International Journal of Internet, Broadcasting and Communication Vol.15 No.4 1-8 (2023)
http://dx.doi.org/10.7236/IJIBC.2023.15.4.1

IJIBC 23-4-1

Improvement of Digital Identify Proofing Service through Trend Analysis of Online Personal Identification

JongBae Kim

Professor, Depart of Software Engineering, Sejong Cyber University
jb.kim@sjcu.ac.kr

Abstract

This paper analyzes the trends of identification proofing services(PIPSs) to identify and authenticate users online and proposes a method to improve PIPS based on alternative means of resident registration numbers in Korea. Digital identity proofing services play an important role in modern society, but there are some problems. Since they handle sensitive personal information, there is a risk of information leakage, hacking, or inappropriate access. Additionally, online service providers may incur additional costs by applying different PIPSs, which results in online service users bearing the costs. In particular, in these days of globalization, different PIPSs are being used in various countries, which can cause difficulties in international activities due to lack of global consistency. Overseas online PIPSs include expansion of biometric authentication, increase in mobile identity proofing, and distributed identity proofing using blockchain. This paper analyzes the trend of PIPSs that prove themselves when identifying users of online services in non-face-to-face overseas situations, and proposes improvements by comparing them with alternative means of Korean resident registration numbers. Through the proposed method, it will be possible to strengthen the safety of Korea's PIPS and expand the provision of more reliable identification services.

Keywords: *Personal identity proofing service, Online service, Personalization service, User authentication and identification method, Non-face-to-face commerce*

1. Introduction

In most countries, there are few laws requiring online service users to verify their personal identities, and online services are provided online or based on user-provided personal information without confirming the user's identity when paying for goods. Digital identity proofing services play an important role in modern society, but some problems exist. The PIPS provides sensitive personal information to the other party, so security and personal information protection are key. Eventually, with the operation of a centralized processing system, there is a risk of data leakage, hacking, or improper access. Costs arising from PIPSs are also emerging as a problem. In fact, online service providers incur costs when applying PIPS services, which ultimately becomes a burden on online service users. This is a structure in which excessive personal identity proofing

Manuscript Received: August. 2, 2023 / Revised: August. 10, 2023/ Accepted: August. 17, 2023
Corresponding Author: jb.kim@sjcu.ac.kr
Tel: +82-2-2204-8627, Fax: +82-2-2204-8111
Professor, Department of Software Engineering, Sejong Cyber University, Korea

requirements are passed on to online service users. Recently, overseas product purchases and payments have become global across countries as there are no borders online. As different PIPSs are used across various overseas online services, there may be a lack of global consistency, which can cause difficulties in international activities. To solve these problems, it is necessary to improve security, regulation, technology, improve accessibility, protect personal information, and strengthen global standards for PIPSs.

In particular, in the case of e-commerce such as online payment, if the payment method is clear and the delivery address is valid, the payer is not required to additionally verify the identity [1-3]. There may be various reasons, but unlike Korea, there is no unique identification information to identify online service users or there is little need for identification. In other words, there is no need to verify the buyer's identity, only payment or delivery is confirmed, which is a business that provides online services based only on the information provided by the buyer. In addition, identification is required when purchasing items such as alcohol or guns online. In most countries, personal identity verification is performed only with the information entered by online service users [4-7]. In Korea, alternative means are created based on resident registration numbers, and personal identification certification services are provided online using this alternative means. These alternatives include mobile phone numbers, credit card numbers, I-PINs, and public certificates [8]. In Korea, the convenience of user selection has increased due to the emergence of various personal identification methods, but there is a problem that personal information of online service users is provided to online service providers due to excessive identification requirements when using online services. In this paper, we would like to analyze the online personal identification method applied by country and suggest improvement measures to strengthen the safety and reliability of Korea's personal identification service.

2. Analysis of online personal identity proofing methods by country

2.1 USA

The USA has introduced social security numbers for various social security guarantees provided by the state, and in the financial sector, social security numbers and additional identification information (driver's license number, passport number, and other various identification numbers) are collected and used as a means of identification. Social security numbers are used for tax information, credit information, school records, and medical records, and are managed so that they are not disclosed. In addition, sites in the field of e-commerce or entertainment provide services to sign up for membership using basic information such as name, address, and payment information (in the case of payment). Since 2009, the National Institute of Standards and Technology (NIST) has planned and developed an authentication system that identifies itself online and has presented a standard guide for use in the public and private sectors [9]. NIST defines Digital Identity Guides and has been revised to SP 800-63-3 versions through government comments and approval processes through collecting opinions from various organizations, and is currently disclosing them that can be used for identification in the public and private sectors. As shown in Figure 1, NIST's digital identity model, the procedure for issuing a user's identity certificate is 1) Applicants apply to the Credential Service Provider (CSP) through the registration process, 2) CSP identity certifies the applicant, and if the certification is successful, the applicant becomes a subscriber. 3) The authenticator and its credentials are established between the CSP and the subscriber. And 4) CSPs maintain credentials, credential status, and registration data collected over the lifetime of the credentials, and subscribers maintain their authenticators.

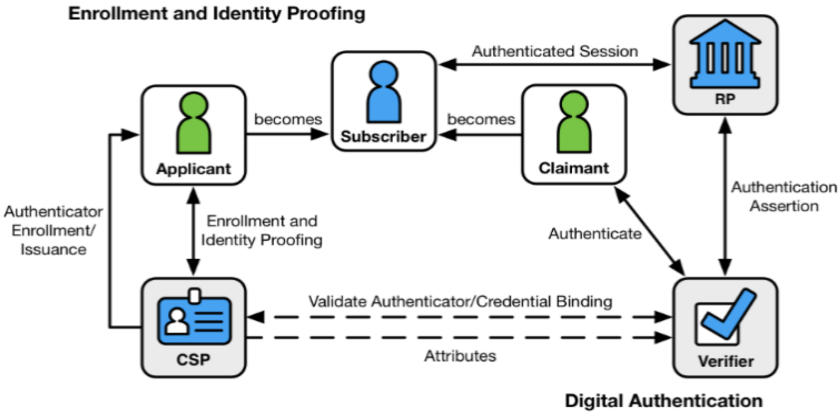


Figure 1. Digital Identity Model [10]

When an online user presents his or her identity certificate on an online service after receiving an identity certificate, operators are required to differentiate the level of security intensity of identification required according to the type of service provided. It is differentiated from Korea's personal identity proofing service. While Korea's identity proofing service consists of a single guarantee level, which is the highest level, the U.S. is differentiating the guarantee receipt in three stages, and attempts to minimize the provision of personal information by presenting identification means that meet the guarantee level when using the service. The identification process may be defined differently according to the guarantee level (LOA) of the identity verification presented by the user.

2.2 EU

The EU recognizes self-authentication through electronic signatures, which aims to secure user convenience by ensuring diversity in authentication systems and procedures. In addition, according to the EU cross-border elDAS regulations[11], various electronic tasks handled between countries in the region, such as foreign university registration and electronic health records, can be safely performed. Companies can reduce time and cost by simplifying administrative procedures, enhance convenience and flexibility when using government services, and use the country's electronic ID to address concerns about security and privacy exposure. As shown in Figure 2, residents in the EU region register their identities through the country's certification authority, and then, when presenting the user's electronic ID in other countries in the EU domain, the EU country shares systematic authentication systems and information between countries so that users can freely verify themselves within the EU. The eIDAS regulations were established to target the appropriate level of security of electronic identification means and trust services, while also correcting the appropriate functioning of the market in Europe. By September 2023, all EU Member States should make EUDI wallets (digital identity wallets[12]) available to all citizens, residents and businesses in the EU and available for all proofs, including sensitive personal data, as well as identification documents. In other words, from the pilot stage in 2023, all member states are set to provide EUDI wallets across the EU by 2024. eIDAS 2.0 has the origin of e-Wallet. Currently, the concept of e-Wallet has expanded from crypto key management to digital identity. eIDAS 2.0 is part of the revision of the Electronic Identification, Authentication and Trust Services Regulations (eIDAS), and the European Union Digital ID (EUDI Wallet) is a project of the European Commission. In the end, it aims to establish a single digital identification system in Europe.

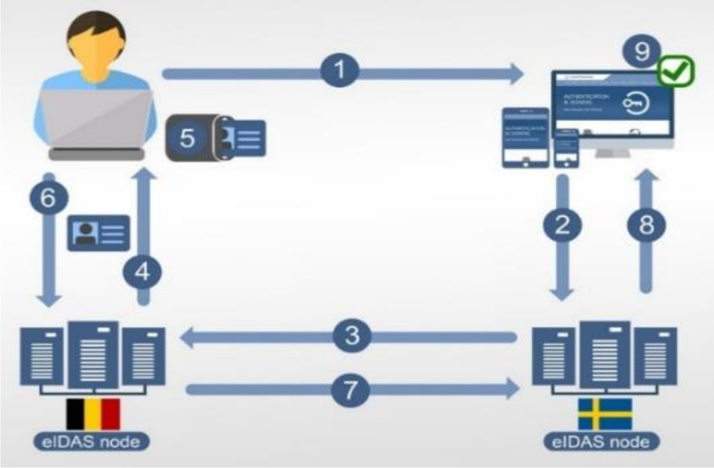


Figure 2. Cross-border customer on-boarding process. [13]

2.3 UK

In the UK, national insurance numbers and national health service numbers are used together as limited means of personal identification. The National Insurance Number is an insurance system for diseases and unemployment and is currently expanding the number given to the public to taxes, retirement pensions, and other social security. The number is issued just before the age of 16, and it also issues a national insurance number to legal foreigners living in the UK. In the UK, government agencies providing online services can connect with the GOV.UK (Government Portal [14]) through government digital service evaluation, GOV.UK Verify is an identity guarantee system developed by the UK Government Digital Services. This system is a service that provides one reliable login to check all digital services of the UK government. As shown in Figure 3, the user provides his or her identity information to a nationally designated and reliable identification agency to be certified as his or her identity and issued a means of identification.

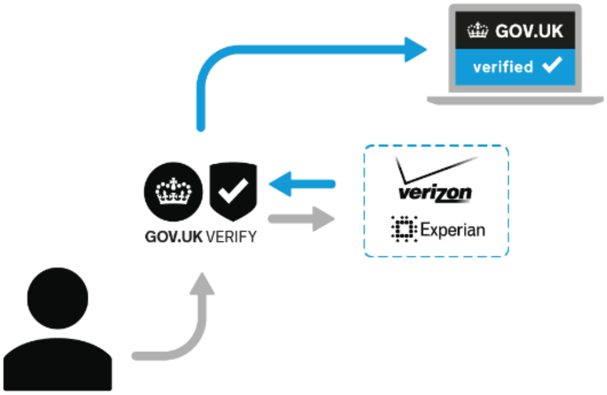


Figure 3. GOV.UK Model [15]

After that, GOV.UK can receive all online services registered on the site through the verification and certification process of the UK site. In this way, if identity verification is performed through the application of SSO technology in the government portal, it does not require a cumbersome identity verification procedure when using other government services. With the British government's institutionalization of online identification, the private sector does not establish an individual identification service, but rather GOV. It is included in the UK to build an ecosystem so that users can conveniently receive online services.

2.4 Japan

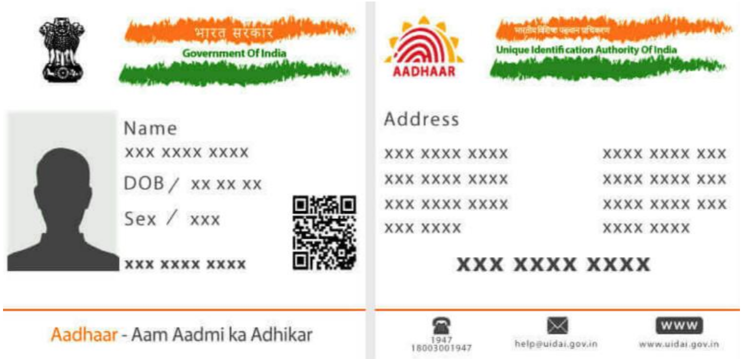
In 1999, Japan granted 11 digits of resident registration numbers to all citizens for administrative work. Subsequently, in 2013, resident registration numbers were also given to foreigners who lived for a certain period of time. There is no face photo attached to the resident registration card, and you can choose whether to attach a photo according to the user's application. However, currently, the issuance rate of resident registration cards is low, so driver's licenses are mainly used for identification. For this reason, the public sector has mandated the use of My Number in the areas of social security, taxation, and disaster response administration since 2016. One My Number is given to citizens or foreigners who have been granted a resident registration card corresponding to the resident registration number on the resident registration card [16]. My number will not be changed for the rest of my life except when it is leaked and may be misused like a Korean resident number. Therefore, use and provision other than those provided to administrative agencies for administrative processing such as social security, taxation, and disaster response are prohibited by law. The card with the My Number recorded can be issued according to the user's request, and the user's face photo is stamped on the front, the My Number is stamped on the back, and identification can be made through number verification and face comparison with one card, and can also be used as an official ID.

2.5 Estonia

Estonia uses digital electronic identification cards to securely identify users online using E-ID or smart-ID or smart-ID. In 2002, the country ID card was introduced, and it is applied to various online services such as online banking and digital signatures. After all, Estonia's national electronic ID plays the same role as Korea's resident registration card. All secure electronic services can be accessed with this country ID, and public key encryption is also provided in the digital environment. However, while the resident registration card is permanent in Korea, the validity period of Estonia's national electronic ID is set in five years, requiring periodic information updates.

2.6 India

Aadhaar is a 12-digit random number issued to residents of India by the Unique Identification Authority of India (UIDAI) after meeting the identification procedures set by the Indian government. Aadhaar stipulates that all individuals living in India, regardless of age or gender, must voluntarily register to receive an Aadhaar number. Those who wish to register must provide minimum demographic and biometric information during the registration process and can register free of charge. It is used as the only means of identifying individuals of the people through the process of checking demographic information and removing biometric authentication. Therefore, the Aadhaar information is used to identify users online and to authenticate using biometric information. As shown in Figure 4, the Aadhaar card includes not only name, address, date of birth, and registration number(EID), but also ten-finger fingerprint information, iris scan information of both eyes, and face photos. Non-resident Indians who have lived in the population for 182 days can also apply, and can be issued in the form of an online app and used online for identification purposes.



भारत सरकार
Government Of India

Name
xxx xxxx xxxx
DOB / xx xx xx
Sex / xxx
xxx xxxx xxxx

Aadhaar - Aam Aadmi ka Adhikar

भारतीय विशिष्ट पहचान प्राधिकरण
Unique Identification Authority Of India
AADHAAR

Address
xxx xxxx xxxx xxxx xxxx xxx
xxx xxxx xxxx xxxx xxxx xxx
xxx xxxx xxxx xxxx xxxx xxx
xxx xxxx xxxx xxxx

XXX XXXX XXXX

1947
18003001947
help@uidai.gov.in
www
www.uidai.gov.in

Figure 4. Example of Aadhaar card [17]

3. Comparative Analysis of Personal Identity Proofing Methods in Online

Currently, there are various technical methods to identify and authenticate users when providing online services. In particular, mobile authentication using smartphones is the mainstream, which is due to the possession and possession of the device, and the issuance of identification when registering for mobile. However, not all countries check their identities when signing up for mobile phones, but most of them check their identities for crime prevention or electronic notification purposes. Of course, some mobile phone subscriptions that cannot be identified are proposed simply for phone calls. In this way, for online identification, authentication services are systematized in a centralized way of central information or provided by online service providers autonomously applying them after simply checking the payment or delivery address. In recent years, due to the spread of COVID-19 around the world, it is imperative to track the movement path of infected people, and user identification is considered most important for vaccine injection prescriptions. Therefore, countries that have not identified users are also preparing user identification measures and there is a movement to define them by law. Of course, the issue of personal privacy infringement arises by forcing the granting of individual identification information by law, and to solve this problem, in order to receive public services, it is required to subscribe to an identity certificate in which individual identification information is recorded. In some countries, users are identified and authenticated on online services by issuing digital IDs, which are mobile identification cards, rather than physical identification cards. This trend has led to the development of IT technology, which uses technologies such as blockchain, biometric, and electronic certificates to ensure safety [18]. However, unlike Korea's identification service, the overseas identification service aims to differentiate the level of identification authentication guarantees. In the case of the United States, the most basic identity verification information, additional address or date of birth information, and SSN information at the last enhanced security level are required to verify identity according to the level of 3 identity authentication.

In Korea, there are identification methods using mobile phones, I-Pin, credit cards, and public certificates, and the level of individual guarantees online is the same no matter what means of identification is used. In other words, there is no differentiation according to the means of identification, and the level of guarantee is the same depending on the means of authentication such as fingerprint, password, and possession within the means. In addition, there are no cases abroad in which personal information provided by users when issuing identification means is provided to online service providers in the form of collective consent, whether central or private identification is controlled. In Korea alone, excessive personal information is provided to online service providers when using an identity verification service based on alternative means of resident registration numbers, and online service providers delete the received personal information and record the necessary information in the storage device. As a result, unnecessary personal information is transmitted on network communication, and personal information of users of the identification service is collected and stored in situations where they are not recognized. Therefore, the following safety enhancement measures are required in Korea's identification service. First, it is necessary to prepare a differentiated identification plan-to issue a differentiated identification means according to the verification method presented by the user. For example, if only the name, name, and address are presented, confirm that the information is correct, and if the date of birth is presented, all online services can be used until adult authentication, and finally if the resident registration number is presented. The second is to provide at least converted personal information-only personal information that the user selectively agreed to when using the identification service. This will enable the provision of minimal personal information. Third, the provision of centralized identification services-Currently, private businesses in Korea are engaged in commercial activities through identification services, and of course, there will be costs for maintaining and managing the information system to provide identification services. However, simply verifying who you are is handled by the state or a centralized system. In the case of Korea, the Ministry of Public Administration and Security, the National Tax Service, the National Health Insurance Corporation, and the National Police Agency hold most of the public's personal information. Fourth, the unification of how to use the identification service-In Korea, due to various identification means, users provide different devices and means, so online service businesses need to install and manage individual modules to require all identification means to online service users. Therefore, it will be possible to reduce the inconvenience of users and online service providers by unifying based on an integrated UI.

4. Conclusions

With the development of digital technology and the spread of online services around the world, safety and security issues in the online environment are emerging as important issues. As online fraud, personal information leakage, and cybercrime increase, identification of online service users is emerging as an important task This paper investigated and analyzed the means that require identity verification when using online services by country. Due to the recent spread of infectious diseases, the demand for non-face-to-face services in the online environment is rapidly expanding, which helps increase convenience and accessibility. However, as a result, security issues for important information such as user personal information and financial transactions are becoming more important. Therefore, identification of users is required to play a key role in maintaining the safety and trust of online services. Through this paper, we investigated and analyzed the current status and trends of means when requesting identity verification from users in online services by country. In addition, a plan to improve compared to Korea's means of identification was suggested. In the proposed plan, it was proposed to prepare a differentiated identification plan, provide minimized personal information, provide centralized identification services, and unify the methods of using identification services. Through the proposed plan, it will be possible to strengthen the safety and reliability of Korea's identification service.

Acknowledgement

This is an extended and revised version of a preliminary conference paper that was presented in ISAAC 2023 [19].

References

[1] D. Drusinsky, "Cryptographic–Biometric Self-Sovereign Personal Identities", Computer, Vol. 55, No. 6, pp.96-102, 2022. DOI: https://doi.org/10.1109/MC.2022.3164527

[2] M. Hansen, A. Schwartz and A. Cooper, "Privacy and Identity Management," IEEE Security & Privacy, Vol. 6, No. 2, pp.38-45, 2008. DOI: https://doi.org/10.1109/MSP.2008.41

[3] Fang Xuan, Ying Tao and Bin Huang, "The establishment and strategy of digital identity authentication system", *IEEE Symposium on Electrical & Electronics Engineering*, pp.175-177, 2012. DOI: https://doi.org/10.1109/EEESym.2012.6258617

[4] D. Augot, H. Chabanne, O. Clémot and W. George, "Transforming Face-to-Face Identity Proofing into Anonymous Digital Identity Using the Bitcoin Blockchain", *Annual Conference on Privacy, Security and Trust*, pp.25-2509, 2017. https://doi.org/10.1109/EEESym.2012.625861710.1109/PST.2017.00014

[5] J. B. Kim, “Sustainable Utilization of Personal Identification Services in Non-face-to-face Online Education Services in the Corona Era”, Review of International Geographical Education Online, Vol. 11, No. 08, pp.2040-2053, 2021. https://rigeo.org/menu-script/index.php/rigeo/article/view/2322

[6] J. B. Kim, “A Study on the Quantified Point System for Designation of Personal Identity Proofing Service Provider based on Resident Registration Number”, International Journal of Advanced Smart Convergence, Vol. 11, No. 4 pp.20-27, 2022. https://doi.org/10.7236/IJASC.2022.11.4.20

[7] J. B. Kim, “A Study on the Improvement of Personal Identity Proofing Service Using an Alternative Method for Resident Registration Number Based on Electronic Signature”, The Journal of the Convergence on Culture Technology, Vol. 7, No. 3, pp.453-462, 2021. https://doi.org/10.17703/JCCT.2021.7.3.453

[8] J. B. Kim, “A Study on Improvement method of designation criteria for Personal Proofing Service Based on Resident Registration Number”, Journal of the Korea Society of Digital Industry and Information Management, Vol. 16, No. 3, pp.13-23, 2020. https://doi.org/10.17662/ksdim.2020.16.3.013

[9] https://pages.nist.gov/800-63-3/

[10] Paul A. Grassi Michael E. Garcia James L. Fenton, “Digital Identity Guidelines”, NIST, 2017.

[11] eIDAS Regulation, https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation

[12] EIDAS AND KYC - FACTS AND IMPACT, https://www.cryptomathic.com/news-events/blog/eidas-and-kyc-facts-and-impact

[13] EU Digital Identity Wallet Pilot implementation, https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation

[14] https://www.gov.uk/

[15] Introducing GOV.UK Verify, https://www.wired-gov.net/wg/news.nsf/articles/Introducing+GOV.UK+Verify+24092014143356?open

[16] https://www.kojinbango-card.go.jp/en/

[17] Know Everything about Aadhaar Card, https://www.loanbaba.com/aadhaar/

[18] H. G. Yeom, D. Choi, K. Jung, “A Study on Big Data Based Non-Face-to-Face Identity Proofing Technology”, KIPS Transactions on Computer and Communication Systems, Vol. 6, No. 10, pp.421-428, 2017. https://doi.org/10.3745/KTCCS.2017.6.10.421

[19] J. B. Kim, "A Study on the Improvement of the Safety of Korea's Digital Identity Proofing Service through the Analysis of the Trends of Identification Means Online", The 11th International Symposium on Advanced and Applied Convergence, pp.66-72, 2023.