International Journal of Advanced Culture Technology Vol.10 No.4 547-554 (2022)
DOI https://doi.org/10.17703/IJACT.2022.10.4.547

IJACT 22-12-64

A Study on the Preparation of Standardized Operation Criteria for Enhancement of Safety and Convenience of Mobile Electronic Notice Service

[1]JongBae Kim

[1]*Professor, Dept. of Software Engineering, Sejong Cyber Univ., Korea*
kjblove@hotmail.com

Abstract

Due to the expansion of non-face-to-face services, the demand for user identification for mobile devices is increasing. Recently, mobile resident registration cards, mobile driver's licenses, etc. are installed in mobile phones and used for user identification and authentication services. In order to identify a user online, unique identification information of the online user is required. In particular, in order to provide information only to online users, it is necessary to accurately deliver information to a mobile device owned by the user. To make this service possible, it was realized with the advent of mobile electronic notice service. However, the identification of online service users and information on mobile devices owned or subscribed by the relevant users require safe management as personal information, and it is also necessary to increase the convenience of online service users. In this paper, we propose an operating standard for providing a mobile electronic notice service that sends electronic notice using a mobile device owned by the user. The mobile electronic notice service is a service that provides notices expressed in electronic information to the recipient's cell phone, mobile app, e-mail, etc. Therefore, as the use of mobile electronic notification service increases and the provision and use of connecting information to identify users increases, it is necessary to expand the mobile electronic notification service while safely protecting users' personal information.

Keywords: *Mobile electronic notice service, personal identity proofing service, connecting information, postal service*

1. INTRODUCTION

By sending and receiving electronic notices, it has the advantage of being able to easily read notices as well as reducing paper production and mailing costs [1,5,6]. For mobile e-notifications, it will be of utmost importance to identify the recipients with mobile devices. The mobile notification recipient identification issue is related to the privacy issue. In order to accurately deliver the mobile electronic notice to the recipient, clear user identification is required, and the user's genuine personal information is essential for clear user identification. However, it will be very difficult for the subject who sends the mobile electronic notification to perform a request to provide personal information to the target recipient online. Even if the recipient of the mobile electronic notification provides personal information, an additional verification process is required to confirm that the recipient is the actual person. As such, in the past, a simple paper-based notice delivery service was a common delivery method to deliver to the recipient through face-to-face confirmation by the postal

Manuscript received: November 26, 2022 / revised: December 4, 2022 / accepted: December 9, 2022
Corresponding Author: kjblove@hotmail.com
Tel: +82-2-2204-8627, Fax: +82-2-2204-8111
Professor, Dept. of Software Engineering, Sejong Cyber Univ., Korea

delivery service. The mail delivery service was a delivery service that could prove delivery, proof of recipient, and even check receipt. On the other hand, the electronic notice service is a service that delivers an electronic notice to the mobile device possessed by the recipient, and how to ensure the effectiveness of the certification is an important issue.

Recently, due to the rapid spread of IT devices, the smartphone penetration rate is more than about 67% of the world's population, and Counter pointer Research has announced that by 2022, it will be 1.357 billion units [7]. As the number of mobile phone subscribers through smartphones is increasing around the world, it can be expected that the paper-based notice delivery service will decrease and the mobile device-based electronic notice delivery service will be realized. However, the electronic notice sender needs to have the mobile device owned by the notice recipient, that is, mobile phone subscription information or online service subscription information. Ironically, in order to realize this, it is necessary for the mobile electronic notification sender to collect the mobile phone number or online service subscription information after confirming the recipient of the notification. Therefore, if information for clearly identifying the effective mobile electronic notice recipient can be provided, it will be possible to accurately deliver the mobile electronic notice to the recipient when sending the mobile electronic notice. The problem of identifying users online is not only a mobile electronic notification service, but also a problem that has emerged first in the e-commerce of online services. In a non-face-to-face transaction such as online, clearly identifying the identity of the other party, paying for the purchased product, and delivering the purchased product is the same environment as the user identification of the mobile electronic notification service. Therefore, by utilizing the user identification method in online e-commerce, it will be possible to identify users in the mobile electronic notification service as well. As shown in Figure 1, according to the Korea Internet & Security Agency's survey on electronic documents [2], the size of the Korean electronic document industry is increasing every year.

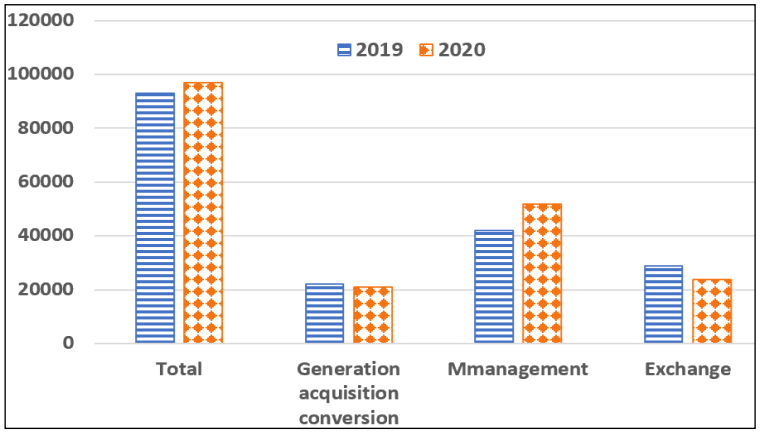

Figure 1. Status of the electronic document industry

The most important part of sending a notice is clearly identifying the recipient [3, 4]. Of course, it will not be necessary to clearly identify the recipient in the delivery of all electronic documents. For example, in the case of a simple guide, it is not necessary to identify the recipient as information provided to an unspecified number of people. However, if the electronic notice needs to take effect legally or to protect the rights of the recipient, it is necessary to identify the recipient.

In Korea, simple notices are sent based on information presented by users who have signed up for online services using an app-based push message method. The mobile electronic notification service implemented in Korea is not just information, but a service that can take effect legally. In other words, when the sender requests

the sending of a notice, the person who relays the sending takes charge of the sending of the notice. At this time, the notification sending relay is accompanied by a process of clearly identifying the recipient. This recipient identification process uses the identity verification service provided in accordance with Korean domestic law.

The personal identity proofing service is a service that verifies who you are by using your resident registration number, which is a unique identification number given to citizens by the government. In this case, the resident registration number is a 13-digit value, and personal information infringement may occur if it is exposed indiscriminately [8-10]. Therefore, in Korea, a personal identity proofing agency system that creates and issues a means to replace the resident registration number is in operation. The designated identity proofing agency identifies the applicant using various methods to identify the applicant for issuing a resident registration number alternative. Methods of identifying the applicant for issuance include SMS text authentication method for mobile phone number possessed by the person, password authentication method for credit card, signature authentication method for digital signature, biometric information-based authentication method, and the like. In addition to identification of applicants for issuance based on knowledge, possession, and biometrics, the national birth database is searched and verified. By using the birth database operated by the government, it is possible to check whether there are dead, missing, or renunciation of nationality. In addition, when a child under the age of 14 requests the issuance of an alternative means, it is checked whether the legal representative is the actual legal representative during the consent process of the legal representative. In online services, online service providers require identification through an alternative means of resident registration number to identify online service users. This is because, as described above, online service providers are an accurate and reliable user identification method because it is an online user identification method guaranteed by the government. Online service users will prove their identity by presenting an alternative means of resident registration number issued to them to the personal identity proofing agency. When an online service user is identified, the personal identity proofing agency provides user identification information to the online service provider. User identification information is information that can be uniquely identified from other online service users.

Therefore, in the mobile electronic notification service, it is necessary to acquire information that can uniquely identify users online. The most convenient way is to provide a smooth service if the mobile electronic notification service-related companies have the recipient's resident registration number. However, Korea's Information and Communications Network Act. of 2012 prohibits the collection of users' resident registration numbers online. For this reason, it is necessary to receive information that can be used to identify users online, which is a mobile electronic notification service-related company, from the personal identity proofing agency. However, the Personal Information Protection Act. of Korea stipulates that personal information can be provided to a third party only with the consent of the information subject. In the end, it goes back to the first problem again. In order to obtain the recipient's online identification information, operators related to the mobile electronic notification service must either request the personal identity proofing service or obtain consent for the collection of identification information. However, in a situation where user identification is impossible, it is not possible to find the recipient and request consent or identification.

To solve this problem, mobile electronic notification service providers convert the resident registration number held by the sending requesting organization into connecting information that can be used to identify users online. Connecting information is a one-way encrypted value that combines a resident registration number and secret information created with an 88-byte length. This information can uniquely identify the user online, so it is called an online resident registration number. Therefore, in order to strengthen the stability of the mobile electronic notice service, it is necessary to prepare effective operating standards in the process of sending, providing, and processing electronic notices including connecting information [1, 4]. In this paper,

we propose operating standards from the point of view of the sending requesting agency and the sending processing agency for the provision, use, and processing of safe mobile electronic notification services.

2. MOBLIE ELECTRONIC NOTIFICATION SERVICE

As shown in Figure 2, the mobile electronic notice service is a service in which an electronic notice sending organization provides a notice by using the mobile device possessed by the recipient.

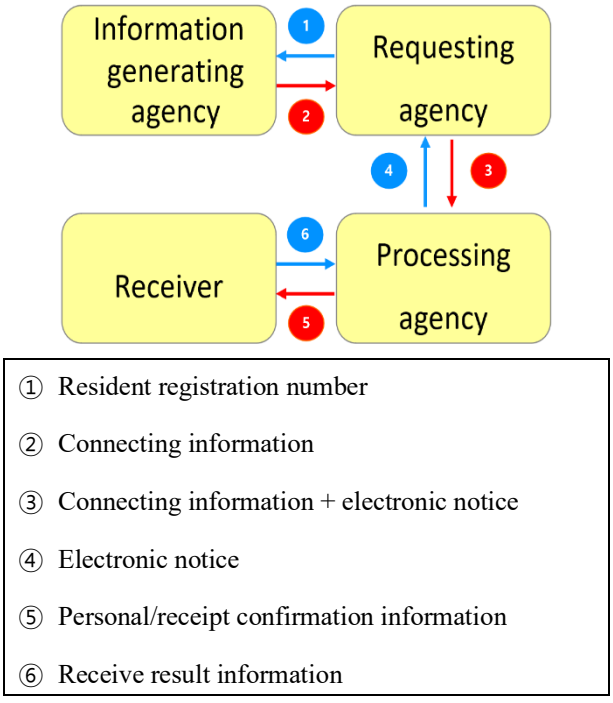

Figure 2. Overview of mobile electronic notification service processing

As shown in Figure 2, the mobile electronic notification service collects and stores users' connecting information and electronic notices at the sending processing agency and the sending requesting agency. In accordance with the Personal Information Protection Act of Korea, prior consent of the user is essential in order to collect and process the user's personal information [2]. However, for the mobile electronic notification service, it is impossible to consent to the processing of personal information to all subscribers in advance. In order to solve these legal regulations, the mobile electronic notification service is a service that focuses more on profits rather than damages to users, and by easing some of the legal regulations, allows users to use personal information without prior consent for personal information processing. In addition, in step ⑤, a system is being operated so that the recipient of the electronic notice must give consent after the fact. In the end, as shown in the figure, the sending requesting agency for the mobile electronic notification service receives the recipient's link information from the identity verification agency.

In this case, the sending requesting agency provides the resident registration number to the personal identity proofing agency without the consent of the recipient, and the personal identity proofing agency also provides the connecting information to the sending requesting agency without the recipient's consent. Thereafter, the recipient's connecting information is used to determine the online sending service the recipient has signed up for, and the mobile electronic notice is sent through the online sending service. When a user who has received a mobile electronic notice decides whether to read it, he/she agrees to the processing and use of his/her personal

information when reading, and then processes the notice so that he/she can read the notice. In the end, it can be said that it is a process of receiving the consent of the recipient's personal information after the fact. In this process, the recipient's connecting information is stored and utilized in various places, and there is no management and operation standard for such connecting information.

2.1 Information generating agency

An information generating agency refers to an organization that provides a personal identity proofing service based on alternative means of resident registration number. The personal identity proofing agency is an organization that converts the resident registration number of online service users into connecting information, and this connecting information can be used as information to uniquely identify users online. In Korea, only the personal identity proofing agency has the authority to create such connecting information. To that extent, the personal identity proofing agency goes through the user identification and authentication process to make sure that the user requested the conversion when creating the connecting information. In addition, a verification process is required to identify whether the information conversion requester is a legitimate user or institution, and an encryption and encryption key exchange process between transmission sections is also required for information reception and delivery.

2.2 Requesting agency

The requesting agency refers to a requesting institution for sending mobile electronic notices for the mobile electronic notice service. For example, a government agency requests a mobile e-notice sending agency to send an electronic notice based on personal information held by the government agency for tax notification, penalty notice, and information guidance to the public. Since user identification information held by government agencies and user subscription information held by mobile e-notice operators are different from each other, information to identify them identically is required. Accordingly, the sending requesting agency provides the resident registration number to the personal identity proofing agency to convert the connecting information. Then, the converted connection information and electronic notice are delivered to the mobile electronic notice service provider, and the mobile electronic notice is sent to the corresponding user.

2.3 Receiver

A mobile electronic notice receiver refers to a person who receives an electronic notice through a mobile device owned by him/herself. At this time, the recipient must be able to confirm that the corresponding electronic notice has been accurately received by him or her. In addition, the sender also requires a process of verifying whether the sender has been sent by a reliable person. Additionally, if it is necessary to be able to read electronic notices arriving on one's mobile device at any time, a function must be prepared to prevent illegal exposure by others.

2.4 Processing agency

A mobile e-notice sender refers to a person who accurately transmits an e-notice based on the user identification information provided to the requesting agency. For user identification, the same user is identified by comparing with online service subscriber information using the received connection information. Then, an electronic notice is sent using an online service means to which the corresponding identifier has subscribed,

for example, using KakaoTalk, Naver Messenger, and mobile phone SMS text. At this time, the original electronic notice is not sent, but a link that allows you to read the electronic notice is transmitted. When transmitting a link, an identification mark is included to identify the sender and prevent forgery. In addition, when the recipient reads the electronic notice, a function is provided to prevent unauthorized reading by others after going through the identity verification and authentication process.

3. STANDATS FOR OPERATING MOBILE ELECTRONIC NOTIFICATION SERVICE

For the mobile electronic notification service, it is necessary to protect the recipient's personal information and provide a safe mobile notification service by the notification sending requesting agency and the sending processing agency. Through this paper, it is possible to prepare a safe service provision plan by presenting the operating standards for the mobile electronic notification service. Table 1 shows the composition of the Mobile Electronic Notification Service Operation Standards Committee. First, prepare all necessary matters for the operation of the mobile electronic notification service. Second, prepare matters related to the operation of information processing institutions for information protection. And third, prepare matters for user personal information management.

Table 1. Standard for mobile electronic notification service

Category	Sub-category
1. Service operation	1.1 Composition of a dedicated organization 1.2 Electronic document sending/receiving function 1.3 Management of Certified Electronic Address Resources 1.4 Electronic notice document distribution information resource management 1.5 Issuance of distribution certificate 1.6 Standard Time Correction 1.7 Recipient Identity Verification 1.8 Creation and verification of electronic document distribution information 1.9 Supervision
2. Information protection management system operation	2.1 Security system installation and operation 2.2 Access Control 2.3 Access record management 2.4 Patch Management 2.5 Physical and Logical Network Separation 2.6 Physical Access Control 2.7 Establishment of disaster and disaster response procedures 2.8 Permission Management 2.9 Account Management 2.10 Backup and Recovery 2.11 Certification Management 2.12 Encryption Enforcement 2.13 Anti-Malware 2.14 Establishment of incident response procedures 2.15 Prevention of Infringement Accidents 2.16 Incident response training and improvement 2.17 Infringement Incident Response 2.18 Information security education program establishment
3. Personal information protection management system operation	3.1 Consent to use of personal information 3.2 Collection of personal information 3.3 Destruction of personal information 3.4 Entrustment of work 3.5 Compliance with the Personal Information Protection Act

As shown in Table 1, the first operating criteria of a mobile electronic notification service organization can be divided into organization composition, resource management, recipient identification, and management supervision. For efficient management of processed personal information, an organization dedicated to service is formed, and each function in the process of sending and receiving electronic documents is defined. In the future, it defines the operational standards for the management of official addresses for distribution certification of electronic documents, management of distribution information, and issuance of distribution certificates. In fact, the issuance of a distribution certificate is performed by a Korean government agency as proof of sending and receiving electronic documents.

The second operating standard is the information security management system. It is an operating standard that requires safe management of personal information as it provides a mobile electronic notification service using connecting information. A security system must be installed and operated for the linked system that processes mobile electronic notices, and access control is applied to stored personal information and records are managed at the time of access. Apply the latest security patches to operating systems related to mobile electronic notification service, separate physical and logical networks, establish disaster response procedures, and conduct regular response training. User rights should be minimized on operating systems, and accounts should be reviewed periodically. After that, the operating standards include the application of encryption and malicious software control to the storage and transmission of personal information, the implementation of periodic personal information protection education, and the management and destruction of stored personal information.

The third operating standard is personal information protection management. In order to effectively manage personal information, when collecting personal information, we prepare procedures for consent from the information subject, collection and destruction of personal information, and when entrusting the mobile electronic notification service, prepare personal information protection standards and review the regular compliance with the Personal Information Protection Act to carry out

4. ACKNOWLEDGEMENT CONCOLISIONS

By providing electronic notices through mobile devices, unnecessary management costs were reduced for the sender, receiver, and dispatcher, and it became possible to deliver notices quickly and accurately. However, for the mobile electronic notification service, it is necessary for all service-related parties to process the recipient's connecting information. Even if the recipient does not receive the mobile electronic notification, connecting information is shared. This causes a problem in the use of the mobile electronic notification service without prior consent for the provision and use of personal information of the information subject. Currently, mobile electronic notification service-related providers are providing mobile electronic notices with the consent of the information subjects, but safe management and operation standards for previously received connecting information are required. In this paper, it is possible to realize safe mobile electronic notification service by presenting service operation standards, information protection management system operation standards, and personal information protection management standards in the mobile electronic notification service using linked information. By preparing the operating standards for the mobile electronic notification service prepared in this study, it is possible to protect recipients' personal information, provide efficient electronic notification service, and expand the provision of safe services.

ACKNOWLEDGEMENT

An extended version of this paper has been published at the ISAAC 2022 conference[11], and this work was supported the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (NRF-2020R1F1A106890011)

REFERENCES

[1] J. B. Kim, “A Study on Establishment of Connecting Information Conversion Criteria for Mobile Electronic Notification Service of Private Institutions,” The Journal of Convergence on Culture Technology, Vol 7, No. 4, pp. 735-743, 2021. https://doi.org/10.17703/JCCT.2021.7.4.735

[2] KISA, https://www.kisa.or

[3] S. H, Bang, “Study on the implementation of electronic notices system : focus on fine and penalty”, M.S. Thesis, Korea University, 2016.

[4] J. B. Kim, “Electronic Notification Service in Public and Administrative Agencies,” The Journal of the Institute of Internet, Broadcasting and Communication, Vol. 20, No, 4, pp. 7-16, 2020. https://doi.org/ 10.7236/JIIBC.2020.20.4.7

[5] S. B. Lim, "Measures to introduce local tax 'smart bill' focusing on electronic notice, delivery, receipt, consultation, and unification using a private platform”, Korea Institute of Local Finance Forum, Vol. 32, pp.106-123, 2017.

[6] Y. A. Yu, “A Study on the Improvement Method of the Local Tax Bill Delivery Service Using the Information System”, Korea Regional Information Chemistry Society, Vol. 22, No. 1, pp. 53-73, 2019. https://doi.org/10.22896/karis.2019.22.1.003

[7] https://korea.counterpointresearch.com/

[8] H. Y. Lee, “Alternative means and management system for resident registration number for personal information protection”, Journal of Advanced Information Technology and Convergence”, Vol. 8, No. 6, pp. 49-58, 2010.

[9] J. H, Sung, “Problems of identification system relying on a unique identification number”, Korean Society of Public Sociology, Vol. 26, No. 2, pp. 208-246, 2016. https://doi.org/10.21286/jps.2016.05.6.2.208

[10] S. J, Kim, K. H, Lee, “A Comparative Study on Reforming the Resident Registration Number”, Journal of the Korea Institute of Information Security & Cryptology, Vol. 25, No. 3, pp. 673-689, 2015. https://doi.org/10.13089/JKIISC.2015.25.3.673

[11] J. B. Kim, “A Study on the Preparation of Operational Standards for Safe Mobile Electronic Notification Service”, International Symposium on Advanced and Applied Convergence, pp.128-134, 2022.