The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 20, No. 4, pp.7-16, Aug. 31, 2020. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2020.20.4.7
JIIBC 2020-4-2

# 공공·행정기관 모바일전자고지서비스의 기술적인 안전성 확보 방안에 대한 연구

# A Study on the Securing Technological Safety of Mobile Electronic Notification Service in Public and Administrative Agencies

**김종배***

Jong-Bae Kim*

**요 약** 최근 비대면 서비스의 급속한 확대로 인해 다양한 분야에서 모바일 기기를 활용한 모바일전자고지서비스가 등장하고 있다. 모바일전자고지서비스는 지류 기반의 우편고지서비스가 가진 여러 문제점(개인정보노출, 오배송, 환경 오염, 비용 증가 등)들을 해결하기 위해서 휴대전화 문자나 앱 기반의 메시지 푸시(push) 기능으로 고지문을 전달하고 송달 여부에 대해 전자문서중계사업자가 유통을 증명해 주는 서비스이다. 공공·행정기관들이 모바일전자고지서비스 제공을 위해서는 이용자가 보유하고 있는 휴대폰 번호나 가입된 앱의 사용자 식별정보(카카오 계정 등)가 필요하다. 그러나 이러한 정보는 개인정보에 해당하여 수집 시 이용자 동의가 필요하고 동의 받은 사용자들에게만 고지가 가능한 한계가 있다. 이러한 한계를 극복하기 위해 ICT규제 샌드박스 제도를 활용하여 공공·행정기관이 보유한 이용자의 주민등록번호를 연계정보(Connecting Information: CI)로 일괄변환을 허용하고, CI를 전자문서중계사업자에게 전달하여 해당 CI 이용자가 보유한 모바일 기기로 공공·행정기관이 전송을 요구한 전자고지문을 발송하도록 임시로 허용하였다. 따라서 본 논문에서는 모바일전자고지서비스에 있어 이용자 CI에 대한 안전한 관리, 전자고지문 열람자의 본인확인, 그리고 전자고지문의 위·변조 방지까지의 기술적인 방안을 제안한다. 제안한 방안에서는 모바일전자고지문 이용자를 식별하기 위해 주민등록번호와 CI를 사용하여 공공·행정기관과 모바일전자문서중계사업자 간의 새로운 식별정보를 생성하고, 모바일 전자고지문 열람자 확인 및 위·변조 방지를 수행하기 위한 절차를 제시한다. 제안한 방안을 통해 이용자의 편리성과 더불어 CI에 대한 기술적인 안전성을 확보함으로써 모바일전자고지서비스의 역기능을 최소화하여 서비스가 활성화 될 수 있음을 확인한다.

**Abstract** The mobile electronic notification service delivers notifications through mobile phone text or app-based message push to solve various problems of the paper-based mail service. And it is a service that an electronic document relay company proves to prove delivery. In order for public and administrative agencies to provide mobile electronic notification service, the user's identification information of the mobile phone number or the subscribed app is required. To overcome these limitations, ICT-regulated sandbox system was used to allow collective conversion of users' resident registration numbers into connecting information (CI). Therefore, in this paper, we propose a technical method for safe management of user CI in mobile electronic notice service, identity verification of electronic notice readers, and prevention of forgery and forgery of electronic notices. Through the proposed method, it is confirmed that the service can be activated by minimizing the adverse function of the mobile electronic notification service by securing the user's convenience and technical safety for the CI.

**Key Words :** Mobile electronic notification service, ICT-regulated sandbox, Connection Information, Personal proofing service

*정회원, 세종사이버대학교 소프트웨어공학과
접수일자 2020년 7월 20일, 수정완료 2020년 8월 7일
게재확정일자 2020년 8월 7일

Received: 20 July, 2020 / Revised: 7 August, 2020 /
Accepted: 7 August, 2020
*Corresponding Author: jb.kim@sjcu.ac.kr
Department of Software Engineering, Sejong Cyber University, Korea

# Ⅰ. 서 론

2019년 정부는 관련 규제 법률들에 인해 활성화되지 못하는 신사업들을 발굴하여 법적인 구속력을 임시로 회피할 수 있는 제도를 마련하였다. 이를 ICT규제 샌드박스라고 불리며 관련 규제에 의해 사업 활성화가 더디거나 불가능한 경우에 대해 심사를 거쳐 임시로 허용하는 제도이다[1]. 이 제도는 4차 산업혁명과 신산업 발굴을 통해 경제성장과 국민들에게 다양한 혜택을 부여데 그 목적이 있다. 공공·행정 규제 샌드박스를 통해 제1호로 허용된 제도가 모바일전자고지서비스이다. 공공·행정기관들은 각종 민원 정보들을 이용자들에게 제공하기 위해 우편 서비스를 이용하고 있다. 그 외 추가적으로 모바일 서비스를 발굴하여 이용자가 선택적인 동의 시 이메일, 휴대전화 문자, 앱 기반의 메시지 푸시 방법으로 정보제공 서비스를 실시하고 있는 상황이다. 이는 공공·행정기관 대상 전체 이용자가 아닌 모바일 서비스 제공을 동의한 이용자에게 한해 제공하고 있다. 그 외 이용자들에게는 현행과 같이 우편 서비스를 통해 송달하고 있다. 예를 들어, 국민연금 관련 정보, 병역에 관련된 정보, 교통범칙금에 관한 정보, 운전면허증 유효기간 만료에 관한 정보, 자동차 검사 기간 도래에 관한 정보 등이 해당한다. 공공·행정기관이 이용자들에게 제공하는 정보들은 대부분의 공공·행정기관의 편익을 위해서가 아니라 정보를 제공받는 이용자의 편익을 위해서이다. 운전면허증 갱신기간 만료라든지 자동차 정기 검사 만료로 인한 자동차로 생계를 유지하는 이용자의 경우, 그로 인한 피해는 실로 말할 수 없이 크다고 할 수 있다. 이처럼 국민 편익을 위해 공공·행정기관이 제공하는 우편 기반의 정보제공 서비스에는 무수히 많은 상황이다. 우편 서비스를 사용하는 이유는 송달 우편문서에 대한 발송과 수신 입증이 가능하기 때문이다. 따라서 공공·행정기관의 전자고지문의 경우도 그림 1과 같이 전자문서중계자를 통해 문서를 전달함으로써 유통증명이 가능하도록 하는 것이 필요하다. 하지만 우편 서비스 제공에는 여러 문제점들이 수반된다. 이용자의 주소 미변경으로 인한 오배송으로 우편 내용의 노출, 배송된 우편물의 관리 부주의에 의한 개인정보 노출, 우편 배송에 대한 비용 증가, 지류 제작에 따른 환경오염 증가 등이 문제점으로 귀결될 수 있다. 물론 정보소외계층이나 사회 취약층들에게는 현행 지류 기반의 우편 서비스의 유지가 필요할 것이다[18]. 그럼에도 불구하고 대다수의 국민들은 모바일 폰을 보유하고 있으며 전체 인구 대비 약 95.9%가 인터넷을 이용하고 있는 것으로 조사되었다[2, 17]. 이러한 환경에서 모바일전자고지를 위해 공공·행정기관이 전자문서중계사업자를 통해 각종 전자고지문을 제공으로써 얻는 경제적, 환경적, 물리적인 이익을 크다고 할 수 있을 것이다. 이러한 공공·행정기관의 모바일전자고지서비스에서 가장 큰 문제점은 공공·행정기관이 이용자의 개인정보를 어떻게 수집할 것인가이다. 공공·행정기관은 행정주민정보가 기록된 데이터베이스에 접근하여 주소, 이름, 주민등록번호, 가족관계 등을 확보할 수 있다. 그 외 공공·행정기관의 특성에 따라 합법적으로 수집할 수 있는 개인정보는 더 많이 존재할 것이다. 하지만, 공공·행정기관이 해당 이용자에게 전자고지문을 전달하기 위해서 이용자가 가입하여 사용하고 있는 통신 수단의 가입정보가 필요하다. 공공·행정기관이 보유하고 있는 통신수단 정보에는 아용자가 제공을 동의한 휴대전화 번호나 이메일 주소일 것이다. 하지만 이용자 제공을 동의한 휴대전화 번호는 본인이 손쉽게 변경할 수 있으며 다른 사용자들에게 재 점유가 가능한 수단이다. 그리고 이메일 역시 해당 이용자의 고유한 정보 전달 수단에는 부족한 상황이다. 이를 해결하기 위해 가장 손쉬운 방법은 그림 2와 같이 주민등록번호를 전자문서중계사업자에게 제공하여 통신가입 여부를 확인하는 것이다.

하지만, 앱 기반의 메시지 푸시 서비스 전자문서중계사업자는 앱 가입자의 주민등록번호를 보유하고 있지 않아 서비스 가입 여부 확인이 불가능하다. 더 큰 문제는 공공·행정기관이 이용자의 주민등록번호를 제3자에게 제공하는 것이다. 「개인정보보호법」제24조(고유식별정보의 처리 제한)에 따르면 이용자의 고유식별정보 처리에 대한 동의를 별도로 받거나 법령에서 구체적으로 허용한 경우에만 처리하도록 규정하고 있다. 따라서 모바일전자고지서비스의 특성상 공공·행정기관이 이용자에게 주민

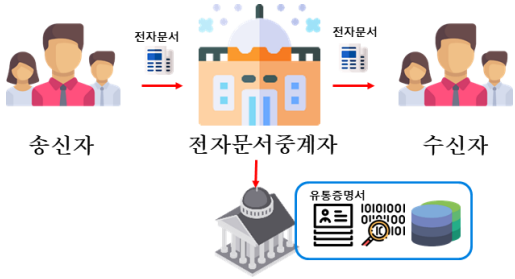


**그림 1. 전자문서중계자를 통한 전자문서 유통 과정 흐름도**
**Fig. 1. Flow of electronic document distribution process through electronic document relay company**

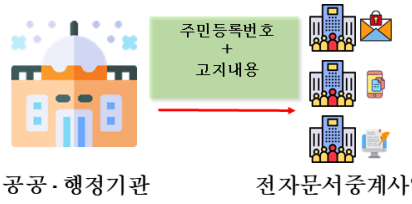


**그림 2. 주민등록번호 기반의 모바일전자고지서비스 개념**
**Fig. 2. Mobile electronic notification service concept based on resident registration number**

등록번호 제공에 대한 처리 동의를 모두 받는 것으로 거의 불가능한 상황이다. 이는 시간적 및 비용적으로 한계가 있는 것이 사실이다. 물론 공공·행정기관이 자신의 이익을 취하고자 주민등록번호를 제3자에게 제공하는 것이 아님은 인지할 수 있으나 법에서 규정한 바에 따라 행정업무를 수행할 수밖에 없는 상황이다. 또한, 앱 기반의 메시지 푸시 서비스 제공기관들은 이용자 서비스 가입 시 이동통신사와 달리 주민등록번호를 수집하지 않기 때문에 공공·행정기관과의 이용자 식별 시 주민등록번호로는 불가능한 상황이다. 이러한 통신 사업자들이 주민등록번호를 수집하는 대신에 본인확인기관이 제공하는 본인확인서비스를 통해 주민등록번호와 1:1로 매칭되는 연계정보(Connecting Information: CI)를 제공받는다. 따라서 전자문서중계사업자들은 온라인 서비스에서 이용자를 식별하기 위해 주민등록번호 대체수단을 통해 제공받은 CI를 활용하는 것이다.

CI는 이용자가 제시한 주민등록번호를 사용하여 본인확인기관이 생성한 88byte로 일방향 암호화된 값이다. 즉, 주민등록번호와 1:1 매칭되는 값으로써 이용자를 고유하게 식별할 수 있는 정보이다. 일반적으로 CI는 이용자가 외울 수는 없으나 온라인 서비스를 위해 시스템 간의 이용자를 식별하고 연계하기 위한 목적으로 사용되고 있다[3, 4]. CI는 이용자가 본인확인기관의 본인확인서비스를 사용하여 자신의 CI를 인터넷서비스사업자(Internet Service Provider: ISP)에게 제공하도록 동의하는 절차를 거치고 있다. 방송통신위원회가 지정한 본인확인기관의 업무 역시 본인확인서비스 이용자의 개인정보를 ISP에게 제공 시에는 서비스 이용자 본인을 확인하고 개인정보를 제공하도록 규정하고 있다[5]. 이때 사용하는 본인확인수단에는 아이핀, 휴대전화번호, 신용카드번호, 범용공인인증서가 있다[6]. 결국 공공·행정기관이 모바일전자고지서비스를 위해서 보유하고 있는 주민등록번호를 본인확인기관에게 제공하여 CI로 일괄 변환하는 과정이 필요하나 이 역시 본인확인기관 입장에서는 개별 이용자의 동의 없이 CI 변환은 본인확인 역무에 벗어나는 업무로써 전자고지서비스 제공이 불가능하다. 더구나 공공·행정기관이 공인문서중계사업자에게 이용자 동의 없이 주민등록번호를 제공할 수도 없다. 가장 합리적인 방법은 온라인상에서 이용자를 고유하게 식별할 수 있는 CI를 공공·행정기관과 전자문서중계사업자 간에 식별 정보로 사용하는 것이다.

이처럼 법적인 관련 규제에 따라 수행할 수 없는 서비스를 제공하기 위해 규제샌드 박스에서는 본인확인기관이 이용자 동의 없이 주민등록번호를 CI로 일괄변환을 허용한 것이다. 그림 3과 같이 공공·행정기관은 주민등록번호에 매칭되는 연계정보(CI)를 활용하여 전자문서중계사업자에게 제공하고, 전자문서중계사업자는 수신 받은 CI를 활용하여 모바일 기기 가입자에게 전자고지문을 발송한다. 모바일 기기를 통해 전자고지문 발송 시 해당 이용자에게 발송되어야 하고, 발송 이후 송달에 관한 유통입증이 가능해야 한다. 이를 위해서는 공인문서중계자가 공신력이 있거나 검증받은 기관이어야 하며 전자문서 중계 이후 발송 이력을 보관하고 유통을 증명해야 한다. 따라서 공인문서중계자는 공인전자주소 생성 및 유통정보 관리를 위해 이용자에게 서비스 제공 동의 징구 받고 한국인터넷진흥원으로 공인전자주소와 유통정보 등록을 요청한다. 모바일전자고지서비스에서 이용자를 명확하게 식별하기 위해 주민등록번호 대신 CI를 사용하여 식별하고, 전자문서 송달 증명을 위해 공인문서중계사업자가 발

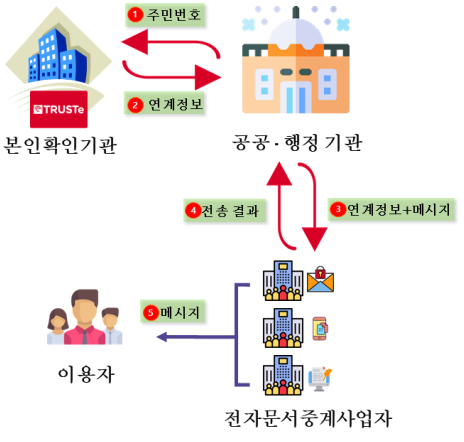


**그림 3. 모바일전자고지서비스 처리 개념도**
**Fig. 3. Mobile electronic notification service processing concept**

송하고 유통증명을 수행함으로써 전자고지문의 송달 입증이 가능하다. 이후 이용자가 전자문서를 개봉 시 열람 입증이 가능하도록 전자문서중계자의 인증서버를 활용함으로써 실현이 가능하다.

결국, 모바일전자고지서비스에서 이용자 개인정보에 해당하는 CI를 어떻게 관리할 것인가가 핵심 이슈로 부각되고 있다. 따라서 본 연구에서는 온라인상에서 이용자를 고유하게 식별할 수 있는 CI의 안전한 관리방안에 대해 제안한다. 그리고 전자문서의 유통과정에서 유·노출, 변조 등과 같은 해킹이 발생하지 않도록 하는 방지 방안도 함께 제시한다. 제안 방안에서 CI를 사용하지 않고 공공·행정기관과 모바일전자고지서비스 사업자간에 이용자를 식별할 수 있는 정보를 손쉽게 생성하고 공유할 수 있다면 가장 효과적인 방안일 것이다.

본 논문에서는 2장에서 모바일전자고지서비스의 개요에 대해 살펴보고, 현재 서비스 중인 사용현황, 그리고 문제점들을 기술한다. 그리고 3장에서는 모바일전자고지서비스 문제점을 해결하기 위한 방안을 제안한다. 제안하는 방안에서는 CI 암호화 및 관리 방안, 열람 시 본인확인 방안, 그리고 전자고지문의 위·변조 방지 방안을 제안한다.

## II. 모바일전자고지서비스 개요

모바일전자고지는 공공·행정기관이 이용자들에게 정확하게 전자고지문을 발송하고, 발송 후에는 송달 확인을 위한 목적으로 제공하는 서비스이다. 이러한 서비스를 위해서는 이용자 개인정보의 안전한 관리와 보안성 강화 방안이 요구된다. 온라인상에서 이용자를 고유하게 식별할 수 있는 CI 암호화와 관리 방안, 그리고 연계방안을 효과적으로 마련함으로써 서비스 활성화뿐만 아니라 이용자 개인정보보호도 가능할 것이다. 그림 4는 모바일전자고지서비스의 개요도이다. 가장 먼저 ① 공공·행정기관에서는 모바일전자고지를 위해 이용자의 주민등록번호를 본인확인기관에 제공하여 CI로 일괄변환을 수행하고 CI와 고지문을 모바일통지 플랫폼으로 전송한다. 이때 공공·행정기관은 모바일전자고지를 위해 서비스 종류를 선택한다. 서비스 종류에는 휴대전화 문자로 고지할 것인지? 앱 기반 푸시 메시지 기반으로 고지할 것인지? 아님 두 종류 다 사용할 것인지를 결정한다. 결정한 후 CI와 고지문을 전자문서중계사업자에게 전달한다. 현재 전자문서중계사업자는 KT와 카카오가 서비스 중이며 하반기에 네이버가 서비스를 시작할 예정이다. ② 해당 CI와 전자고지문을 공공·행정기관이 선택한 전자문서중계사업자로 전송한다. ③ 전자문서중계사업자는 해당 CI 이용자에게 고지문을 발송한다. ④ 발송결과를 모바일통지 플랫폼으로 전송한다. ⑤ 이용자의 모바일 단말기에 보안 URL을 전송한다. ⑥ 모바일전자고지서비스 가입 및 공인전자주소 생성 동의 절차를 수행한다. ⑦ 발송된 전자문서를 열람한다. ⑧ 전자문서고지서비스 동의 모바일 통지 플랫폼이 수신한다. ⑨ 공공·행정기관에 발송 결과를 전송한다. ⑩ 공인전자주소와 유통정보를 관리하기 위해

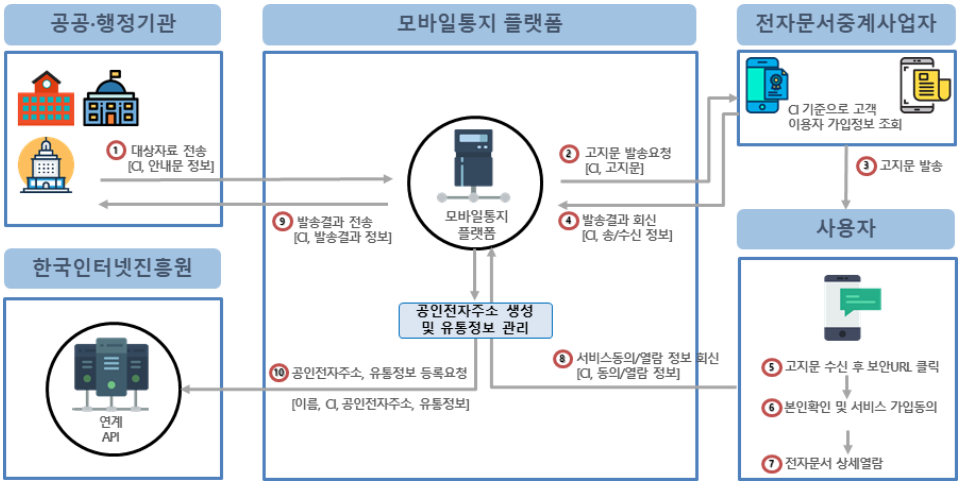


**그림 4. 모바일전자고지서비스 처리 개념도**
**Fig. 4. Mobile electronic notification service processing concept**

한국인터넷진흥원으로 등록을 요청한다. 그림 4의 처리 과정에서 알 수 있듯이 이용자 CI는 다양한 기관에 처리되는 것을 알 수 있다. 따라서 모바일전자고지서비스에서 이용자 식별을 위해 사용하는 CI에 대한 관리 방안을 마련하는 것이 주요한 사항이다.

## 1. 모바일전자고지 서비스 활용 현황

모바일전자고지 서비스는 공공기관, 일반 기업 등에서 각종 안내문, 통지문 등을 이동통신사 가입자 혹은 모바일 앱 서비스 가입자들에게 우편 대신 등기효과가 있는 문자 메시지(MMS 등), 앱 기반의 푸시 메시지로 발송하는 서비스이다. 등기효과의 근거에는 「전자문서법」18조의 5에 의거 공인전자주소를 통하여 전자문서 송신 수신 열람된 사실에 대한 추정력 부여하는 것으로써 현재 KT, 카카오페이, 네이버가 공인전자문서중계자로 지정되어 있다. 모바일전자고지 서비스를 위해서는 공공·행정기관이 보유한 주민등록번호를 CI로 일괄 변환하는 과정이 요구된다. 2019년 공공·행정기관 대상 모바일전자고지 발송 현황은 표 1과 같다. 전자고지문 발송 시점이 2019년 2월 18일부터 서비스를 시작하여 현재까지 약 천만건 이상의 발송 수를 보이고 있다.

**표 1. 공공·행정기관 모바일 고지 서비스 현황**
**Table 1. Status of mobile electronic notification service for public and administrative agencies**

| 구분 | '19.1분기 | 2분기 | 3분기 | 4분기 | '20.1분기 |
|---|---|---|---|---|---|
| 발송 건수 | 1,146,117 | 8,780,702 | 7,656,409 | 8,024,862 | 11,679,977 |
| 발송 서식수 | 12 | 28 | 35 | 68 | 93 |
| 이용 기관수 | 2 | 7 | 8 | 17 | 16 |

## 2. CI 이용 현황

CI는 온라인상에서 두 사업자가 이용자를 식별하기 위한 목적으로 사용되는 연계정보이다. CI는 방송통신위원회가 지정한 주민등록번호 대체수단 기반의 본인확인기관에서만 생성 및 발급이 가능하다. 본인확인기관이 CI 발급 시에 해당 이용자가 허무인(사망자, 국적포기자, 국적상실자, 실종자 등) 여부를 확인하고 이용자 동의와 본인 확인 과정을 거쳐 수행된다. 많은 ISP들이 결제, 회원가입, 정보변경, 환불 등에서 정당한 이용자인지 확인하기 위해 대체수단 기반의 본인확인서비스를 활용하고 있다. 기존 연구[3, 7]에서는 2019년 약 16억 건 이상의 대체수단 기반의 본인확인서비스 이용 건수를 제시하고 있는데 이는 국내 인터넷 사용 가능한 인구가 연 평균 약 40회 이상 사용하고 있는 상황이다. 이용자가 ISP로부터 요구받은 대체수단 기반의 본인확인서비스를 수행하면 본인확인기관은 이용자를 확인하고 본인확인기관이 보유한 개인정보를 ISP에게 제공한다. 이때 본인확인기관이 ISP에게 제공하는 개인정보는 이름, 생년월일, 성별, 내외국정보, 연령대정보, 청소년여부, 아이핀번호(아이핀 서비스), 휴대폰번호 및 가입통신사정보(휴대전화 서비스), 연계정보(CI), 중복가입방지확인정보(DI), 그 외 기타 정보들을 제공한다. 이러한 이용자 개인정보를 전달받은 ISP들은 서비스에 필요한 정보만을 DB에 저장하고 나머지는 삭제 처리하는 것이 일반적이다. 이때, CI는 주민등록번호와 1:1일 매칭되는 고유한 정보이고, DI는 해당 ISP에서만 유일하게 이용자를 식별할 때 사용하는 정보이다. 따라서 CI만 알고 있으면 해당 정보주체가 온라인상에서 어떠한 행위를 하였는지 식별이 가능하고 정보주체의 권리행사도 가능한 환경이다[8-10]. 2012년 당시 주민등록번호 오·남용으로 인한 개인정보침해 이슈가 부각되어 법령에 근거를 둔 환경에서만 수집 및 처리가 가능하도록 한 바가 있다. 물론 주민등록번호는 사람이 외울 수 있는 13자리 숫자로 구성되어 있는 반면에서 CI는 88byte로 암호화되어 있는 값으로써 사람이 외워서 활용하는 것보다는 시스템간의 연계를 통해 식별하는데 활용하고 있다. 결국, 주민등록번호의 역기능으로 인해 불필요한 수집 및 처리를 금지한 것과 같이 현재는 CI가 주민등록번호의 자리를 대신하고 있는 상황이다. CI 생성 알고리즘 역시 2008년에 개발된 512비트 키 길이를 가지는 HMAC 함수를 사용하고 있으나 HMAC 함수의 오류 검증 과정을 수행한 바가 없으며, 본인확인기관과 KISA간의 비밀키 관리에 대한 검증도 수행한 바가 없는 상황이다. 또한 최근에는 양자컴퓨터 등 대량의 수학적 계산이 가능한 컴퓨팅 시대에 도래함에 따라 대량의 CI와 매칭되는 주민등록번호를 보유하고 있다면 HMAC의 역함수 추론과정을 통해 비밀키 추정이 가능할 것이다. 결국, 공공·행정기관뿐만 아니라 민간·금융기관들에서 모바일전자고지서비스 제공 시 CI를 사용한 방안을 재검토할 필요가 있다.

## 3. 모바일전자고지서비스 문제점

모바일전자고지서비스 제공에 있어 기술적으로 해결해야 할 문제점들 다음과 같다.

첫째, 공공·행정기관과 본인확인기관 간의 데이터(주민등록번호, CI) 전송 시 암호화 및 관리 방안

둘째, 전자고지문 열람자의 본인확인 적용 방안

셋째, 전자고지문의 위·변조 방지 방안

이처럼 다양한 문제점들을 해결하기 위해 본문에서는 모바일전자고지서비스의 기술적인 안전성 강화를 위한 방안을 제안한다. 해당 문제 중에서 가장 주요한 사항은 공공·행정기관과 본인확인기관 간에 전송하는 데이터(주민등록번호, CI)에 대한 암호화 방안, CI에 대한 안전한 관리 방안, 전자고지문의 위·변조 방지 방안 마련이다. 이를 위해 현행 본인확인기관과 ISP들간의 정보 연동과정을 참고하여 기술적인 안전성 강화 방안을 제시한다. 무엇보다도 CI에 특화된 암호화 방안과 연계 방안이 요구되는데 CI에 대한 모바일전자고지서비스용으로 사용 가능한 암호화 방안을 제시하고 전자고지문의 위·변조 및 스미싱을 해결하기 위해 안심문자 포함 발송 등의 해결방안을 제시한다.

## Ⅲ. 모바일전자고지 서비스 개선방안

### 1. CI의 암호화 및 관리 방안

모바일전자고지 서비스의 가장 큰 이슈는 온라인상에서 이용자를 고유하게 식별할 수 있는 CI의 안전한 활용방안에 있다. 모바일전자고지서비스에서 CI를 두 기관간 식별정보로 활용하는데 대해 재검토할 필요가 있다. 물론 온라인상에서 이용자를 고유하게 식별할 수 있는 정보는 CI이다. 이 때문에 많은 ISP들이 주민등록번호 대체수단 기반의 본인확인서비스를 이용하고 있다. 그럼, 모바일전자고지 서비스에서 정말 CI가 필요한 것일까? 모바일전자고지를 제공하고자하는 공공·행정기관들은 발송대상 이용자에게 고지문을 정확하게 전달하고 해당 고지문을 송달하였다는 확인을 받으면 어떤 이용자 식별정보가 제공되더라도 관계가 없을 것이다. 즉, 공공·행정기관은 CI가 아니더라도 전자문서중계사업자가 이용자를 정확하게 식별할 수 있는 수단이 있다면 어떠한 식별정보를 사용하여도 무방할 것이다. 그럼, 이용자의 동의 없이 왜 CI를 일괄변환하는 것이 필요한 것인가? 그 이유는 전자문서중계사업자에 있다. 전자문서중계사업자가 저장하고 있는 이용자 개인정보중에서 고유하게 식별할 수 있는 정보가 CI이기 때문이다. 그럼, 이제 CI의 과도한 사용에 따른 이용자 개인정보침해의 문제를 해결할 수 있는 방안이 제시되었다. 바로 CI 사용이 아닌 공공·행정기관과 전자문서중계사업자가 이용자를 고유하게 식별할 수 있는 정보를 생성하여 공유하면 가능할 것이다.

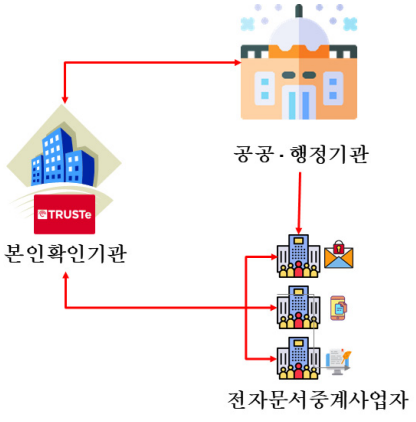


**그림 5. 모바일전자고서비스를 위한 정보 공유 흐름도**
**Fig. 5. Information sharing flow for improving mobile electronic notification service**

공공·행정기관, 본인확인기관, 전자문서중계사업자가 공동으로 이용자 식별정보를 공유하면 CI가 아닌 다른 정보로도 충분히 서비스가 가능할 것이다. 하지만, 여기서 고려해야 할 사항이 있다. 첫 번째는 공공·행정기관이 기존에 보유하고 있는 CI 변환이 필요하다. 두 번째는 전자문서중계사업자의 수가 많지 않아야 한다는 사항이다. 공공·행정기관이 다른 서비스를 위해 보유하고 있는 CI 변환과 주민등록번호의 변환, 그리고 전자문서중계사업자가 보유한 CI 변환을 동시에 만족하는 방안 마련이 요구된다. 그림 5와 같은 서비스 처리 과정의 경우에도 결국에는 CI가 아닌 모바일전자고지용 이용자 식별정보를 광범위하게 활용하는 문제점이 발생한다. 이는 해당 업권별 공유식별정보를 활용하는데 기인한 문제라 할 수 있다. 따라서 근본적으로 모바일전자고지서비스에서 CI 암호화 및 관리를 위해 그림 6과 같은 방안이 필요하다. 즉 공공·행정기관별 서로 다른 이용자 식별정보를 활용하는 것이다. 그림 6의 구조에서는 다음과 같은 이점이 있다. 첫 번째, 본인확인기관은 어떤 공공·행정기관이 일괄변환을 요구하는지 인지할 수 없다. 두 번째, 모바일전자고지용 이용자 식별정보가 공공·행정기관별로 서로 달라 유출되더라도 그 영향도는 작다. 셋째, CI와 모바일전자고지용 이용자 식별정보가 파편화된 방안으로 생성되어 안전성이 높다. 다만, 공공·행정기관별로 고유한 이용자 식별정보를 생성할 것인가 아니면 공공·행정기관들을 유형별로 분류하여 같은 식별정보를 생성 및 활용할 것인가

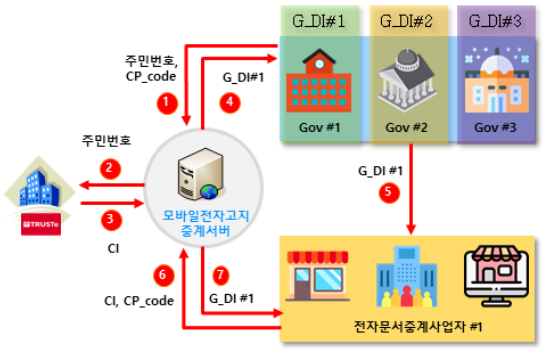


**그림. 6. 모바일전자고서비스 개선방안의 처리 흐름도**
**Fig. 6. Utilization of shared information for each business sector to improve mobile electronic notification service**

는 서비스 영향도를 분석하여 구분이 가능하다. 여기서 언급하는 G_DI는 공공·행정기관의 모바일전자고지 시 이용자를 식별정보이다.

$$G\_DI = HMAC_{gk}(CI \| cp\_code)$$
$$CI = HMAC_{sk}((RN \| Padding) \oplus S_A) \quad (1)$$

여기서, $HMAC()$는 암호화 함수, $RN$은 주민번호, $Padding$은 정해진 자리 수를 만들기 위한 과정, $S_A$는 본인확인기관과 KISA이 공유하는 비밀정보, $sk$는 본인확인기관과 KISA가 공유하는 비밀키, $\oplus$는 베타적 논리합, ||는 앞뒤를 연접하는 기호, 그리고, cp_code는 공공·행정기관에게 부여된 고유한 숫자, $gk$는 모바일전자고지중계서버와 서비스 관리주체가 공유하는 비밀키이다. 추가적으로 본인확인기관과 공공·행정기관 혹은 모바일전자고시중계서버간의 데이터 전송 시 암호화 키는 매년마다 키 체인 기반의 교환을 과정을 통해 변경하도록 한다.

## 2. 전자고지문 열람자의 본인확인 방안

모바일전자고지문을 안전하게 전자문서중계사업자가 사전에 등록한 이용자의 휴대전화 혹은 인증한 모바일 단말기로 전송한 이후 해당 이용자만이 전자고지문을 열람하도록 본인확인 방안의 적용이 필요하다. 이는 모바일 전자고지문의 위·변조 방지 방안과 연계될 수 있다. 우선 전자문서중계사업자들은 사전 이용자 개인정보를 보유하고 있다. 예를 들어 휴대전화 기반의 전자문서중계사업자는 휴대전화 가입자의 개통에 관련된 개인정보, 그리고 앱 기반 메시지 푸시 기능의 전자문서중계사업자는 앱 가입 시 제공받은 개인정보이다. 휴대전화 문자 메시지를 사용하여 전자고지문을 발송하는 경우 실제 해당 휴대전화를 본인이 소지하고 있는지에 대한 확인 과정이 필요하다. 다만, 앱은 소지 기반이 아닌 지식기반의 인증 방식으로써 추가적인 확인 과정이 요구된다[16]. 전자문서중계사업자는 전자고지문 열람자의 정보를 공공·행정기관으로부터 CI를 암호화한 G_DI정보를 보유하고 있다. ① 전자문서중계사업자가 가입자 정보를 기반으로 이용자의 모바일 단말기에 본인확인을 요구하는 링크가 포함된 메시지를 전송한다. ② 이용자는 전자고지문 열람을 위해 본인확인 링크를 클릭하고 본인확인에 필요한 정보를 입력한다. 만약 최초 모바일전자고지서비스 이용자라면 주민등록번호 대체수단 기반의 본인확인서비스를 이용하여 정당한 이용자인지 확인한다. 이후 서비스 때는 사용자가 선택한 인증방법(PIN 번호, 지문, 패턴 등)을 적용한다. 휴대전화 문자 기반의 전자고지서비스라면 휴대전화번호, 통신사 정보는 입력창을 비활성화하고 사용자 이름, 생년월일, 성별, 그리고 동의 여부만 수정할 수 있도록 한다. 앱 기반의 전자고지서비스라면 본인확인에 필요한 정보 입력과 함께 앱이 설치된 단말기 기기 정보(IMEI, UUID 등)를 전자문서중계사업자에게 전송한다. ③ 전자문서중계사업자는 본인확인기관에게 이용자가 입력한 정보를 기반으로 본인확인을 요청한다. 이때 본인확인기관에게 전송되는 정보에는 해당 서비스가 모바일전자고지서비스용 본인확인이란 사실이 포함된 공공·행정기관 코드를 함께 전송한다. ④ 본인확인기관은 해당 요청이 모바일전자고지용 본인확인임을 기관 식별코드로부터 인지하고 G_DI를 전달한다. ⑤ 전자문서중계사업자는 공공·행정기관으로부터 전달받은 G_DI와 본인확인기관으로부터 전달받은 G_DI의 비교과정을 수행하고 일치할 경우 전자고지문을 열람할 수 있도록 한다.

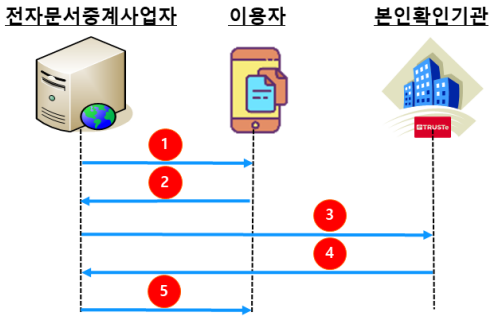


**그림. 7. 전자고지문 열람자의 본인확인 처리 흐름도**
**Fig. 7. Flow of identity verification of electronic notice readers**

### 3. 전자고지문의 위·변조 방지 방안

휴대전화 문자 및 앱 기반 메시지 푸시를 통해 전자고지문 전달과정에서는 악의적인 목적으로 공공·행정기관이 발송한 모바일전자고지문과 같이 위조하여 이용자에게 발송하고 해당 이용자로 하여금 고지문에 포함된 링크 클릭을 유도한 후 개인정보를 탈취하는 문제점이 존재한다[11-13, 15]. 이를 방지하기 위해 그림 8과 같이 우선 모바일전자문서중계사업자는 해당 이용자의 모바일 단말기에 대한 기기 인증을 최초 수행한다. 기기 인증은 기기 단말기 고유 정보인 USIM , IMEI 등의 정보를 획득한다[14]. 이용자 식별정보 테이블에 함께 관리한다. 그리고 모바일전자고지문 발송 시 문자 이용자 단말기 여부 확인, 이용자 휴대전화번호 확인, 앱 인증 여부 확인 후 발신을 요청한 공공·행정기관의 전화번호, 안심마크 이미지, 그리고 이용자 인증을 위한 링크를 전송한다. 해당 링크는 모바일전자고지 인증서버로 연결되고 연결 시 기기인증 정보를 재확인하고, 대체수단 기반의 본인확인(최소 수행 시)을 거친 후 전자고지문을 열람하는 과정을 진행한다. 모바일전자고지 인증서버에 접근 시 이용자 인증과정을 최초에는 주민등록번호 대체수단 기반의 본인확인서비스를 적용하여 인증하고 이후에는 사용자가 지정한 인증방법, 핀 번호, 생체인증, 패턴 등을 선택적으로 사용할 수 있도록 하여 서비스 이용의 편리함을 제공한다. 따라서 모바일전자고지문의 위조 발송 시에도 수신한 이용자가 안심마크 확인, 발신인 전화번호 확인을 통해 위조 여부를 확인할 수 있으며, 실제 전자고지문 개봉 때에도 사용자 인증과정을 수행함으로써 타인의 불법적인 열람을 차단할 수 있다.

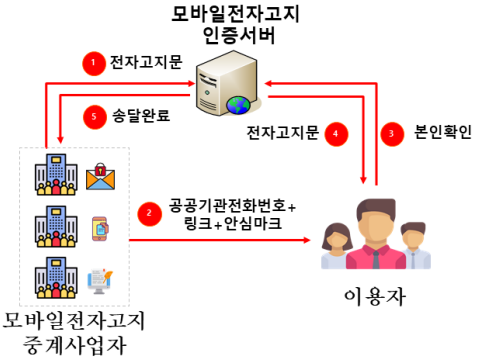


**그림. 8. 모바일 전자고지문 위변조 방지 방안**
**Fig. 8. Prevention of forgery and alteration of mobile electronic notice**

## Ⅳ. 결 론

본 논문에서는 공공·행정기관에 제공하는 모바일전자고서비스에 기술적인 안전성을 확보하기 위한 방안을 제안하였다. 온라인상에서 이용자를 고유하게 식별할 수 있는 연계정보(CI)의 사용을 최소화하고 모바일전자고지문 이용자의 확인 방법과 전자고지문의 위·변조 방지 방안을 제안하였다. 주민등록번호와 1:1 매칭되는 연계정보의 활용으로 명확하게 이용자를 식별할 수 있으나, 연계정보의 오남용으로 인해 개인정보가 침해되는 경우를 최소화하는데 목적이 있다. 제안한 방안에서는 연계정보를 사용하지 않고 안전하게 모바일 전자고지문을 해당 이용자에게 전송하는 방안, 전자고지문 열람 시 이용자 본인확인 처리 방안, 그리고 모바일전자고지문의 위·변조 방지를 수행하기 위한 방안을 제시하였다. 모바일전자고지를 위해 공공·행정기관과 전자문서중계사업자가 이용자를 식별하기 위한 정보를 공유해야 한다. 이를 위해 제안한 방안에서는 연계정보를 두 기관 간에 공유하는 비밀키를 사용하여 일방향으로 암호화한 G_DI를 생성한다. G_DI는 연계정보와 공공·행정기관 식별코드를 입력으로 생성된 암호화된 값이다. 그리고 전자문서중계사업자들 역시 보유하고 있는 연계정보를 본인확인기관에 제공하여 G_DI로 일괄변환을 수행한다. 이 과정은 전자문서중계사업자가 공공·행정기관과 모바일전자고지서비스 위탁계약 시 일괄변환 과정을 거침으로써 서비스 제공이 가능하다. 전자고지문의 최초 열람 시에는 대체수단 기반의 본인확인서비스를 적용하고 이후 서비스부터는 이용자가 설정한 인증 방법을 사용하여 열람하도록 한다. 그리고 전송된 모바일전자고지문의 위·변조 여부를 확인하기 위해 발송 공공·행정기관의 대표전화번호와 안심마크 이미지를 고지문에 함께 삽입하여 원천적으로 전화번호 발신지 변작 시도를 차단한다. 앱 기반 메시지 푸시서비스의 전자고지 경우에는 서비스 위탁계약 시 사전에 등록된 공공·행정기관명과 안심마크 이미지 함께 메시지 영역이 아닌 노출 화면의 부 영역에 포함하여 전송함으로써 악의적인 메시지와 구분할 수 있도록 한다. 현재는 공공·행정기관만 모바일전자고지서비스를 제공하고 있으나 올해 초 임시 허가된 민간·금융기관의 모바일전자고지서비스가 시행될 경우 현재보다 더 많은 연계정보가 활용될 것이다. 따라서 주민등록번호의 오남용에 따른 역기능을 확인한 바가 있어 사전에 연계정보의 오남용을 사전에 방지하기 위한 방안으로 본 연구의 의의가 크다고 할 수 있다. 제안한 방안을 모바일전자고지서비스에 적용함으로

써 현행 서비스 유형을 유지하면서 이용자 개인정보를 보호할 수 있는 장점을 가지고 있다. 향후 모바일전자고지서비스의 연동 과정을 표준화하여 신규 사업자들로 하여금 시장에 진입할 수 있는 방안을 마련하고자 한다.

## References

[1] ICT regulation sandbox, https://www.sandbox.or.kr/

[2] Internet World Stats (2020.07.20.) https://internetworldstats.com/asia.htm#kr

[3] J. B. Kim, "A Study on Improvement of Personal Identity Proofing Service(PIPS) Based on Alternative Methods of Resident Registration Number", Journal of The Korea Society of Digital Industry and Information Management, Vol. 15, No. 2, pp. 29-42, 2019. DOI: https://doi.org/10.17662/ksdim.2019.15.2.029

[4] J. B. Kim, "Safety Improvement Methods of Personal Identification Services using the i-Pin", Journal of Information Technology Services, Vol. 16, No 2, pp. 97-110, 2017. DOI: https://doi.org/10.9716/KITS.2017.16.2.097

[5] 방송통신위원회, 본인확인기관 지정 등에 관한 기준 고시, http://www.law.go.kr/행정규칙/본인확인기관지정등에관한기준

[6] Y. J. Shin, J. B. Kim H. Y, Han, Research on alternative means of resident number and research on improvement of certification procedure, KISA, 2015.

[7] J. B. Kim, "A Study on Differentiated Personal Proofing Service Based on Analysis of Personal Identification Requirements in Online Services", Journal of the Institute of Internet, Broadcasting and Communication, Vol. 20, No. 2, pp. 201-208, 2020. DOI: https://doi.org/10.7236/JIIBC.2020.20.2.201

[8] Y. J. Shin, S. H, Shin, J. S. Lee, W. K. Han, "A Study on Improvement of Identification Means in R.O.K", Journal of The Korean Association for Regional Information, Vol. 18, No. 4, pp. 59-88, 2015. DOI: https://doi.org/10.22896/karis.2015.18.4.003

[9] H. K, Lee, "The Problems and Reformation of the Personal Identification by the Resident Registration Number on the Internet", Hanyang Law Association, Vol. 23-1, No. 37, pp. 341-371, 2012. UCI: G704-001896.2012..37.005

[10] W. M, Sim, "Issues and Alternatives on Internet Identification: Analysis on the Basis of Architectural Regulation Theory", Korean Journal of Law & Society, Vol. 47, pp. 209-237, 2014. UCI: G704-001292.2014..47.004

[11] H. K, Choi, H. R. Kim, "Design and Implementation of a Malicious SMS Training System for Preventing Smishing", The Journal of KIIT., Vol. 17, No. 10, pp. 93-99, 2019. DOI: https://doi.org/10.14801/jkiit.2019.17.10.93

[12] J. K. Park,,"A Study of Realtime Malware URL Detection & Prevention in Mobile Environment", Journal of the Korea Society of Computer and Information, Vol. 20, No. 6, pp. 37-42, 2015.

[13] G. W, Seo, L. Y. Moon,, "A Study of Technical Countermeasure System for the Smishing Detection and Prevention Based on the Android Platform", Journal of Advanced Navigation Technology, Vol. 18, No. 6, pp. 569-575, 2014. DOI: https://doi.org/10.12673/jant.2014.18.6.569

[14] L. D. Nhac, N. T. Trang, N.T. Hau, N. H. Nam, G. S. Choi, "Detecting smartphone user habits using sequential pattern analysis", International Journal of Internet, Broadcasting and Communication, Vol, 7, No. 1, pp. 20-22, 2015. DOI: https://doi.org/https://doi.org/10.7236/IJIBC.2015.7.1.20

[15] S. H. Song, S. T. Kim, J. H. Shin, J. H. Lee, "Recovery Phrase Management Scheme for Public Blockchain Wallets based on OTP", The Journal of the Institute of Internet, Broadcasting and Communication, Vol. 20, No. 1, pp. 35-44, 2020. DOI: https://doi.org/10.7236/JIIBC.2020.20.1.35

[16] S. H. Kim, Y. G. Kim, "A Study on the Blockchain-based System Authentication Method", The Journal of the Institute of Internet, Broadcasting and Communication, Vol. 20, No. 1, pp. 211-218, 2020. DOI: https://doi.org/10.7236/JIIBC.2020.20.1.211

[17] S. J. Nam, S. T. Kim, J. H. Shin, "Context-Aware Mobile User Authentication Approach using LSTM networks", The Journal of the Institute of Internet, Broadcasting and Communication, Vol. 20, No. 1, pp. 11-18, 2020. DOI: https://doi.org/10.7236/JIIBC.2020.20.1.11

[18] H. I. Choi, I. U. Song, "The Mediating Effect of Self-efficacy between the Elderly's Digital Information Literacy and Life Satisfaction", Journal of the Korea Academia-Industrial cooperation Society, Vol. 21, No. 6, pp. 246-255, 2020. DOI: http://dx.doi.org/10.5762/KAIS.2020.21.6.246

## 저 자 소 개

김 종 배(정회원)

- 2000년 : 부산대학교 컴퓨터공학과 학사(공학사)
- 2002년 : 경북대학교 컴퓨터공학과 (공학석사)
- 2004년 : 경북대학교 컴퓨터공학과 (공학박사)
- 2006년 ~ 2019년 : 서울디지털대학교 컴퓨터공학과 교수
- 2019년 ~ 현재 : 세종사이버대학교 부교수
- 주관심분야 : 온라인서비스, 정보보호, 인공지능

※ This work was supported by the Technology Innovation Program(20011675) 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)