Privilege Sharing and Transfer Based on Passwordless Authentication

Yasuhiko Yoshimura, Yurika Suga, Yoshihiko Omori, Takao Yamashita, and Akira Shibata

Abstract

Research is underway at the NTT laboratories on an authentication platform that provides both security and convenience. This article describes secure and passwordless authentication platform technology for application to a variety of services that use smartphones and other mobile devices that have grown in popularity. This technology is expected to be applied to a wide array of services to improve their convenience of use.

Keywords: authentication, passwordless, FIDO

1. Introduction

The explosive increase in the use of mobile devices such as smartphones has been accompanied by the ability to use all sorts of online services regardless of location. Although the method of authentication using an identifier (ID) and password has become commonplace when using individual services, it requires the user to remember and input a different password for each service. This presents a problem in terms of convenience. There is also concern about spoofing (impersonation) due to leaked IDs and passwords. In response to these problems, we have been studying technologies with the aim of achieving secure and convenient authentication.

2. FIDO-related technology

The FIDO (Fast IDentity Online) Alliance proposes an authentication method using public key encryption technology to achieve secure and convenient authentication (**Fig. 1**) [1]. One set of FIDO specifications presents the Universal Authentication Framework (UAF) protocol that assumes the use of mobile devices such as smartphones. The UAF protocol stores a private key for authentication in a secure area of the mobile device (such as a secure element (SE) or trusted execution environment (TEE)) and uses the mobile device as an authentication token. Using public key encryption technology at the time of authentication provides a high level of security without the need for secret information (such as a password) shared by the server and device. Passwordless authentication can also be achieved using some means of personal confirmation such as biometric authentication that mobile devices are beginning to provide as standard.

3. Overview of convenience-enhancing technology

Various service providers have begun to introduce FIDO-certified authentication ecosystems reflecting the ongoing spread of FIDO technology. We at the NTT laboratories seek to make people's lives more convenient by enabling users to share privileges to use products and services provided by the application with FIDO technology.

When using public key encryption technology that is used in secure authentication methods such as FIDO UAF, as many keys as the number of services being used will be registered in the mobile device, but when using a new device such as when upgrading to a new model, a user has to re-register those keys. The proposed convenience-enhancing technology would ease the burden of such re-registration by providing a

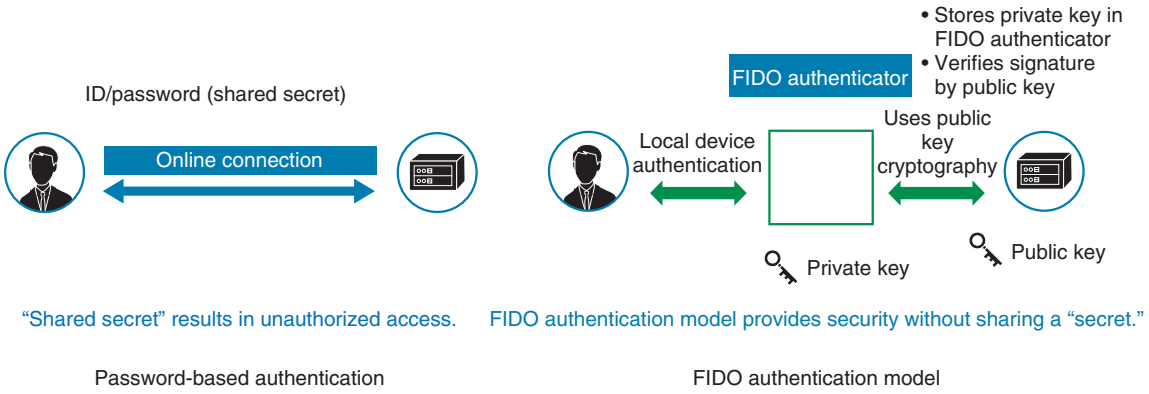


Fig. 1. Features of FIDO authentication.

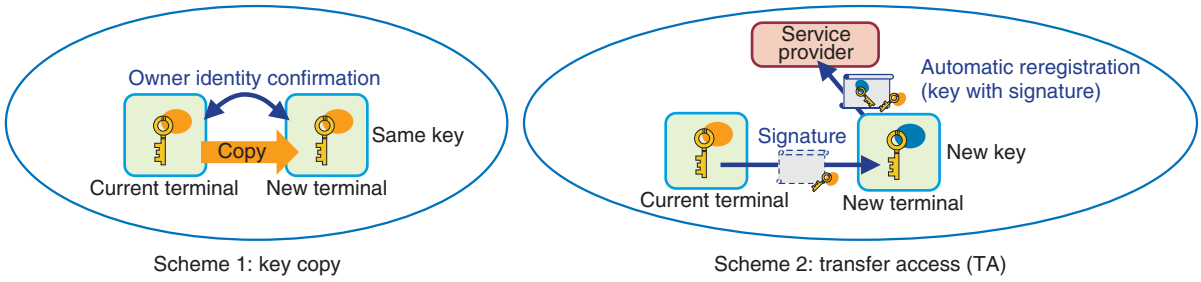


Fig. 2. Overview of key-sharing (transfer) schemes.

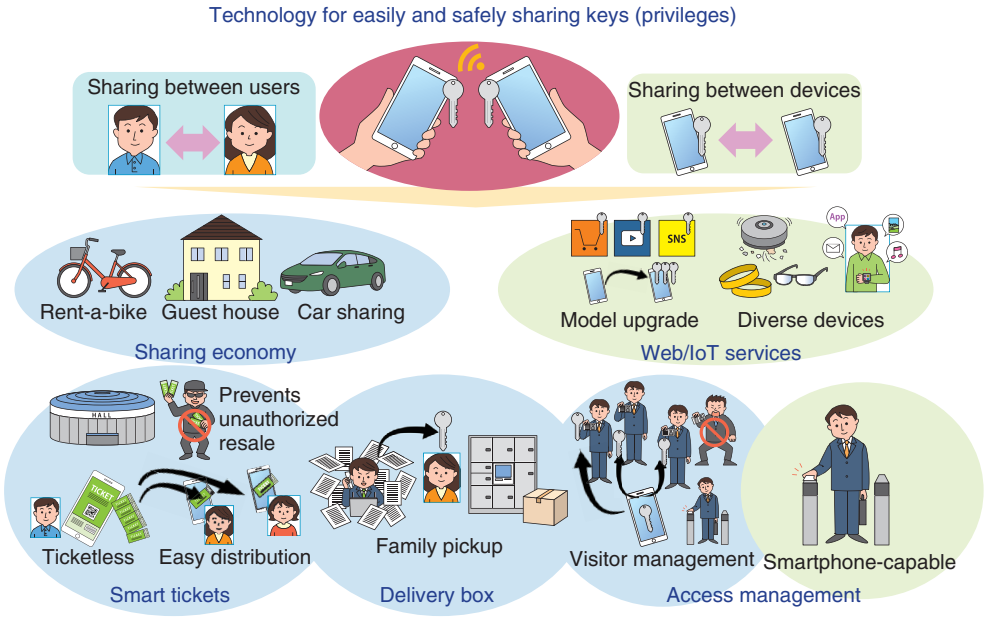
mechanism for securely and easily sharing keys among multiple devices.

An overview of key-sharing (transfer) schemes at the core of this convenience-enhancing technology is shown in **Fig. 2**. Scheme 1 is a key-copy scheme that duplicates a private key stored in the SE/TEE area of a device in a new device. To ensure security, this scheme incorporates various methods to verify the user of a device such as biometric authentication and identity confirmation using a digital certificate, and it uses proximity communication methods to eliminate communications over the Internet such as near-field communication or Bluetooth [2]. In addition, key sharing between two devices can be achieved by a simple device operation using biometric authentication and device-pairing via device-to-device contact.

Scheme 2 is a transfer access (TA) [3] scheme developed by researchers at the University of Washington in Seattle, USA. In this scheme, a new device notifies the server (service provider) that the user of a new device is the same as a user whose private key has already been registered by sending a digital signature calculated using the private key. This scheme is effective when a service provider needs to detect the addition of a device by a user, though it requires the modification of an authentication server.

4. Application of convenience-enhancing technology

We are researching methods to achieve privilege sharing (transfer) to use services and resources by using mechanisms such as those for sharing private keys among devices used in convenience-enhancing technology [4]. Enabling the current device and a new one in the TA scheme in Fig. 2 to correspond to user A and user B, respectively, public key registration by user B will mean, from the viewpoint of the service provider, that user A who already has the privilege to use a service has passed it to user B. This technology can be applied not only to sharing privileges to use services between devices but also to various types of services by using it to grant certain privileges from one user to another (**Fig. 3**).



App: application
IoT: Internet of Things
SNS: social networking service

Fig. 3. Application of convenience-enhancing technology.

5. Future outlook

We described a secure and convenient method for sharing and transferring privileges to use services without the need for passwords. Looking to the future, we plan to study specific systems for applying this method to a variety of services as shown in **Fig. 3** to achieve a general-purpose and sophisticated authentication platform and add value to related services.

References

[1] FIDO Alliance, https://fidoalliance.org/
[2] H. Nishimura, Y. Omori, T. Yamashita, and S. Furukawa, "Secure Authentication Key Sharing between Mobile Devices Based on Owner Identity," Proc. of the 4th International Conference on Mobile and Secure Services (MobiSecServ 2018), Miami Beach, FL, USA, Feb. 2018.
[3] A. Takakuwa, T. Kohno, and A. Czeskis, "The Transfer Access Protocol - Moving to New Authenticators in the FIDO Ecosystem," Technical Report UW-CSE-17-06-01, The University of Washington, 2017.
[4] Y. Omori, H. Nishimura, and T. Yamashita, "A Study on the Authorization for the Use of Services among Many Users on the Internet," Proc. of the 2018 IEICE Society Conference, B-7-18, Kanazawa, Japan, Sept. 2018 (in Japanese).

Trademark notes

Yasuhiko Yoshimura
Senior Research Engineer, Server Network Innovation Project, NTT Network Service Systems Laboratories.

He received an M.S. in engineering from Kyushu University in 2001. Since joining NTT in 2001, he has been engaged in research of quality of service (QoS) management technologies, video streaming technologies, network architecture, and authentication technologies. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).

Yurika Suga
Server Network Innovation Project, NTT Network Service Systems Laboratories.

She received a B.S. in mathematics from Japan Women's University, Tokyo, in 2018. She joined NTT in 2018, where she has been researching authentication technologies and personal data management on the Internet.

Yoshihiko Omori
Research Engineer, Server Network Innovation Project, NTT Network Service Systems Laboratories.

He received an M.E. in electrical communication engineering from Tohoku University, Miyagi, in 1993. Since joining NTT in 1993, he has been researching traffic control in IP (Internet protocol)-based networks, QoS control, operation systems for virtual private networks, authentication technologies, and packet networks for mobile communications at NTT Telecommunication Networks Laboratories and NTT DOCOMO. He is a member of IEICE.

Takao Yamashita
Senior Research Engineer, Server Network Innovation Project, NTT Network Service Systems Laboratories.

He received a B.S. and M.S. in electrical engineering in 1990 and 1992 from Kyoto University, where he also received a Ph.D. in informatics in 2006. He joined NTT in 1996, where he has been conducting research on multimedia communications, clock synchronization, data replication, grid computing, network security, and user authentication. His current research interests encompass information security, cloud computing, Internet of Things, and distributed algorithms. He is a member of IEICE, the Institute of Electrical and Electronics Engineers, the Information Processing Society of Japan, and the American Physical Society.

Akira Shibata
Director, Senior Research Engineer, Supervisor, Server Network Innovation Project, NTT Network Service Systems Laboratories.

He received a B.E. and M.E. in electrical engineering from Waseda University, Tokyo, in 1991 and 1993. He joined NTT Communication Switching Laboratories in 1993. Since then, he has been involved in research and development of network service systems. His current research interests include network security operations. He is a member of IEICE.