International Journal of Advanced Culture Technology Vol.10 No.2 194-200 (2022)
DOI https://doi.org/10.17703/IJACT.2022.10.2.194

IJACT 22-6-26

A Method for Effective Mobile Electronic Notification Service of Private Institutions

[1]JongBae Kim

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

Abstract

Traditionally, postal services that produce and deliver paper-based notices have been the mainstream. The reason is that it has the function of distribution and proof of delivery in the postal delivery system as well as the advantage of information delivery through postal delivery. After all, for the purpose of distribution and proof of delivery, many organizations use paper-based postal notices. However, in recent years, it has been in the spotlight to produce a paper-based postal notice as an electronic notice and deliver information to a mobile device through the Internet. In this paper, we propose a safe interworking method for user identification information required for private institutions to transmit mobile electronic notices. In order for a private institution to accurately deliver an electronic notice to a mobile service subscriber, a means to confirm whether the private institution and the mobile device subscriber are the same person is required. In the mobile electronic notification service, the connecting information provided by the personal identity proofing agency is used as a means of user identification. Connecting information is called a resident registration number on the Internet and is one-way hash information that can only be created by the personal identity proofing agency designated by the government. In order to transmit a mobile electronic notice, it is necessary to share connecting information for the same user identification between the institution that requests the sending of the electronic notice and the institution that processes the sending of the electronic notice. Connecting information is personal information that can uniquely identify a user, and if it is disclosed, damage such as personal information infringement may occur. As such, it is necessary to prevent problems that may arise from misuse and abuse of connecting information as well as increase in the benefits of sending the mobile electronic notice. In this paper, a safe and effective mobile electronic notification service can be performed by suggesting a method for safe interworking of information related to the mobile electronic notification service.

Keywords: *Mobile Electronic Notice Service, Personal Identity Proofing Service, Connecting Information, Postal Service*

1. INTRODUCTION

Mail is a service that transmits information to mail recipients in an economical way. For such a postal service, it is necessary to produce a postal mail including the sender, the recipient, and even transmission information, and deliver it to the postal service delivery institution, which is the sending entity. Looking at this process, the sender, the recipient, and the contents of the postal mail are inevitably disclosed to third parties as well as to

Manuscript received: April 7, 2022 / revised: May 10, 2022 / accepted: June 1, 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

the unknown delivery system. Therefore, services using security systems or protection methods (registration, parcel, etc.) are being added according to the importance and speed of information delivery using postal mail.

Recently, the issue of coexistence of the economy and the environment called low-carbon green growth is rapidly emerging. In particular, it has been suggested that the realization of low carbon is important to achieve green growth in the recent social environment that values the environment. Such green growth was first discussed at the International Environment and Development (ESCAP) Ministerial Meeting held in Seoul in 2005[1]. Green growth is a concept that seeks to achieve growth in harmony with the economy and the environment, and is positioned as an essential element for achieving sustainable growth[2]. Through this concept, it is suggested that it is necessary to minimize the benefits of climate change, reduce greenhouse gases, secure clean energy, and realize low carbon emission. However, in order to realize low carbon emission such as greenhouse gas reduction, scientific technology development and promotion of related industries such as awareness system will be a part that can be achieved only after a long period of time.

The practice that emerged from this low-carbon emission concept is the mobile electronic notification service. It has become a reality that traditional paper mail has a negative impact on the environment, such as consumption of energy generated by paper-based mail delivery, increased use of paper due to damage to trees, and waste generated due to insufficient recycling of mail. In fact, the production of paper mail has an environmental impact due to the consumption of natural resources and the generation of carbon dioxide. According to previous studies, it has been suggested that the amount of carbon dioxide generated by the production of 1g of paper is also about 1g. In the end, even for green growth through environmental protection and carbon emission reduction, it is required to minimize the sending of paper-based mail.

The service of sending electronic notices using mobile devices is one of the representative low-carbon emission policies. The mobile electronic notice service is a service that sends an electronic notice to a mobile device possessed by the party receiving the electronic notice [3]. Unlike paper-based mailing, paper production is unnecessary and there is no additional carbon emission such as environmental pollution during the delivery process. For the mobile electronic notification service, it is necessary to identify and identify the mobile device information or subscriber information possessed by the user. However, it is impossible for the electronic notification sending institution to grasp the information of a specific mobile service subscriber in real time. Even if the user provides the mobile service information (ID, mobile phone number, e-mail, etc.) to the electronic notification sending agency, it is impossible to verify whether the subscriber information is actually his or her information, and there is a practical problem was raised. The fundamental reason for sending paper-based mail to this day is that it has the advantage of being able to send in bulk and can prove distribution and delivery by a third party with public trust, so that it can have counter power in legal disputes that may arise in the future. As such, the mobile electronic notification service using IT devices has emerged due to various problems as well as the advantages of the paper-based mail delivery service. The mobile electronic notification service is a service that uses the user's subscriber information on the mobile device possessed by the user to identify the target user and electronically send a notice to the possessed terminal to simultaneously perform the proof of delivery and the proof of distribution.

A representative mobile electronic notification service provides a means for identifying and authenticating users when using the initial service through the Internet service, mobile communication service, bank or insurance subscription that the user has signed up for. As a user identification method, KYC (Know Your Customer) information based on proof of residence or date of birth is used[4]. In addition, the service is used by providing an authentication method using confidential information that only the identified user can use. As such, only the service provider who clearly identifies the user is the subject to send the mobile electronic notice. And, it is necessary for the requesting organization that sends the mobile electronic notice to provide information identifying the user information subscribed to the mobile electronic notice service provider. Only

then can you confirm that you are the same user between the sending agency and the sending agency. It is possible to identify users by using connecting information called resident registration numbers on the Internet that is uniquely assigned to users.

Connecting information creates link information by using resident registration number, a number system uniquely assigned to citizens by the government [5]. The resident registration number consists of a unique 13-digit number, and misuse of it may cause privacy issues. For this reason, the indiscriminate use of resident registration numbers was prohibited. As a result, as the number system that can uniquely identify users between online operators disappeared, a separate identification method was required. This is the connecting information. Connecting information is linked information so that the government-designated personal identity proofing agency receives the user's resident registration number and generates an 88-byte hash value[6]. Connecting information has limitations in human memory and is used for the purpose of user identification between systems[7]. However, connecting information is also personal information that is used to uniquely identify users online, so it is necessary to prepare safe and appropriate protection measures.

In this paper, we propose a safe and effective linkage method for connecting information used for the purpose of identifying users in the mobile electronic notification service. In the proposed method, a safe information linkage standard between the mobile electronic notification sending requesting institution and the personal identity proofing agency is presented [9, 10], and the connecting information processing plan for using the mobile electronic notice service according to the standard is suggested. By applying the proposed method to the mobile electronic notification service, it can be seen that the user's personal information can be used more effectively and safely.

2. PROPOSED METHOD

In the proposed method, the basic concept of the service that converts the user's resident registration number into connecting information (CI), the main system, the main process of the service, and the flow of personal information processing are proposed. In addition, the CI batch conversion service presents the roles, stakeholders, and basic processes within the mobile electronic notification service. In particular, since the CI batch conversion service is a service that deals with personal information and CI, basic principles for using it are presented. We present a plan for safe and effective mobile electronic notification service to be utilized.

2.1 Security standards for connecting information

The requirements for CI batch conversion service to ensure reliability and safety of CI distribution are as follows.

i. If it is necessary to store CI, it must be encrypted and stored in a secure way.
ii. User organizations that use CI batch conversion service and personal identity proofing agency that provide services must transmit and receive personal information and CI in a safe manner by applying communication message and network section encryption.
iii. When using data encryption keys [8], user organizations that use CI batch conversion services and personal identity proofing agency that provide services must ensure stability by exchanging encryption keys periodically (at least once a year).
iv. The user organization that uses the CI batch conversion service must store and manage the received CI in a safe way, and the personal information collection and storage organization must comply with relevant laws and regulations.

The personal identity proofing agency that provides CI batch conversion service cannot keep the converted CI, and the processed personal information must be destroyed without delay in a way that cannot be restored when the purpose is achieved.

2.2 Conversion service for connecting information

The CI batch conversion service is a service in which the user organization converts the recipient's resident registration number into CI for the purpose of mobile electronic notification. For CI batch conversion in the Figure 1, the electronic notification sending requesting institution first provides the resident registration number through the personal identity proofing agency to request the batch conversion to CI, and uses the received CI to deliver it to the electronic notice sending institution, and then sends the electronic document to the user. At this time, the personal identity proofing agency has a CI batch conversion system, and for the identity confirmation service, the user's unique identification information, that is, the resident registration number and the secret information possessed only by the personal identity proofing agency, is used to generate CI. The CI batch conversion system is a system that generates CI by receiving resident registration numbers provided by private organizations. Private organizations use the dispatch management system to provide mobile electronic notification services by using the linkage text to the personal identity proofing agency and certified professional relay brokers.

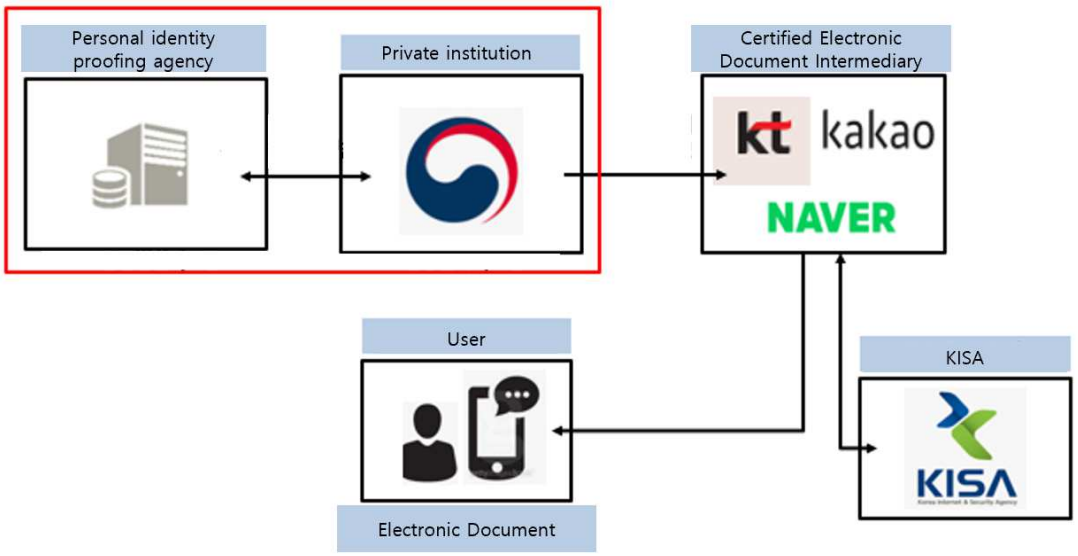

Figure 1. Overview of CI batch conversion service and mobile electronic notification service

The systems operated by service in the CI batch conversion service area are shown in Figure 2.

The operating entity of the sending notices management system is a mobile electronic notification sending requesting institution, and this system is a system of a user organization that manages the sending target's personal information (resident registration number, etc.) for the purpose of sending electronic documents through the mobile electronic notification service. In addition, the CI batch conversion system is a system of the personal identity proofing agency that uses the personal identity as the subject, converts the resident registration number requested by the user organization into CI for the purpose of converting connecting information for the purpose of mobile electronic notification service, and responds to the user organization.

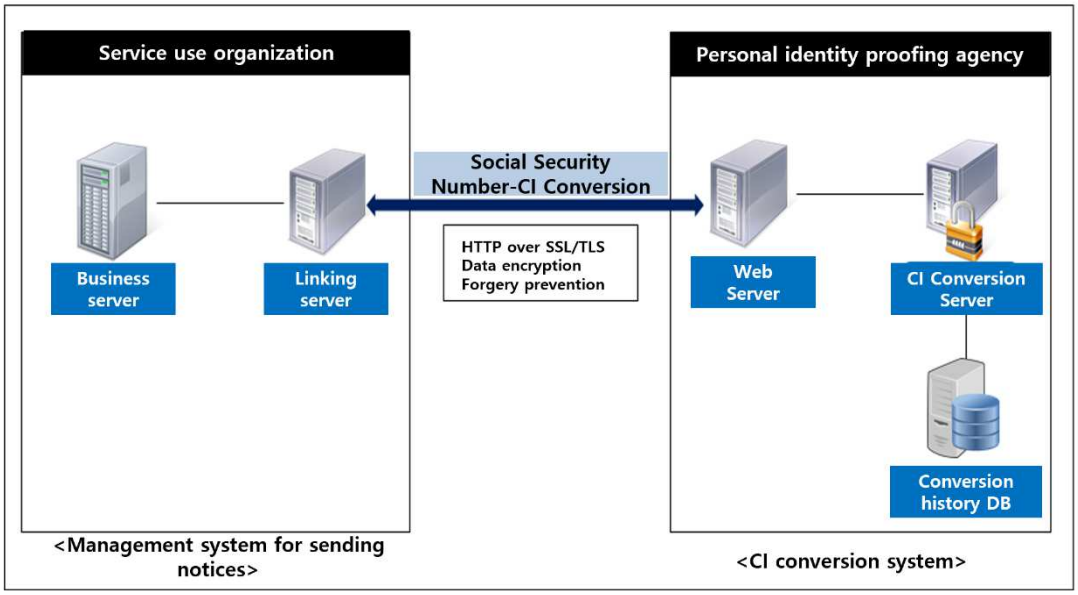

Figure 2. Overview of CI batch conversion service and system configuration

2.3 Connecting information conversion service processing flow

As the CI batch conversion service is used or provided, the main service process between the user organization and the personal identity proofing agency is shown in Figure 3.

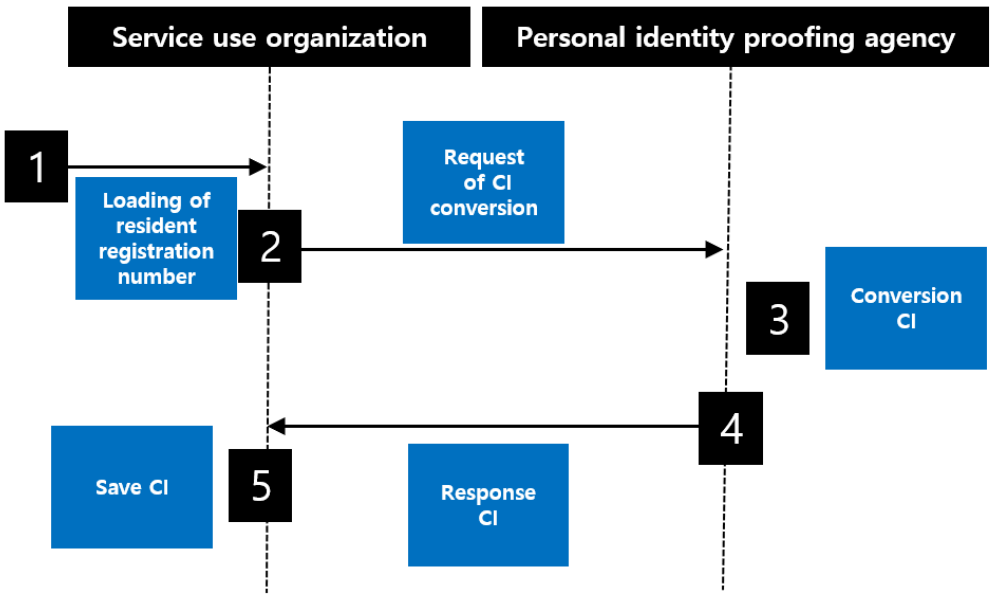

Figure 3. CI batch conversion service process

When the user organization delivers the recipient's resident registration number for use of the mobile electronic notification service to the personal identity proofing agency, the personal identity proofing agency converts the resident registration number into CI and delivers it to the user organization. The user organization sends an electronic notice to the recipient using the mobile electronic notice service using the converted CI.

When a user organization requests CI conversion from the personal identity proofing agency, it is necessary to transmit the user organization's unique identification number together. Also, there are cases where information is transmitted between the user organization and the personal identity proofing agency using the general public Internet network other than the dedicated line. Therefore, in order to CI between the user organization and the personal identity proofing agency, data encryption between each other and data encryption transmission between transmission sections are required. For data encryption and transmission section encryption, the encryption key exchange procedure between devices should also be defined [11].

2.4 Criteria for using connecting information

In order to use the CI batch conversion service, it must be linked in a predefined way between the personal identity proofing agency and the user organization. For safe CI conversion, the linkage standards that the personal identity proofing agency and user organization must comply with are as follows.

i. The recipient's personal information processed for CI conversion must be collected and processed with a minimum number of items.
ii. In case the existing CI cannot be used due to leakage of CI, etc., a plan for distributing a new CI (CI2) that replaces the existing CI should be prepared.
iii. The personal identity proofing agency shall prepare a plan to confirm whether the user organization requesting CI conversion is a legitimate request from the actual user organization.

3. DISCUSSION

In this paper, we proposed a method for safe conversion and management of connecting information used for common user identification by the sending agency and the sending agency for electronic notification in the mobile electronic notification service. In the proposed method, it is possible to unify the technical standards of various mobile notification services by defining the standard for batch conversion processing of connecting information, service overview, and processing flow chart, and to protect user personal information by suggesting a plan to utilize connecting information for user identification. Because the use of user-linked information is rapidly increasing due to the activation of the electronic notification service, it will be possible to present the standards for conversion, utilization, and processing of connecting information in advance, and a safe and efficient mobile electronic notification service will be possible.

ACKNOWLEDGEMENT

This work was supported by the Technology Innovation Program(20016800) funded By the Ministry of Trade, Industry & Energy (MOTIE, Korea) and the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (NRF-2020R1F1A106890011).

REFERENCES

[1] M.H. Lee, “A Study about Development of Environment Printing Technology and CO2,” The Korean Graphic Arts Communication Society, Vol. 30, No. 3, pp. 89-114, 2012.
[2] L.K. Chaoui, et al., “Implementation of the Korean Green Growth Strategy in Urban Areas,” OECD Regional Development Working Papers 2011/02, OECD Publishing, 2011.

[3] J.B. Kim, “A Study on the Utilization of Mobile Electronic Notice Service using Korean Digital Identity Guidelines,” Turkish Journal of Computer and Mathematics Education, Vol. 12, No. 13, pp. 2855-2861, 2021.

[4] J.B. Kim, “A Study on Establishment of Connecting Information Conversion Criteria for Mobile Electronic Notification Service of Private Institutions,” The Journal of the Convergence on Culture Technology, Vol. 7, No. 4, pp. 735-743, 2021.

[5] Y.J. Shin, et al., “A Study on the Improvement of Personal Identification Means in South Korea - Focused on the Diagnosis and Suggestion for Improvement Direction by Professionals,” The Korean Association for Regional Information Society, Vol. 20, No. 4, pp. 145~179, 2017.

[6] H.Y. Yum, “A proposal of assurance model based on i-PIN assurance level,” The Society of Digital Policy & Management, Vol. 14, No. 9, pp. 287-299, 2016.

[7] J.B. Kim, “A Study on the Actual Use of Mobile Electronic Notification Service,” The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 21, No. 5, pp. 167-180. 2021.

[8] T. Zhu, X. Hu, P. Xiong, W. Zhou, “The Dynamic Privacy-Preserving Mechanisms for Online Dynamic Social Networks”, IEEE Trans. On Knowledge and Data Engineering, Vol. 34, No. 6, pp. 2962-2974, 2020.

[9] M. S. Ferdous, R. Port, “Portable personal identity provider in mobile phones”, 12th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, pp. 736-745, 2013.

[10] NIST, Digital Identity Guidelines, https://pages.nist.gov/800-63-3/

[11] Y. Ding, Y. H. Li, “Integration of Signature encryption and key exchange”, IEEE Int. Conf. on Computational Intelligence and Security, vol. 2, pp. 299-302, 2008.