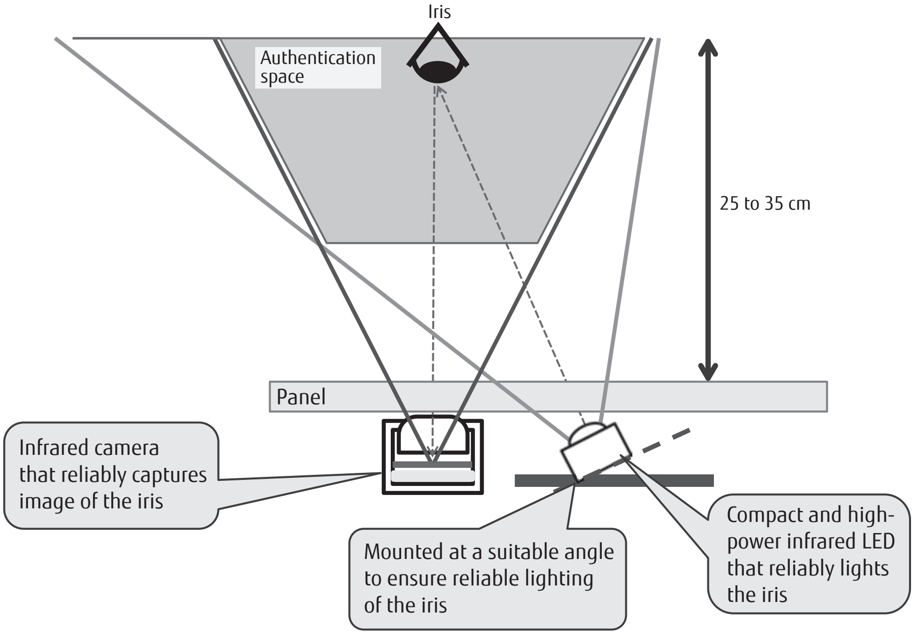

Iris
Authentication space
25 to 35 cm
Panel
Infrared camera that reliably captures image of the iris
Mounted at a suitable angle to ensure reliable lighting of the iris
Compact and high-power infrared LED that reliably lights the iris

Figure 4
Authentication space using infrared camera and infrared LED.

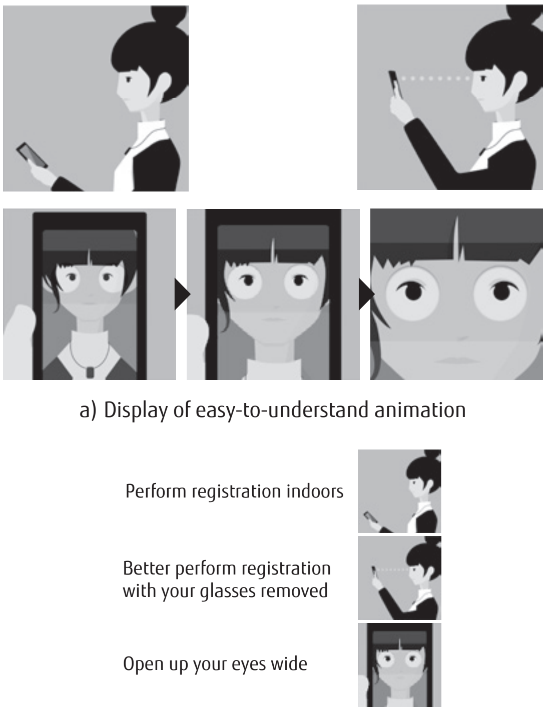
recommended approach (**Figure 5**).

The ARROWS NX F-04G smartphone for NTT DOCOMO was the first smartphone in the world to feature an iris authentication function that unlocks the screen through iris authentication that uses the above-described technologies. We implemented also password-less login to online services through the above-mentioned FIDO compliance.

5. Future prospects and challenges

As various types of terminals become equipped with biometric authentication functions, the advantages of biometric authentication technologies as a way to improve not only security but also convenience are being recognized. Another demand has been a cloud-based authentication service that allows use anywhere following registration, and we have been developing technologies with a view to providing such a service.

The focus of corporate customers is on treating the biometric data of users that has been registered in the past as an asset, and also to maintain data compatibility. On the other hand, there is also concern on the user side about placing in the cloud biometric information that cannot be modified. We are also conducting research and development to make biometric


a) Display of easy-to-understand animation

Perform registration indoors
Better perform registration with your glasses removed
Open up your eyes wide

b) To-the-point and easy-to-understand explanations

Figure 5
Iris authentication guidance for smartphone users.

authentication processing inside terminals more secure, allow the registered data to be changed freely like passwords, and create biometric information protection technology for stronger irreversible processing.

The cost of the sensors that are used is expected to fall with the spread of biometric authentication. Fujitsu will aim to further expand the application environment and convenience of biometric authentication through multi-biometrics technology combining multiple authentication methods. Moreover, with regard to the application of biometric authentication to wearable devices, we will promote the use of a variety of authentication methods that are right for the situation.

6. Conclusion

This paper has introduced biometric authentication technologies developed by Fujitsu such as palm vein authentication and iris authentication.

We have successfully downsized palm vein authentication to a level that allows its use in tablets, while maintaining a high level of authentication accuracy even compared with other biometric authentication methods. For iris authentication, we have successfully created and commercialized implementations that allow an infrared camera and infrared LED to be mounted in the limited space available on smartphones.

Fujitsu aims to further evolve biometric authentication technologies to allow their everyday use by everyone, from children to the elderly. We will proceed with research and development work on biometric authentication technology to make our lives safer, more secure, and more convenient. Aiming beyond security for personal computers, tablets and smartphones, we will develop a wide range of products that include also cloud-based services and other solutions.

Hiroshi Yokozawa
Fujitsu Ltd.
Mr. Yokozawa is currently engaged in development of security devices for terminals.

Takashi Shinzaki
Fujitsu Laboratories Ltd.
Mr. Shinzaki is currently engaged in research on biometric authentication technology and systems.

Akira Yonenaga
Fujitsu Ltd.
Mr. Yonenaga is currently engaged in development of iris authentication and other security devices.

Atsushi Wada
Fujitsu Ltd.
Mr. Wada is currently engaged in development of authentication applications for personal computers.