A Study on Improvement of Digital Personal Information Identification Service using Various Authentication Methods

Jong Bae Kim
Dept. of Computer and Software,
Sejong Cyber University, S. Korea,
jb.kim@sjcu.ac.kr

Article Info
Volume 81
Page Number: 2329 - 2336
Publication Issue:
November-December 2019

Article History
Article Received: *5 March 2019*
Revised: *18 May 2019*
Accepted: *24 September 2019*
Publication: *12 December 2019*

Abstract

In this paper, we analyze the trend of the authentication method used as a means to verify the identity of users in online non-face-to-face transactions. In addition, the proposed method describes matters to be considered when applying the authentication method for identity verification. On-line authentication technologies are mainly composed of multiple authentication technologies using various means. However, there is a problem that the complex authentication technology increases inconvenience for the online service users. In addition, online service providers are also experiencing service cost problems due to the combination of authentication methods. In this paper, we propose a method to improve the authentication of various inconveniences of the complex authentication technology. The proposed method investigates the current status of the authentication technology used in Korea and overseas, analyzes the types and characteristics of each authentication technology, and presents an effective method for applying it in the online service field. We propose the advantages and disadvantages of each authentication technology by analyzing the trend of the authentication technology and suggest a method to utilize it effectively in online service markets. Through the application of the proposed authentication technology, it can be used to build more secure and reliable online service.

Keywords*: identity verification, online service, personal identity information, personal authentication service.*

1. INTRODUCTION

Generally, for secure online service, it is necessary to clearly identify or authenticate the user [1-4]. Personal identification is the process of proving and authenticating to third parties that the user is legitimate and agreed to in accordance with reasonable procedures. And, the personal verification is a process of confirming whether the user is actually the user through the electronic personal information provided by the online service user [5]. There are many ways to identify yourself in face-to-face or non-face-to-face manner [9-11]. The face-to-face method is primarily used by resident centers, banks, and telecom companies, and non-face-to-face is an online authentication method used in electronic banking and online transactions [6]. The means of identification can be divided into electronic and non-electronic media. An authentication method using an electronic medium is I-PIN, a public certificate, a cellular phone authentication, an ID/PW, and a biometric authentication method. And authentication methods using non-electronic medium include certifications (identification card, driver's license, passport, etc.), passbook, and credit card.

Table 1 shows the classification of identity verification methods [6].

Table 1: Classification of identity verification means

Methods	Explanation	Limitations
face-to-face/non-face-to-face	classified by space and method	Increased non-facing contact than face-to-face contact
electronic/non-electronic medium	classified according to the information needed to identify you	Increased non-electronic way of digitization of personal information

As shown in Table 2, the means for authenticating the user are divided into an ownership base, a knowledge base, and a feature base. Various technologies for personal identification are emerging. In order to complement the advantages and disadvantages of Table 2, personal identification services are becoming mainstream through compound authentication. However, the complex authentication using various authentication methods can increase the authentication strength, but the user 's usability is poor. Therefore, it is necessary to propose effective measures to enhance the security level of user authentication in online service while also providing convenience for users.

The proposed method examines the types of authentication methods and examines the current situation in Korea and abroad and analyzes the advantages and disadvantages of each authentication method. Based on the results of the analysis, we propose a personal identification method that can guarantee the user 's convenience while enhancing security strength in online service. It is necessary to analyze the development of technical means for domestic and foreign personal identification and the application trends of online service, and to examine the features of each authentication technology [7-9].

Online service providers are aware that various authentication technologies exist, but they are not using it for online service. In Korea, there is a resident registration number that uniquely identifies the user, so diversification of authentication technology is slow.

In Korea, there is a resident registration number that uniquely identifies the user, so diversification of authentication technology is slow. However, in the case of overseas, a variety of personal authentication technologies are appearing and utilizing due to the absence of information that can uniquely identify the user. Therefore, we analyze the status of the authentication service that is used in the online service from abroad and seek ways to utilize it.

Table 2: Advantages and disadvantages of authentication methods

Methods	Advantages	Disadvantages
ownership	Relatively safe due to high level of security Usage change and substitution possible	High stolen, lost, forged Inconvenience of carrying Additional costs such as purchase, distribution, management, and license renewal
knowledge	No additional costs except development and management fees Usage change and substitution possible	Low security level Impersonation is easy Depends on individual memory
feature	Accurate identity verification Low theft, lost, high convenience	High cost of introduction and management No change or substitution User Rejection due to Biometric Information Storage

2. STATUS OF PERSONAL IDENTIFICATION TECHNOLOGY

The authentication means can be divided into possession, knowledge, features, etc., and each type of authentication means can be listed as shown in Table 3. Each authentication method is currently used in online services, and some of them are being used as a means of personal identification, which replaces the Korean resident registration number.

Technologies that utilize ownership, knowledge, features, and other means for identity verification are now in use. Most of the authentication technologies are applied to confirm the personal identity in the online and are used for the purpose of confirming the users' opinions. In Korea, technologies using alternative means based on resident registration numbers are used to uniquely identify users. Alternative means include the I-Pin, cell phones, credit cards, and accredited certificates [11].

2.1 Ownership-Based Personal Identification

A representative means of ownership-based personal identification technology is certificates. Among the major overseas countries, many of the public certificates are using private certificates. As a representative example, the Bank of America (BOA) and US bank, which have internet banking services in the US, provide a question-and-answer login authentication such as Sitekey and ID Shield in addition to ID/PW. In the UK [2], Lloyds TSB bank provides telephone authentication services, and Barclays bank and Royal bank of Scotland provide ID/PW and smart card reader OTP for 2-factor authentication for login and account transfer. Ownership-based personal identification technologies are mostly compound authentication technologies that utilize a variety of means. Especially, in order to guarantee the trust and accuracy of users such as banks, many of the proprietary authentication techniques are applied.

2.2 Knowledge-Based Personal Identification

There is a digital one-pass service in the knowledge-based self-certification service that is utilized in the Korea. The digital one pass service is a service that performs personal identification by knowledge base in major public institutions. This service provides a way to identify with the QR code and mobile certificate without Active-X installation at the user’s computer when using the authorized certificate. Digital Integrated ID is a personal identification service that enables personalized service usage on multiple websites through one authentication. In other words, it is a service that enables individual identification on-line through a single-user authentication method as well as single sign-on (SSO) of various websites with one ID/PW.

Major countries are adopting e-government services considering the accessibility of the public to the nation, and they are also applied in the financial sector considering convenience and safety. In the case of countries, the United States is called 'Connect.Gov' to strengthen the security interlocking between government and private services and apply the authentication method required by the people themselves. Canada has introduced 'SecureKey Concierge Program', which is being used by financial institutions. It also provides Sign-in-Prater function in addition to existing government homepage login method. Currently, it applies to more than 120 government services such as medical support services and welfare services. Australia has been using ‘myGov’ for services such as medical care, health, welfare, child support, tax refunds, disability support, and national patriotism. The UK has established 'Gov.UK Verify (Integrated Authentication System)' to provide online certification services. The authentication strength of the knowledge-based personal identification method is lower than that of other means, and additional authentication means are supplemented. Therefore, the authentication strength is being increased by using it as an ID/PW and an additional authentication means.

2.3 Feature-Based Personal Identification

FIDO is a representative method of authentication technology based on feature information. FIDO is an emerging technique for solving the problem of password authentication means. The frequency of use is rapidly increasing due to the development of mobile device technology with a biometric sensor. The biometric information, which is a characteristic of the user, can be authenticated through the mobile device possessed by the user. As a result, FIDO technology has become a means of privacy protection and safe and convenient authentication. FIDO 's authentication is a feature-based authentication method that performs local authentication of a device held by a user. The user's device performs remote authentication based on the FIDO standard on behalf of the authenticated user. At this time, the public key cipher is used, and the private key is stored only on the user's device and is not exposed to the outside. When the user authenticates the device, the cipher text is generated using the stored private key, and the cipher text is transmitted to the server. The server verifies the cipher text transmitted using the pre-stored public key and completes the user authentication. As a result, FIDO regarded the conformity assessment standard as an authentication means as an appropriate authentication means based on safety, convenience, determinism, and standard. Currently, the adoption of FIDO technology in Korea is centered mainly on the financial sector, but telecommunication companies and certification service companies also aim to develop FIDO based platforms. Based on FIDO server construction, we plan to provide various simple settlement services and authentication services to card companies, and the introduction of FIDO technology throughout the industry will continue. Currently, financial institutions are considering FIDO to introduce biometric authentication methods for non-face-to-face real name authentication. Therefore, it is used as an additional authentication method to replace OTP, security card, etc., and substitute FIDO authentication for the authorized certificate password. Application examples of FIDO authentication technology exist in financial institutions, telecommunication companies, manufacturers, card companies, and settlement and authentication.

2.4 Others Personal Identification

Recently, technologies using block chains have emerged as technologies that are used as personal identification methods. The block chain is a technology that records and manages transactions by distributing the authority for recording and managing transactions through a P2P network without a central organization. A block in which all transaction information generated during a specific time (10 minutes) is generated, and can be engaged in a transaction only when the validity of the transmitted block is confirmed after transmitting to all the members. The field of using the block chain can be applied not only to finance but also to various fields such as cryptography, international remittance, trade finance, damage insurance, sovereign voting, logistics industry, P2P power trading, online advertising transaction, personal authentication.

It has already been applied to financial institutions (banks, financial service companies), companies and educational institutions. In recent years, Kakao bank in Korea has introduced 'Kakao Pay Certificate' which replaces the official certificate in the simple payment authentication process. This certificate, which can be used through the KakaoTalk app, has been evaluated as having excellent security by adopting the same public key-based (PKI) digital signature technology and block chain. IBM

Canada and SecureKey technologies announced they are developing a new consumer digital authentication network based on IBM blockchain. Canada DIACC and Command Control and Interoperability Center for Advanced Data Analytics (CCICADA) are also investing in the commercialization of a new block-chain-based approach. The IBM blockchain service allows the user to control the authentication information shared by the user himself or herself and provides new services by confirming the identity of the customer promptly and efficiently.

2.5 Combined Personal Identification

The combined personal identification method is to apply ID/PW and additional authentication. In the United States and Japan, ID/PW is used as the basic authentication method, and additional questions, OTP, etc. are also used. When transferring from financial services, the United States does not perform basic authentication, but Japan does basic authentication with OTP, security card, and transfer password.

In US financial institutions, all services are available with login ID/PW for identity verification, and PC authentication is performed to enhance login security [12-14]. Generally, if the user confirms the pre-set image or if the IP address of the connected PC is different, it will ask for further inquiry or authentication. Here, for additional personal identification, optional questions, e-mail security codes, security software installation and so on. In this way, ID/PW and additional authentication are used as the main authentication method of pintech payment method. It uses a 2-channel authentication method that combines ID/PW + pre-authenticated public certificates and SMS that have been set in advance. At present, two or more fingerprints are applied through PayPal, Ali Pay, Google Wallet, Amazon Payments, etc. through fingerprint authentication pads.

Table 3: Types of authentication methods

Methods		Means of Auth.	Contents
Ownership	SW Token	Security card	Authorized certificate and additional authentication means of ID / PW
		OTP	One-time PW generation and authentication method
		mOTP	One-time PW generation and authentication method in mobile phone
		Certified certificate	Electronic identification that adds public key owner information
		USIM	Universal Subscriber Identity Module
		QR Code	Scan the QR code to create a secure channel to complete identity verification and provide electronic signatures
		PIN	Method to prove yourself by entering numbers instead of signatures
		e-ID	A smart card that stores personal information and biometric information in a contactless IC chip
	HW Token	eSE(embedded SE)	Storing authentication information in the mobile SE zone
		HSM	Encryption hardware security module developed to securely manage encryption keys
Knowledge	PW	ID/PW	Authentication using ID and PW stored in the server
		I-PIN	Personal identification number that can be used in place of the resident registration number
		Financial	Account number issued through face-to-face verification

		account number	
		Time pass	Passwords change with time
Features	Bio-based	Fingerprints, veins, iris, ear / lips	Save some body information and compare and authenticate
	Behavior based	Voice, typing habits, sign	Authentication using user's habits and actions
Others	Graphic authentication, etc.		Verify through user-specified image

3. CONCLUSIONS

Until recently, a variety of authentication technologies have appeared online, and technologies have been developed as a way to enhance security while maintaining convenience to users as much as possible. Typically, the hybrid authentication technology using biometric information is the mainstream for online identity verification both domestically and abroad. However, in order to utilize such a technology, a mobile device equipped with a sensor capable of biometric information recognition is indispensable. If only online users can receive services with specific media, they will have a big impact on online service expansion. As a result, it is necessary to present a solution that does not depend on a particular medium for personal identification. Also, it is required to present the authentication technology that does not have the alienated class in the online service market. In this paper, we propose a combination of traditional knowledge-based identity authentication technology and owner-based identity authentication technology. For example, ID/PW and picture pattern, ID/PW and address authentication, ID/PW and string input. Of course, the knowledge-based identity authentication technology has little security limitations. However, it is necessary for the user to have appropriate protection responsibilities for his / her authentication method if he or she can selectively determine the authentication means himself and present the composite authentication to utilize it. It would be a reasonable idea to provide online services to the online service providers based on the authentication means themselves, rather than forcing the online service users to comply with their identity verification obligations. As a result, online self-certification will enable users to securely use online services by following their own obligation to protect their authentication means and making them live. Recently, authentication technology based on biometrics has emerged widely, so it is possible to utilize mobile phone in various ways rather than using direct biometric information. For example, the user authentication can be performed by the shaking of the mobile device, key button stroke locker, specific pattern input, voice recognition, etc. These methods should be done with compound authentication rather than single authentication. As a result of analyzing the application status and trend of the authentication technology, it is analyzed that most online businesses require the authentication service using the latest technology. Although the latest authentication technology emphasizes more safety, users of online services are more inconvenienced by the authentication of the users, and they are hurting the activation of online services due to excessive collection of personal information. Therefore, it is necessary to require the authentication of the user for the purpose of confirming the identity of the user in providing the online service. If the online service requires authentication, it is necessary to require authentication by differentiating it according to the risk through risk analysis such as the scale of the online service, the legal requirements, and the risk of the online service. If the risk of online service is low, simple self-certification is required, and vice versa. By applying this differentiated identity authentication, an environment will be created for online service users and business operators to live together by eliminating the rejection of the use of new authentication means and reducing the need for excessive authentication. So, how to analyze the risk of the service in online service delivery is an important issue. Measuring the risk of online service can be divided into law violation, life risk, financial loss, reputation inhibition, and use inconvenience. It is necessary to divide each risk measurement into several grades according to the importance of online service and to classify them according to the characteristics of the online businesses as the respective measurement standards. For example, in the case of a banking system, the account inquiry service simply performs ID/PW and knowledge-based authentication, and in the case of bank transfer, compound authentication is additionally applied according to the amount transferred. As such, it is necessary for online providers to apply various compound authentication methods to determine their own risks and reduce their risks.

ACKNOWLEDGEMENT

This work was supported by the Ministry of Education, Science and Technology (NRF-2016R1D1A1B03931986) and the Korea Internet & Security Agency (KISA2019-0114).

REFERENCES

1. M. Kathuria. **Design of a Vein Based Personal Identification System**, *Int. Conf. on Advances in Recent Technologies in Communication and Computing*, pp. 284-286, 2010.

   https://doi.org/10.1109/ARTCom.2010.104

2. E. M. Callister, T. Grance, K. Scarfon. **Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)**, *NIST Special Publication* 800-122, 2010.

3. R. Rana; R. N. Zaeem; K. S. Barber. **US-Centric vs. International Personally Identifiable Information: A Comparison Using the UT CID Identity Ecosystem**, *Int. Carnahan Conf. on Security Technology*, pp.1-5, 2018.

   http://dx.doi.org/10.1109/CCST.2018.8585479

4. R. Weingärtner; C. M. Westphall. **A Design Towards Personally Identifiable Information Control and Awareness in OpenID Connect Identity Providers**, *IEEE Int. Conf. on Computer and Information Technology*, pp. 37-46, 2017.

   https://doi.org/10.1109/CIT.2017.30

5. D. H. Bae, C. J. Kim. **A Secure SMS Self-Authentication Method in Mobile Networks**, *Internet and Information Security*, Vol. 1, No. 2, pp. 24-41, 2010.

6. Y. J. Shin, et al,. **The Research for Alternatives of the Resident Registration Numbers and Improvement of Authentication Process**, *KISA Report*, KISA-WP-2015-0028, 2016.

7. H. M. Sun, Y. H. Chen, and Y. H. Lin. **oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks**, *IEEE Trans. on Information Forensics and Security*, Vol. 7, No. 2, pp. 651-663, 2012.

   https://doi.org/10.1109/TIFS.2011.2169958

8. J. B. Kim. **A Study on Digital Identity Guidelines of NIST**, *Proceedings of Korea Information Processing Society*, pp.160-163, 2019.

9. J. S. Choi, S, J, Lee, J. B. Kim. **A Study on improvement of the reliability of personal identification service based on the replacement methods of resident registration number by differentiated assurance levels**, *Proceedings of KICS*, pp. 858-859, 2019

10. J. S. Choi, J. B. Kim. **Study of enhancing safety of personal authorization methods**, *Proceedings of IEEK.*, Vol. 1, pp. 298-301, 2015.

11. J. S. Choi, J. B. Kim. **A Study of improving user authentication procedures for enhanced safety**

of personal authorization methods, *Proceedings of KIPS*, Vol. 22, No.2, pp. 668-671, 2015.

12. Prakash, G., Darbandi, M., Gafar, N., Jabarullah, N.H., & Jalali, M.R. (2019) A New Design of 2-Bit Universal Shift Register Using Rotated Majority Gate Based on Quantum-Dot Cellular Automata Technology, International Journal of Theoretical Physics, https://doi.org/10.1007/s10773-019-04181-w.

13. Akhmetova, S.O., Suleimenova, M.S., Rebezov, M.B. 2019. Mechanism of an improvement of business processes management system for food production: case of meat products enterprise. Entrepreneurship and Sustainability Issues, 7(2), 1015-1035. http://doi.org/10.9770/jesi.2019.7.2(16)

14. Bublienė, R.; Vinogradova, I.; Tvaronavičienė, M.; Monni, S. 2019. Legal form determination for the development of clusters‘ activities, Insights into Regional Development 1(3): 244-258. https://doi.org/10.9770/ird.2019.1.3(5)