The Journal of the Convergence on Culture Technology (JCCT)
Vol. 9, No. 2, pp.483-491, March 31, 2023 pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2023.9.2.483
JCCT 2023-3-60

모바일전자고지서비스를 위한 민간기관과 공인전자문서중계사업자 간 연계정보 활용방안에 관련 연구

Study on Development of Technology Standards for Batch Conversion of CI between Private and Personal Identity Proofing Organizations for Safe Mobile Electronic Notification Service

김종배*

JongBae Kim*

요 약 모바일전자고지서비스는 이용자 소유한 모바일기기로 전자고지문을 발송하여 이용자의 수신 및 개봉 증명과 발송자의 송달 증명을 전자적으로 확인하는 서비스이다. 이로 인해 전통적으로 종이 기반의 고지 서비스가 전자고지문으로 급속히 대체되고 있으나, 이용자를 명확하게 식별하기 위한 연계정보가 필수적으로 사용된다. 연계정보는 온라인상의 주민등록번호와 같이 이용자를 고유하게 식별할 수 있는 정보로써 안전하게 활용하기 위한 방안 마련이 요구된다. 본 논문에서는 모바일전자고지서비스 제공에 있어 필수적으로 사용되는 연계정보를 사용하는 전자고지문 발송기관과 공인전자문서중계사자 간의 안전한 활용방안을 제안한다. 제안한 방안에서는 본인확인기관으로부터 전달받은 연계정보를 포함한 전자문서의 안전한 송수신 절차, 암호키 교환, 전자문서 열람 등을 통한 활용방안을 제시한다. 제안한 방안 공공·행정·민간기관의 모바일 전자고지서비스에 적용함으로써 보안 안전하고 체계적인 서비스 제공이 가능하고 서비스 확대를 통한 이용자 편익도 증가할 수 있다.

주요어 : 모바일전자고지서비스, 연계정보 활용방안, 전자문서 송·수신, 전자문서 보호

Abstract Due to the spread of mobile devices, the use of mobile electronic notification services is increasing. For the mobile electronic notification service, the connecting information is required to identify the owner of the mobile device and the recipient of the notification. The connecting information is an online resident registration number, and safe management is essential. Therefore, in this paper, the processing flow, interconnecting standard, and management plan are proposed when a mobile electronic notification requesting agency requests the identity verification agency to convert the resident registration number of the recipient of the electronic notification to connecting information. In the proposed method, it is suggested that a safe mobile electronic notification service is possible by defining the process of collective conversion of connecting information between private organizations and personal identity proofing agency, information transmission and reception methods, and interworking standards.

Key words : Mobile electronic notification service, Connecting information batch conversion service, Connecting information linkage standard

*정회원, 세종사이버대학교 소프트웨어공학과 교수
접수일: 2022년 11월 30일, 수정완료일: 2023년 2월 24일
게재확정일: 2023년 3월 8일

Received: Novemember 30, 2022 / Revised: February 24, 2023
Accepted: March 8 2023
*Corresponding Author: jb.kim@sjcu.ac.kr
Dept. of Software Engineering, Sejong Cyber Univ, Korea

Ⅰ. 서 론

모바일전자고지서비스는 그동안 수신자의 우편 주소 기반으로 종이 우편물을 발송하는 고지서비스에서 이용자가 소지는 모바일기기 정보 기반으로 전자문서를 발송하여 고지하는 서비스이다 [1-4]. 이때 발송기관이 수신자의 모바일기기 정보를 수집하거나 보유하고 있지 않아 직접적인 고지문 발송은 불가능하다. 따라서 이러한 전자고지문을 발송요청기관과 수신자(이용자) 간의 중계를 수행하는 공인전자문서중계자가 존재한다. 공인전자문서중계자는 이용자 가입 과정 등 통해 사전에 이용자의 개인정보를 보유하고 있어 전자고지문 이용자를 온라인상에서 식별할 수 있는 특징을 가지고 있다. 하지만, 전자고지문 발송요청기관은 수신자의 온라인상의 식별정보를 보유하고 있지 않아 기관이 보유하고 있는 정보를 기반으로 온라인상의 식별정보로 변환하는 것이 필요하다. 현재는 규제샌드박스를 통해 이용자의 직접적인 동의 없이도 모바일전자고지서비스와 마이데이터 서비스 제공자는 기관이 보유한 주민등록번호를 본인확인기관에게 제공하고 본인확인기관은 온라인상에서 이용자를 고유하게 식별할 수 있는 연계정보로 변환하여 제공한다 [5-7]. 다만, 해당 서비스 이용 시 수신자가 서비스 이용 시 사후 동의를 받도록 절차를 마련하고 있다. 모바일 전자고지문 발송을 원하는 발송요청기관은 공인전자문서중계자에게 연계정보와 발송 고지문 정보를 제공하여 수신자에게 발송을 요청한다. 2018년에는 공인전자문서중계자가 6개이었으나 2022년 현재는 11개로 중계사업자가 증가하게 되었다. 그만큼 전자고지문 수신자 입장에서는 선택지가 많아 다양한 공인전자문서중계사업자로부터 전자고지문을 수신할 수 있다. 하지만, 그 반대의 경우로 본다면 전자고지문 수신자의 연계정보가 다수의 공인전자문서중계사업자에게 제공하는 문제점이 있다. 즉, 이용자가 특정 공인문서중계사업자의 전자고지문 플랫폼에 가입하거나 소유하고 있지 않다면 해당 전자고지문을 열람할 수 없는 문제점이 있다. 그림 1과 같이 전자고지문 발송요청기관은 수신자가 해당 공인전자문서중계사업자의 플랫폼을 통해 미열람 시 다른 공인전자문서중계사업자로 연계정보와 전자고지문을 전송하여 재요청을 하게 된다. 이렇게 수신자가 공인전자문서중계자의 플랫폼을

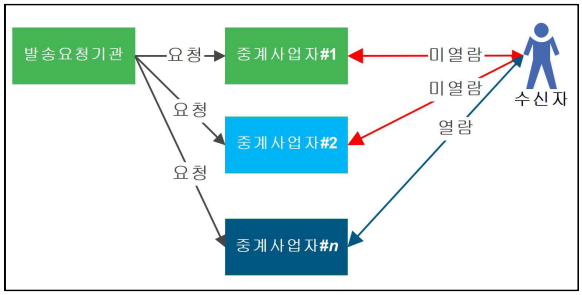

그림 1. 공인전자문서중계사업자 별 모바일 전자고지서비스 제공 현황
Figure 1. Status of provision of mobile electronic notification service by certified electronic document relay service provider.

설치 혹은 가입하지 않는 경우 발송요청기관은 다른 공인전자문서중계사업자에게 동일하게 발송 요청을 제공한다. 전자고지물 발송 요청 시에는 전자고지문 내용은 제공하지 않고 발송기관 서버에 저장하고 있는 링크를 보내어 전자고지문 송달 서비스를 제공하는 기관도 있으나 필수적으로 연계정보를 발송하는 것이 필요하다. 이러한 문제점을 해결하기 위해 2022년 08월 한국인터넷진흥원에서는 그림 2와 같이 공인전자문서중계사업자들 간의 연계정보 공유를 통해 수신자를 식별하고 전자고지문을 발송하는 통합 플랫폼 연계 방안을 추진할 계획을 제시한 바 있다[8]. 하지만 이러한 연계는 수신자의 연계정보를 공인문서중계사업자가 공유해 활용하는 것으로서 이용자의 동의 절차 없이 진행되는 문제점이 있으며 연계정보의 과도한 사용으로 인해 개인정보 침해 이슈가 발생한 가능성이 크다. 기존 연구[4, 5]들에서와 같이 연계정보는 88byte로 구성된 온라인상의 주민등록번호와 같이 고유하게 수신자를 식별할 수 있는 수단으로써 모바일전자고지 목적뿐만 아니라 비대

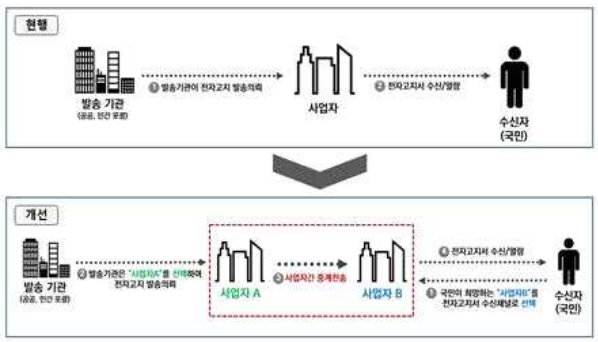

그림 2. 모바일전자고지서비스 개선 방안 (한국인터넷진흥원 [8])
Figure 2. Proposal for improvement of mobile electronic notification service.

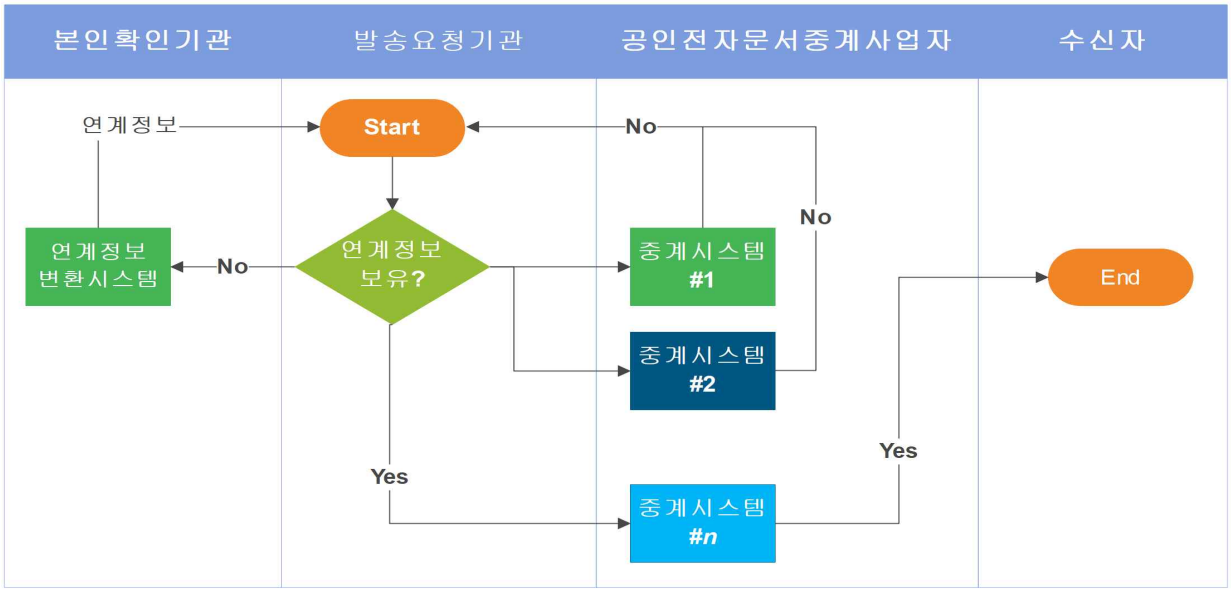

그림 3. 모바일 전자고지서비스 처리 흐름
Figure 3. Flow of mobile electronic notification service processing.

면 서비스에서 이용자를 식별하는 수단으로 다양한 분야에서 사용하고 있어 안전한 활용이 필요하다[9-11]. 이러한 원인에는 그림 3과 같이 모바일 전자고지서비스의 흐름도 구성에 있다. 발송요청기관은 연계정보 미보유시 본인확인기관에게 주민등록번호를 제공하여 연계정보를 일괄변환[2]하고, 이후 모바일전자고지서비스 목적으로 계약된 공인전자문서중계사업자들에게 순차적으로 연계정보와 발송하고자 하는 고지문을 제공하여 고지문 발송을 요청한다. 결국, 고지문 발송요청기관은 이용자가 어떤 중계사업자 플랫폼에 가입하거나 소유하고 있는 알 수가 없어 발생한 문제이다. 이를 해결하기 위해 중계사업자들 간의 연계체계 마련을 제시하고 있으나 궁극적으로 수신자를 식별하기 위한 개인정보인 연계정보의 공유 활용이 필요하다.

따라서 본 연구에서는 공공, 행정, 민간기관에서 모바일전자고지서비스 목적으로 수신자의 연계정보를 안전하게 활용하기 위한 모바일 연계정보 활용 서비스를 제안한다. 제안한 방안에서는 데이터 연계, 연계정보의 안전한 활용, 수신자 보호조치, 그리고 통신 구간의 보호조치 방안 등을 제시한다. 제안한 방안을 통해 안전하고 이용자의 정보가 보호될 수 있는 모바일 전자고지서비스의 활성화를 기대할 수 있다.

II. 모바일 연계정보 활용 서비스

1. 서비스 정의

모바일 연계정보 활용 서비스는 모바일 전자고지서비스에서 전자문서를 수신자에게 제공 시 수신자 식별 과정에서 안전하게 연계정보 활용하는 서비스이다. 모바일전자고지서비스는 그림 4와 같이 전자고지 연계 시스템, 수신자 식별 시스템, 전자고지 발송 시스템, 공인전자문서중계자 시스템으로 구분할 수 있다. 그림 4의 모바일전자고지서비스의 주요 시스템의 수행 역할은 표 1과 같다.

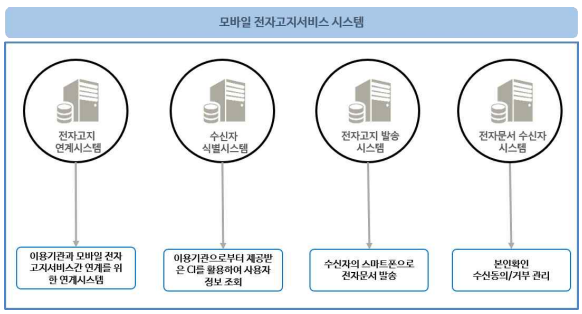

그림 4. 모바일 전자고지서비스 시스템 수행 역할
Figure 4. The role of performing the mobile electronic notification service system

본 논문에서는 모바일전자고지서비스에서 이용하는 연계정보 활용 서비스 제공 시 기본적으로 준수해야 할 기본 사항은 표 2와 같이 제시한다. 모바일 전자고지서비스 목적으로 기관 간 데이터 송수신 시 포함되는 연

표 1. 모바일 전자고지서비스 주요 시스템
Table 1. Main system of mobile electronic notification service

시스템명	설명
전자고지 연계 시스템	• 이용기관에서 모바일 전자고지서비스 이용을 위한 연계 서비스 제공 • 전자문서 송신요청 • 전자문서 송신, 수신, 열람 결과 확인 • 유통증명서 발급요청
수신자 확인 시스템	• 이용기관으로부터 전달받은 연계정보를 활용하여 수신자를 식별하는 시스템 • 송신요청의 연계정보로 공인전자문서중계자의 회원정보 조회 • 공인전자문서중계자의 가입자면 전자문서 송신 • 공인전자문서중계자의 회원이 아닌 경우 송신실패로 처리
전자고지 발송 시스템	• 전자문서의 송신과 관련된 기능 및 수신자의 전자문서 이용을 위한 기능을 관리하는 시스템 • 전자문서 송신 • 전자문서 송신, 수신, 열람 결과 관리 • 본인확인 서비스 관리 • 수신자 동의정보 관리 • 수신거부 해제·기타 관리
공인전자문서중계자 시스템	• 공인전자문서중계자가 전자문서 유통에 대한 증명 서비스를 위한 관리 시스템 • 공인전자주소 관리 • 유통정보 관리 • 유통증명서 발급 • 전담기관 연계

계정보의 암호화, 불필요한 정보의 차단, 통신 구간의 암호화 적용, 전자고지문 수신자 열람 시 본인확인, 수신자의 권리보호를 위한 수신거부 및 해제, 그리고 연계정보의 안전한 보관 이행을 준수하는 것을 제안한다. 모바일 전자고지서비스 생태계를 구성하는 각 구성원이 안전한 연계정보의 활용으로 개인정보의 침해 방지와 서비스 활성화를 꾀할 수 있다.

2. 서비스 프로세스

모바일 전자고지서비스의 주요 프로세스는 그림 5와 같이 구성되며 각 구성원들이 처리하는 주요 프로세스

표 2. 모바일 연계정보 활용 서비스의 기본 원칙
Table 2. Basic Principles of mobile connecting information utilization services

기본원칙	설명
데이터 송수신 연계정보 암호화	• 이용기관과 공인전자문서중계자 간 연계정보 정보교환 시 안전한 방법으로 암호화하여 전달 • 암호화에 사용되는 암호키는 주기적 갱신 (최대 2년)
불필요한 정보의 제한	• 이용기관은 공인전자문서중계자에게 정보교환 시 전자문서 송신을 위해 필요한 정보 외에 불필요한 정보 제공 금지 • 전자문서 송신을 위해 필요한 정보는 이용기관과 공인전자문서중계자 협의에 따라 관련법을 준수
통신구간 보호조치	• 이용기관과 공인전자문서중계자간 정보교환 시 통신구간의 보호조치 이행
본인확인	• 전자문서를 열람할 때는 반드시 본인확인을 통해 열람하려는 자가 수신자 본인인지를 반드시 확인 필요
수신거부	• 수신자는 전자문서의 수신 거부
수신거부 해제	• 수신거부를 한 수신자는 전자문서의 재수신을 위하여 수신거부 해제
연계정보의 보관	• 공인전자문서중계자는 연계정보를 보관하는 경우 안전한 방법으로 보관 및 관리 • 연계정보의 보유 및 이용기간은 관계 법령을 준수하여 개인정보처리방침을 수신자에게 고지
연계정보의 파기	• 공인전자문서중계자는 이용기관으로부터 전달받은 연계정보에 대해 이용목적 달성 시 즉시 폐기해야 한다.

들은 표 3과 같이 정의한다. 주요 프로세스들에는 암호화키 확인, 송신요청, 송신, 열람, 송신결과, 그리고 공인전자문서중계자 전담기관 연계 등의 프로세스로 구성

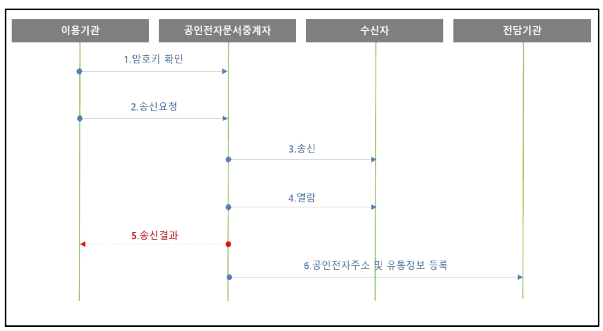

그림 5. 모바일 전자고지서비스 주요 프로세스
Figure 5. Flow of main Process of Mobile Electronic Notification Service

한다. 여기서 공인전자주소 및 유통정보등록 프로세스는 본 논문에서 다루지 않는다 [12, 13].

표 3. 모바일 전자고지서비스 주요 프로세스 및 설명
Table 3. Description of the main process of mobile electronic notification service

프로세스 명	설명
암호키 확인	• 연계정보를 암호화하기 위한 암호키 요청 • 공인전자문서중계자는 이용기관별 암호키 생성 및 이용기관에 제공 • 이용기관은 연계정보 암호화 전달
송신 요청	• 이용기관은 송신요청 연계규격에 따라 전자문서 송신요청 • 전자문서 송신요청 시 공인전자문서중계자가 수신자를 식별하기 위한 연계정보 제공 • 연계정보는 이용기관이 암호화하여 요청하고 공인전자문서중계자가 복호화하여 활용하는 방법으로 통신구간의 보호조치 적용
송신	• 공인전자문서중계자는 연계정보를 활용하여 수신자를 식별 밑 전자문서 송신
열람	• 수신자는 전자문서 열람 시 본인확인 수행 • 전자문서 수신자와 열람하려는 자가 일치하는지 여부 확인
송신 결과	• 공인전자문서중계자는 전자문서의 송신, 수신, 열람에 관한 결과를 이용기관에 제공

III. 모바일 연계정보 활용 세부 프로세스

3.1. 서비스 상태 확인 절차

모바일 전자고지서비스에서 연계정보를 활용한 서비스에는 수신자(이용자) 식별, 전자고지문 발송, 전자고지문 열람, 전담기관 연계 등으로 나열할 수 있다. 연계정보는 수신자를 식별할 목적으로 활용되기 때문에 전자고지문 수신자를 식별하는 용도로 활용한다. 이러한 연계정보 활용 서비스를 위해서는 전자고지문 발송요청기관(이용기관)이 공인전자문서중계자와 연계정보 제공이 필요하고, 공인전자문서중계자는 이용자 가입정보를 검색하여 전자고지문 수신자를 식별하는 프로세스 처리가 필요하다. 우선 그림 6과 같이 이용기관은 모바일 전자고지서비스가 이용 가능한 상태인지를 확인한다. 모바일전자고지문을 발송하고자 하는 이용기관은 공인전자문서중계자가 전자고지문과 연계정보를 수신할 수 있는 확인하는 과정으로써 공인전자문서중계자의 수신시스템에 정상적인 ACK 여부를 확인하는 프로세스이다. 서비스 상태 확인 프로세스는 모바일 전자고지서비스의 상태 확인을 요청하고, 서비스 상태정보 프로세스는 모바일 전자고지서비스의 상태정보를 이용기관에 제공한다. 각 서비스 상태 확인을 위한 서비스 연동규격은 표 4와 같이 정의한다.

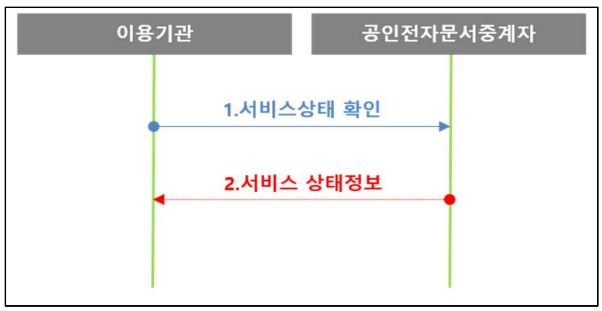

그림 6. 모바일 전자고지서비스 서비스 상태 확인
Figure 6. Process of checking the status of mobile electronic notification service.

표 4. 서비스 상태 확인 연동규격
Table 4. Integration specification for service status check

순서	항목	길이	설명
1	서비스 상태코드	4	서비스 상태 코드 ex)정상:0000, 오류:0001~9999
2	서비스 상태내용	200	서비스 상태에 대한 내용 ex)서비스 정상, 서비스 중지 등

3.2. 암호키 교환 절차

이용기관은 모바일 전자고지서비스를 위한 정보 송신요청 시 연계정보를 암호화하기 위한 암호키 확인 요청과 제공 프로세스를 진행한다. 그리고 이용기관이 공인전자문서중계자에게 전송하는 정보는 전자고지문과 연락처 수단 정보, 그리고 연계정보가 전송된다. 따라서 전송하는 정보에 대한 안전한 보호조치가 요구되고 이를 위한 암호화 등의 조치를 적용이 필요하다. 결국 두 구간 사이에 정보 전송 시 데이터 및 전송 시 암호화하는 것이 필요하고 암호화 시 요구하는 암호화키 교환 프로세스가 이행된다. 모바일 전자고지서비스 암호화키 교환을 위한 처리 프로세스는 표 5와 같으며, 암호화키 확인을 위한 연동규격은 표 6과 같이 정의한다.

3.3. 전자문서 송·수신 절차

표 5. 암호화키 교환 프로세스 및 설명
Table 5. Description of the cryptographic key exchange process.

프로세스명	설명
암호키 확인요청	• 이용기관은 연계정보 암호화를 위한 암호키 확인요청을 한다.
암호키 제공	• 공인전자문서중계자는 이용기관별 암호키를 생성하여 이용기관에 제공한다. • 이용기관에 암호키를 제공할 때는 이용기관의 공개키로 암호화하여 제공한다.

표 6. 암호화키 확인을 위한 연동규격
Table 6. Integration specification for encryption key verification.

순서	항목	길이	설명
요청정보			
1	이용기관 구분정보	20	이용기관을 식별할 수 있는 고유 식별 정보, ex)NP00000001
요청결과			
1	처리여부 코드	4	서비스 호출 정상여부 코드 ex)정상: 0000, 오류: 0001-9999
2	처리내용	200	서비스 호출 시 오류가 발생한 경우 오류에 대한 설명
3	암호키	30	CI를 암호화하기 위한 암호키 값

전자문서의 송신, 수신, 열람에 대한 절차와 각 절차에 따른 상세내용은 그림 7의 모바일 전자고지서비스 전자문서 송·수신 절차이며, 표 7의 모바일 전자고지서비스 전자문서 송·수신 절차 상세와 같이 절차별 상세내용에 대해 정의한다. 송신요청 프로세스는 이용기관이 공인전자문서중계자로 전자문서 송신을 요청하고, 전자문서 송신요청 시 연계정보는 암호화하여 전송한다. 이때 연계하는 항목에는 이용기관 구분정보, 송신식별정보, 연계정보, 전자문서 제목, 전자고지문 내용, 열람 마감일시, 전자문서 해시값 등을 포함한다. 송신 프로세스는 공인전자문서중계자가 연계정보를 활용하여 수신자를 식별하고 수신자의 스마트폰으로 전자문서를 송신하는 과정이다. 이때 송신하는 항목에는 전자문서 제목, 전자고지문 내용, 전자문서의 주소 등을 포함한다. 수신자 송신결과 확인 프로세스는 공인전자문서중계자가 송신한 전자문서의 송신, 수신, 열람에 관한 결과를 확인하는 과정으로 수신자에게 전자문서 송신한 결과를 확인한다. 수신자는 스마트폰에 전자문서가 수신된 결과를 확인하고 본인확인을 한 후 전자문서를 열

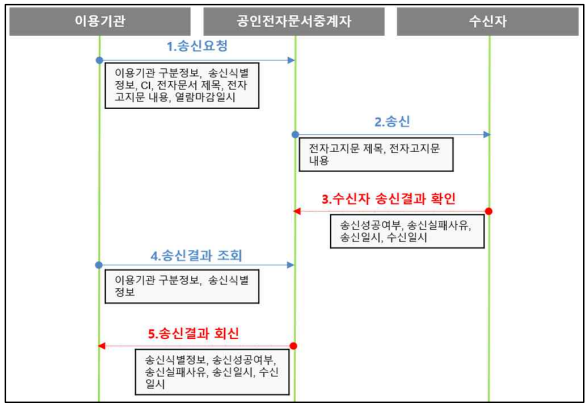

그림 7. 전자문서 송·수신 절차
Figure 7. Procedures for sending and receiving electronic documents.

람한 결과를 확인한다. 이때 확인하는 항목에는 송신실패 사유, 송신일시, 수신일시, 열람일시 등이 해당한다. 송신 결과 조회 프로세스는 이용기관이 전자문서의 송신, 수신, 열람에 관한 결과를 공인전자문서중계자로 요청하고, 이용기관이 송신요청 시 전자문서 단위로 생성한 송신식별정보를 이용하여 결과를 확인한다. 이때 연계하는 항목에는 이용기관 구분정보, 송신식별정보 등이 해당한다.

표 7. 전자문서 송·수신 결과 확인 연동규격
Table 7. Integration specification for confirmation of sending and receiving results of electronic documents.

순서	항목	길이	설명
요청정보			
1	이용기관 구분정보	20	이용기관을 식별할 수 있는 고유 식별 정보, ex)NP00000001
2	송신식별 정보	50	이용기관에서 전자문서 단위로 생성하는 고유 식별 정보
요청결과			
1	처리여부 코드	4	서비스 호출 정상여부 코드 ex)정상: 0000, 오류: 0001-9999
2	처리내용	200	서비스 호출 시 오류가 발생한 경우 오류에 대한 설명
결과내용			
	송신식별 정보	50	이용기관에서 송신요청 시 제공한 송신식별정보
	송신성공 여부	4	송신성공여부 ex)0000: 성공, 0001-9999: 실패
	송신실패 사유	200	송신실패사유 ex)단말기 수신불가 등
	송신일시	14	수신자 스마트폰으로 송신한 일시
	수신일시	14	전자고지문 수신한 일시
	열람일시	14	수신자가 전자문서를 열람한 일시

3.4. 전자문서 열람 절차

수신자가 전자문서 열람을 위해서는 반드시 본인확인을 해야 하며 공인전자문서중계자는 수신자와 열람하려는 자가 일치하는지를 확인하는 것이 필요하다. 따라서 전자문서 열람을 처리하기 위한 프로세스는 그림 8과 같다. 송신 프로세스는 수신자의 스마트폰으로 전자문서를 송신하는 과정이다. 본인확인 요청 프로세스는 수신자가 전자문서 열람을 위해서는 본인확인을 이행하는 것으로서 공인전자문서중계자가 수신자에게 본인확인을 할 수 있도록 관련 서비스를 제공한다. 이러한 본인확인 방법에는 휴대폰 본인확인, 지문인증, 패턴인증, PIN번호 인증, PASS 인증서 등으로 발송기관의 요구사항에 따라 달리 정할 수 있다 [14-16]. 수신자 본인여부확인 프로세스는 전자문서 수신자와 열람하려는 자가 일치하는지를 확인하는 과정이다. 그리고 전자문서 열람 프로세스는 본인확인이 성공하고 전자문서 수신자 본인일 때 전자문서를 열람하는 프로세스이다.

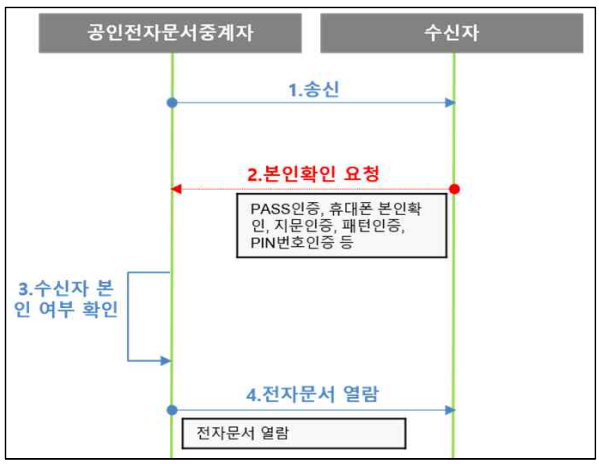

그림 8. 모바일 전자고지서비스 전자문서 열람 절차
Figure 8. Procedures for viewing electronic documents.

3.5. 연계정보 암호화 처리 절차

이용기관과 공인전자문서중계자 간 데이터 송·수신 시 연계정보를 암호화하는 절차는 그림 9의 모바일 전자고지서비스 암호화 처리 절차와 같다. 암호키 확인 요청 프로세스는 이용기관이 연계정보를 암호화하기 위하여 공인전자문서중계자로 암호키 확인 요청하는 과정이다. 암호키 제공 프로세스는 공인전자문서중계자가 연계정보 암호화에 필요한 암호키를 생성하여 이용기관에 제공하는 과정으로써 암호키를 제공할 때는 보안에 유의하여 비대칭 키 암호 방식을 사용하여 이용기관의 공개키로 암호화 후 제공하고, 이용기관은 암호화된 암호화키를 개인키로 복호화하여 사용한다. 연계 프로세스는 이용기관이 공인전자문서중계자로 데이터 전송 시 연계정보가 포함되면 공인전자문서중계자로부터 제공받은 암호화키로 암호화하여 전송하고, 공인전자문서중계자는 암호화된 연계정보를 복호화하여 사용한다. 그리고 이용기관과 공인전자문서중계자란 데이터 송·수신 시 연계정보의 암호화 방식은 속도에 유리한 대칭키 암호 방식을 사용한다 [17].

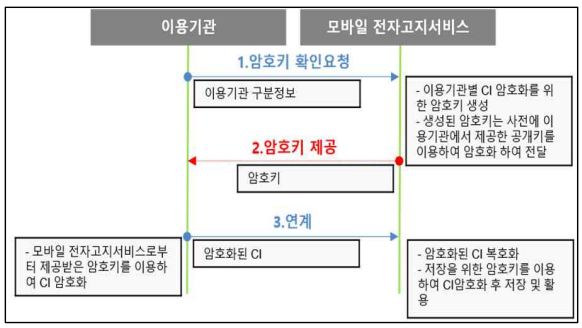

그림 9. 연계정보 암호화 처리 절차
Figure 9. Procedures for encryption processing of connecting information

3.6. 수신자 및 전자문서 보호 절차

모바일 전자고지서비스에서 가장 중요한 부분 중의 하나는 전자문서 및 수신자의 보호 방안이다. 수신자 보호 방안으로 전자문서의 위·변조 및 도용 방지, 본인확인 등이 있으며 공인전자문서중계자는 수신자 보호 방안에 대한 기능을 적용하여 수신자 보호조치를 이행할 필요가 있다. 전자고지문의 위·변조 및 도용 방지 방안으로는 공인전자문서중계자가 송신자 식별정보, 안심식별부호, 이용기관 검증 등의 있다. 따라서 공인전자문서중계자는 송신자 식별정보, 안심식별부호, 이용기관 검증 중 최소 1개 이상의 기능을 적용하여 전자문서의 위·변조 및 도용방지 조치를 적용한다. 송신자 식별정보는 공인전자문서중계자가 전자문서를 송신할 때 타인 도용이 불가능한 기능을 적용하여 수신자를 보호하는 방법들이다. 첫째로는 발신번호 변작방지(문자메시지) 서비스가 있다. 이동통신사의 발신번호 변작방지 기능을 이용하여 도용방지 조치를 하는 것이다. 휴대폰 문자의 경우에는 문자 발송 시 송신자의 번호를 임의로 변경할 수 없어 타인이 이용기관의 발신번호를 도용하여 문자 송신이 불가능하다. 두 번째로는 전용 메시지함을 사용하는 것이다. 모바일 전자문서 어플리케이션의 경우에는 공인전자문서중계자만 접근 가능한 모바일 전자고지서비스 전용 메시지함으로 전자문서를 송

신하는 방법으로 타인의 도용방지 조치가 가능할 것이다. 세 번째로는 안심식별부호를 전자문서에 함께 포함하는 것이다. 안심식별부호는 공인전자문서중계자만 접근 가능한 영역에 특정 마크를 표기하는 방법으로 공인전자문서중계자가 인증된 기관의 전자문서에만 특정 마크를 표기하기 때문에 일반사용자가 송신한 문서와는 구별할 수 있고 마크가 표기되는 위치는 공인전자문서중계자만 접근 가능한 영역이므로 타인이 도용하는 것이 불가능하다. 마지막으로는 이용기관 검증으로 수신자 보호를 이행할 수 있는데 공인전자문서중계자는 전자문서 송신요청에 대해 이용기관을 검증하여 허용되지 않은 기관이나 사용자의 송신요청을 차단하는 것이다. 이용기관 검증을 위해 접근토큰을 이용할 수 있으며, 이용기관이 서비스 이용요청 시 이용기관 구분정보, 접근토큰을 발급하고 송신요청 발생 시 이용기관을 검증하는 절차를 이행함으로써 안전한 모바일 전자고지서비스 제공이 가능할 것이다.

Ⅴ. 결론

본 논문에서는 모바일 전자고지서비스에서 발송요청기관(이용기관)과 공인전자문서중계사업자 간에 전자고지서비스 이용 시 이용자 식별을 위해 사용하는 연계정보의 안전한 관리와 전자고지서비스의 연계가 필요한 다양한 세부 프로세스들을 정의하고 연동규격을 제시한다. 모바일 전자고지서비스 제공을 위해서는 전자고지문 발송요청기관과 공인전자문서중계사업자가 서로 이용자 식별을 위한 연계정보 사용이 필수적이다. 하지만 이 연계정보는 온라인상의 주민등록번호와 같이 고유하게 이용자를 식별할 수 있는 정보로써 안전하게 관리하고 서비스에 활용 시 규격화된 연동기준에 따라 연계하는 것이 필요하다. 모바일 전자고지서비스는 ICT 규제개혁에 따라 규제샌드박스를 통과함으로써 이용자의 개인정보 제공에 사전 동의 없이 사후 동의로 고지문 발송 서비스가 가능하게 되었습니다. 하지만 이용자 개인정보에 대한 안전한 관리 방안 부재로 인해 모바일 전자고지서비스에 특화된 이용자 개인정보보호 방안과 서비스 안전성 확보를 위한 참여 기관 간에 서비스 연동기준 마련이 필요하다. 본 논문에서는 모바일 전자고지서비스 제공 시 발송요청기관과 공인전자문서중계자 간에 다양한 서비스 연계 시 필요한 연동 프로세스는 제시하고 연동 과정에서 연계정보의 보호 방안을 제시하였다. 기관 간 정보 연동 시 서비스 상태 확인 프로세스, 암호화 키 교환 프로세스, 전자문서 송·수신 프로세스, 전자문서 열람 프로세스, 연계정보 암호화 처리 프로세스, 그리고 수신자 및 전자문서 보호 프로세스를 제시한다. 세부적인 연동규격은 참여하는 기관들간의 서로 다른 시스템 정의에 따라 달리 처리할 수 있으나 전자고지문의 송·수신, 열람, 수신확인, 본인확인, 전자문서 보호 등을 위해서 최소한의 연동기준을 제시함으로써 안전하고 효율적인 모바일 전자고지서비스 제공이 가능할 것입니다. 다면 현재는 모바일 전자고지서비스 제공 시 이용자 개인정보의 변환과 활용에 있어 법적인 근거가 미비한 실정이다. 결국, 표준화된 서비스 가이드라인 혹은 기준 마련과 더불어 법적인 근거 확보를 통해 모바일 전자고지서비스 제공이 있어 강화된 요건을 요구하도록 참여 기관들에 적용할 필요가 있다. 향후 연구에서는 모바일 전자고지서비스 활성화를 위한 방안과 법적인 근거 마련을 위한 기초 연구를 진행하고자 한다.

References

[1] Mobile Electronic Notification Service, https://전자고지.kr

[2] 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.

[3] 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.

[4] J. B. Kim, “Electronic Notification Service in Public and Administrative Agencies”, Journal of The Institute of Internet, Broadcasting and Communication, vol. 20, no. 4, pp. 7-16, 2020.

[5] 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.

[6] 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 Korean Association for Regional Information Society, vol. 18, no. 4, pp. 59-88, 2015.
[7] K. H. Park, "A study on the improvement of personal identity proofing service using alternative method of resident registration number : focusing on guaranteeing user's right to control personal information", KonKuk University, M.S.Thesis, 2020.
[8] KISA, 모바일 전자고지 서비스 개편, 2022.08.03., https://www.etnews.com/20220803000120
[9] Y. S. Chio, Y. H. Lee, S. J, Kim, D. H. Won, "Security Analysis on the Implementation Vulnerabilities of I-PIN", Journal of The Korea Institute of Information Security and Cryptology, vol. 17, no. 2, pp. 145-185, 2007.
[10]H. B. Chang, C. M. Lee, S. Y. Cho, "A Proposal of Offline Identification Service using FIDO, NFC, and Blockchain", The Korean Institute of Communications and Information Sciences Winter Conference, vol 1, pp.141-142, 2022.
[11]I. Y. Chang, H. Y. Yum, "A study on the activation method of i-PIN, a means of identification on the Internet", Journal of The Korea Institute of Information Security and Cryptology, vol. 19, no. 5, pp. 81-94, 2009.
[12]S. M. Shim, "Electronic document distribution service based on authorized electronic addresses", The Korean Association of Computer Education Summer Conference, pp. 393-414, 2013.
[13]J. H. Park, "Study on the Secure Distribution and Storage of Financial institutions' documents-Focused on the authorized electronic address and the Certified e-Document Center System", Seoul Law, vol. 21, no. 3, pp. 347-388, 2014.
[14]J. Y. Lee, "A Proposal of Offline Identification Service using FIDO, NFC, and Blockchain", The Korean Institute of Communications and Information Sciences Spring Conference, pp. 620-623, 2022.
[15]J. H. Lee, H. K. Chi, "Password and Third Party Based Authentication for IoT", The Korean Institute of Communications and Information Sciences Winter Conference, pp. 424-425, 2018.
[16]S. S. Park, C. S. Oh, Y. K. Ryu, "Adaptive Hybrid Matching Method Using Filterbank and inutiae Information" The Journal of The Institute of Webcasting, Internet Television and Telecommunication, vol. 7, no. 1, pp. 47-52, 2007.
[17]H. R. Bae, M. Y. Kim, S. K. Song, S. G. Lee, Y. H. Chang, "Security Attack Analysis for Wireless Router and Free Wi-Fi Hacking Solutions", The Journal of the Convergence on Culture Technology, vol. 2, no. 4, pp.65-70, 2016.