The Journal of the Convergence on Culture Technology (JCCT)
Vol. 7, No. 3, pp.453-462, August 31, 2021. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2021.7.3.453
JCCT 2021-8-53

전자서명 기반의 주민등록번호 대체수단을 사용한 본인확인서비스 개선 방안에 대한 연구

A Study on the Improvement of Personal Identity Proofing Service Using an Alternative Method for Resident Registration Number Based on Electronic Signature

김종배*

Jong Bae Kim*

요 약 최근 전자서명법 개정으로 인해 공인인증서(현. 공동인증서) 지위가 만료됨에 따라 전자서명 기반의 공인인증서도 주민등록번호 대체수단에서 지휘가 상실되었다. 이로 인해 공인인증기관들은 방송통신위원회로부터 주민등록번호 대체수단 기반의 본인확인기관 지정심사를 통해 본인확인서비스 제공 기관으로 최근 지정받은 바 있다. 하지만, 기존의 주민등록번호 대체수단인 아이핀, 휴대폰, 그리고 신용카드들과 달리 인증서 발급 신청자의 신원확인 절차가 기존 대체수단들과는 상이한 부분이 존재하고 있다. 특히, 발급 신청자의 신원을 등록대행기관이 수행하고 있다. 본 연구에서는 전자서명 기반의 본인확인서비스 제공 시 대체수단 발급 과정에서 신원확인, 허무인 확인, 신원보증인 확인 등에 대한 개선방안들을 제안한다. 제안한 방안은 전자서명 기반의 본인확인서비스에 적용함으로써 이용자 개인정보보호와 보편·타당하고 안전한 본인확인서비스 제공이 가능함을 알 수 있다.

주요어 : 주민등록번호 대체수단, 본인확인서비스, 전자서명, 신원확인, 공동인증서

Abstract As the status of public certificates expired due to the recent revision of the Electronic Signature Act, electronic signature-based public certificates were also lost in the means of replacing resident registration numbers(RRN). As a result, public certification institutions have recently been designated by the Korea Communications Commission as identity verification service providers through a review of the designation of personal identity proofing agency based on alternative means of RRN. However, unlike existing RRN replacements such as i-PIN, mobile phones, and credit cards, the personal identity proofing process for applicants for certificates is different from existing alternatives. The proposed method shows that it is possible to protect users' personal information and provide universal, reasonable, and safe identification services by applying improvements to electronic signature-based personal identity proofing services.

Key words : Alternative means for resident registration number, Personal identity proofing service, Electronic signature, Public certificate

*정회원, 세종사이버대학교 소프트웨어공학과 교수 (제1저자)
접수일: 2021년 4월 10일, 수정완료일: 2021년 7월 15일
게재확정일: 2021년 7월 25일

Received: April 10, 2021 / Revised: July 15, 2021
Accepted: July 25, 2021
*Corresponding Author: jb.kim@sjcu.ac.kr
Dept. of Software Engineering, Sejong Cyber Univ, Korea

Ⅰ. 서 론

현재 인증서는 전자거래에서 사용자의 신원확인, 문서의 위·변조 예방, 부인방지 등의 목적으로 인증기관이 발행한 전자 신분증명서로 활용되고 있다 [1]. 인증서에는 전자서명 검증에 필요한 공개키에 사용자 정보를 추가하여 발행하며, 개인키와 한 쌍으로 존재하고 있다. 이러한 인증서 내에는 소유자명, 공개키, 인증서 발급자명, 유효기간 등의 정보를 포함하고 있는 일련의 데이터 구조를 신뢰할 수 있는 기관에서 자신의 개인키로 전자서명하여 발급한 정보를 저장하고 있다. 이때 신뢰할 수 있는 기관을 인증기관으로 칭하며, 국가가 지정한 인증기관을 공동인증기관(구. 공인인증기관)이라 한다. 인증기관의 역할은 전자서명 인증체계에서 인증서를 발급, 관리하는 서비스를 제공하는 기관이다. 결국 전자서명은 서명자를 확인하고 서명자가 전자문서에 서명하였음을 나타내는데 이용하기 위해 전자문서에 논리적으로 결합된 전자적인 형태의 정보이다 [2]. 이처럼 전자문서가 위변조가 발생하지 않았음을 보장하는 동시에 전자문서에 대한 사용자 인증, 무결성, 부인방지 등의 기능을 제공함으로써 온라인서비스에서 활발히 사용되고 있다 [3, 4].

그러나 2020년 12월 「전자서명법」 개정으로 약 20년간 유지되어 온 공인인증서의 법적 지휘가 상실되었다. 그동안 공인인증서가 온라인 시장에서 법적인 지배력이 확고하여 사설인증서(민간인증서)의 온라인 시장 진입에 어려움이 존재하였다. 이로 인해 신기술 발전이 저해되고 온라인 시장에서 신원확인의 독과점으로 귀결되어 더 이상의 새로운 신기술 개발 및 신규 방안 도입이 어려운 환경이 있었다. 현재는 관련 법 개정으로 공인인증서의 법적인 지휘가 사설인증서와 동일한 기준으로 사용자 인증, 본인확인, 전자서명 등의 서비스를 제공하게 되었다.

최근 5년간 공인인증서의 발급 건수를 비교하면 표 1과 같이 지속적으로 증가하고 있는 추세이다 [5]. 그만큼 시장에서의 지배력이 뛰어나다고 할 수 있으며 사설인증서의 시장진입이 어려움을 나타내고 있는 것이다. 사실 공인인증서의 사용처는 다양하게 존재하고 있으나 가장 많이 활용하는 것이 비대면 거래에서의 본인확인서비스이다.

표 1. 공인인증서 발급 건 수
Table 1. Number of public certificates issued

년도	2015	2016	2017	2018	2019
발급 건수	33,875,325	35,445,533	37,921,515	40,135,276	41,082,437

본인확인서비스도 다양한 수단을 활용하고 있는 상황에서 본 연구에서는 주민등록번호 대체수단을 활용한 본인확인서비스에 초점을 맞고 있으며 특히 전자서명 기반의 인증서를 이용한 주민등록번호 대체수단의 개선방안을 제시하고자 한다.

주민등록번호 대체수단 기반의 본인확인서비스는 그림 1과 같이 이용자가 소지하고 있는 주민등록번호가 포함된 신원정보 본인확인기관에게 제시하여 대체수단(본인확인정보: 아이핀, 휴대폰, 신용카드, 공동인증서)을 발급받는다 [6]. 그리고 이용자는 본인확인정보와 비밀정보를 본인확인기관에게 제시하여 자신임을 입증받은 후 본인확인기관이 인터넷 서비스 사업자(Internet Service Provider: ISP)에게 이용자의 개인정보(이름, 성별, 청소년여부 등)를 제공한다 [7].

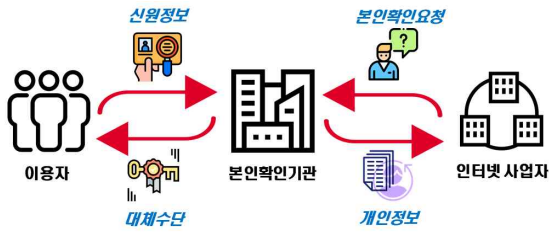

그림 1. 주민등록번호 대체수단 발급 흐름도
Figure 1. Flowchart for issuing alternative means of resident registration number

전자서명 기반의 인증서를 사용하여 본인확인서비스를 이용하는 경우는 이용자가 인증서 비밀번호를 입력하여 전자서명문을 생성하여 인증기관에 전달한다. 인증기관은 수신한 전자서명문에 이용자의 공개키로 확인하고 검증을 수행한다. 전자서명의 유효성이 확인되면 인증기관이 보유하고 있는 이용자의 개인정보를 본인확인서비스 요청자에게 제공한다 [8, 9].

본인확인기관이 ISP에게 제공하는 본인확인정보는 이름, 성별, 생년월일, 청소년여부, 내외국인 여부, 연계정보(Connecting Information: CI), 중복가입확인정보(Duplication Information: DI) 등이다 [10, 18]. 연계정

보는 식(1)과 같이 온라인상의 주민등록번호로써 주민등록번호와 일대일 매칭되는 88byte로 암호화된 정보이다. 생성 방법은 이용자의 주민등록번호(RN)과 패딩 정보를 연접하고, 연계정보 생을 위해 본인확인기관 간 공유한 비밀정보(SI)와 배타적 논리합으로 정보($Temp$)를 생성한다. 이후 본인확인기관 간 공유된 비밀 키(SK)를 이용해 해시값을 256비트 이상 출력값을 갖는 해시함수에 입력하여 해시 기반 메시지 인증 코드 값을 생성하여 연계정보를 획득한다 [11]. 기존 연구에서 제시한 바와 같이 연계정보는 결국 온라인상에서 유일하게 이용자를 식별할 수 있는 정보로써 무분별한 오남용을 방지할 필요가 있다 [12].

$$Temp = (RN \| padding) \oplus SI$$
$$\text{연계정보} = HMAC_{SK}(Temp) \quad (1)$$

그리고 중복가입확인정보는 해당 온라인 사이트에서 유일하게 이용자를 식별할 수 있는 64byte로 암호화된 정보로써, 연계정보 생성 시 온라인서비스 사업자(ISP)의 기관 코드를 추가적으로 삽입하여 생성한다. 결국, 해당 온라인 사이트에서만 이용자를 구분할 수 있는 정보로 활용된다. 하지만, 현재 온라인 시장에서 중복가입확인정보보다는 이용자를 유일하게 식별할 수 있는 연계정보가 널리 활용되고 있다.

이처럼 본인확인기관은 온라인 서비스 이용자의 진성 개인정보들을 제공함으로써 대체수단 가입 시 이용자 신원확인이 무엇보다도 중요하다. 현재 주민등록번호 대체수단을 이용한 본인확인서비스는 비대면 휴대폰 개통, 신용카드 및 통장 개설, 세금 정산, 공공 민원서비스 제공, 모바일전자고지서비스 제공 등 거의 모든 온라인 서비스에서 활용하고 있다. 그 만큼 보편적으로 온라인상에서 이용자를 식별하는 수단으로 자리 잡고 있다. 이전 연구를 통해 사회활동을 영위하는 국민들이 한해 동한 평균적으로 대체수단을 활용한 본인확인서비스 이용을 최소 40회 이상 수행함을 확인한 바 있다 [10, 12].

또한, 대체수단을 활용하여 본인확인서비스 사용 시 이용자의 실제 존재 여부 파악도 중요한 사항이다. 이용자의 진위 확인과 더불어 실존 인물인지 확인하는 것도 중요하다. 만약 존재하지 않는 이용자에 대한 본인확인서비스 제공 시 사회적으로 막대한 피해가 가져올 것이다. 예를 들어 실종자, 사망자, 국적포기자, 국적상실자 등 허무인의 경우 본인확인기관이 해당 이용자의 본인확인서비스 제공을 차단하거나 중지하는 방안 마련이 요구된다. 하지만, 민간 본인확인기관들이 현실적으로 허무인 여부를 실시간으로 파악하는 데는 한계가 있다. 근본적으로 본인확인업무가 필요한 원인에는 주민등록번호 수집금지에 따라 이를 대체하기 위한 수단이 필요하게 되었으며 국가가 이용자를 식별할 수 있는 수단의 활용 금지에 따라 민간기관에게 본인확인 업무를 위탁한 것이라 볼 수 있다. 이것이 본인확인기관 지정 제도이다 [13]. 그만큼 본인확인서비스는 대국민 보편·타당한 서비스로서 소외계층에 대한 서비스 이용권리 보장, 신뢰성 있는 서비스 제공, 차별 없는 서비스 제공 등이 요구된다.

현재 주민등록번호 대체수단에는 아이핀, 휴대폰, 신용카드, 그리고 공인인증서 발급기관들이 본인확인기관으로 지정받아 본인확인서비스를 제공하고 있다. 이중 공인인증서 기관들은 방송통신위원회의 본인확인기관 지정심사 없이 법적 의제에 따라 본인확인기관의 지휘를 부여받아 본인확인서비스를 제공하고 있었으며, 과학기술정보통신부의 관리·감독 하에 규제를 받고 있었다 [12]. 그러나 현 시점에는 공인인증서의 법적 지휘가 상실됨에 따라 자동적으로 본인확인기관의 법적인 의제에 따른 기관지정도 삭제되어 추가적으로 방송통신위원회에 본인확인기관 지정심사를 받아 본인확인서비스를 제공하는 것이 필요하다.

그림 2와 같이 인증기관에서 주민번호 대체수단인 인증서 발급 시 발급 신청자의 신원확인과 허무인 확인은 초기 발급단계에서 가장 중요한 사항이다. 하지만, 인증기관은 주민등록번호 대체수단이 인증서 발급 시 발급신청자의 신원을 직접 확인하지 않는 문제점이 존재한다. 즉, 인증서를 발급하는 인증기관이 확인하는 것이 아니라 등록대행기관(RA)이 신원을 확인하고 이용자의 이름과 주민등록번호를 인증기관에 제공하여 발급을 요청하고 있다. 예를 들어, 은행을 방문하여 인증서 발급 시 신원확인을 은행이 수행하고 이후 인증기관에는 연동전문으로 이름과 주민등록번호를 전달하여 인증서 발급을 요청하고 있다. 인증기관은 은행을 신뢰하여 추가적인 이용자 신원확인 및 허무인 여부 파악 없이 인증서 발급을 위한 참조번호와 인가코드를 전송한다. 참조번호는 가입자 식별 값이고, 인가코드는 인증

비밀번호이다 [14]. 참조번호와 인가코드 역시 인증기관이 발급 신청자에게 직접 제공하는 것이 아니라 등록대행기관에 전달하고 이를 이용자에게 제공하는 방식이다. 참조번호는 인증기관의 웹페이지에서 인증서 발급 요청 시 사용하는 정보이다.

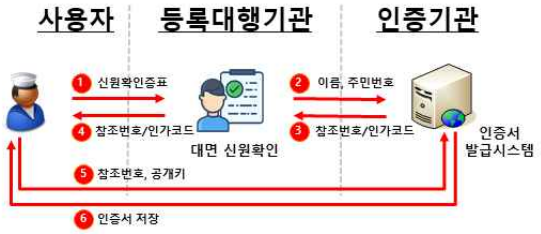

그림 2. 공인인증서 발급 처리 흐름도
Figure 2. Flowchart for issuing public certificates

따라서 현행 주민등록번호 대체수단으로 지정된 공동인증서가 본인확인서비스를 제공하기 위해서는 발급 신청자의 신원확인, 허무인 확인, 발급과정의 처리흐름, 이용자의 권리 보장 방안 등의 방안 마련을 통해 안전하고 신뢰성이 있는 본인확인서비스의 개선 방안 마련이 요구된다. 본 연구에서는 공인인증서 생성 시 포함된 전자서명 기반의 본인확인서비스 제공 시 기존 주민등록번호 대체수단과 비교하여 안전성을 개선하기 위한 방안을 제시한다. 또한 본 연구를 통해 전자서명 기반의 본인확인서비스의 안전성 확보와 이용자 보호 방안을 마련할 수 있다.

II. 주민등록번호 대체수단

1. 현황

주민등록번호 대체수단은 2012년부터 온라인상에서 주민등록번호 수집이 금지됨에 따라 주민번호를 대체하여 온라인 이용자를 식별할 수 있는 수단의 활용이 급격하게 증가하였다. 2006년부터 주민등록번호를 대체할 수 있는 아이핀(I-Pin)을 개발하여 시범서비스를 통해 주민번호 대체수단으로써의 활용을 확대한 바 있다. 방송통신위원회로부터 지정받은 주민등록번호 대체수단에는 현재 아이핀, 휴대폰번호, 신용카드번호, 그리고 공동인증서가 있다. 이용자가 주민등록번호 대체수단을 발급, 생성. 관리하는 본인확인기관에게 신원증표를 제시하여 신원확인을 통해 대체수단을 발급받아 온라인상에서 본인확인수단으로 활용하고 있다. 특히 최근 감염증 확산에 따라 비대면 거래가 폭발적으로 증가하고 있는 상황에서 상대방의 신원을 확인하는 서비스가 급증하고 있다. 최근에는 재난지원금 지급 등을 위한 신원확인, 이동경로 파악을 위해 신원확인 등에서 본인확인서비스가 활용되고 있다. 근본적으로 주민등록번호에 근간을 두고 사회적, 제도적, 관행적으로 온라인 서비스를 구성하고 있어 주민등록번호를 활용한 이용자 식별체계를 변경하는 것은 사회적인 비용 증가와 기존 소비자의 혼란이 가중 될 수 있다. 하지만, 주민등록번호 수집 금지에 따라 주민등록번호 체계가 아닌 이용자 식별방법의 도입이 검토되어야 한다. 표 2는 해외 국가별 개인식별번호 현황을 나타낸 것이다 [15]. 표와 같이 다양한 식별체계를 활용하여 온라인상에서 이용자를 본인확인하기 위한 방안의 마련도 필요하다.

표 2. 해외 국가별 개인식별정보 현황
Table 2. Status of personal identification information by foreign countries

국가명	개인식별정보
미국	사회보장번호(SSN)
독일	건강보험번호, 연금보험번호, 조세식별번호 등
영국	국민건강보험서비스(NHS) 등록 시 개인식별번호 부여
캐나다	사회보험번호(SIN)
일본	마이넘버
중국	주민번호(CIN)

2. 본인확인서비스

본인확인서비스는 비대면 환경에서 상대방의 신원을 신뢰할 수 있는 제3자에게 해당인이 본인임을 입증해 주는 서비스이다. 본인확인서비스 제공을 위해서는 이용자의 신원확인이 명확해야 한다. 또한 식별된 이용자를 구분하기 위해 발급 후 제공하는 대체수단은 유일하게 해당 이용자를 식별할 수 있어야 한다. 대체수단을 통해 이용자를 식별하기 위해 대체수단은 위·변조 방지는 물론 부인방지, 기밀성, 무결성, 가용성 등이 확보되어야 한다. 본인확인서비스 제공을 위해서는 제공기관이 보증하는 수단을 활용하는 것이 필요하다. 현재 국내에서는 방송통신위원회가 지정한 주민등록번호 대체수단 기반의 본인확인서비스가 있으며 사설 본인확인/인증서비스들도 존재한다. 둘 간의 차이점은 주민등록번호를 수집하여 이를 대체하여 유일하게 식별할 수 있는 연계정보와 중복가입확인정보를 생성할 수 있느냐가 차이점이다. 방송통신위원회는 본인확인기관으로

지정함으로써 연계 및 중복가입확인정보의 생성 혹은 발급 권한을 부여하는 것이라 할 수 있다. 또한 이러한 정보 생성을 위해서는 주민등록번호를 수집할 수 있는 법적 근거를 「정보통신망법」에서 확보하고 있는 차이점을 가지고 있다. 이로 인해 사설 본인확인/인증서비스는 국가가 지정한 주민등록번호 대체수단 기반의 본인확인서비스에 비해 온라인 시장에서의 확장이 어려운 것이 사실이다. 현행 대체수단 기반의 본인확인서비스 제공 시 간편인증 방식의 도입으로 이용자들이 손쉽게 본인확인서비스를 이용하고 있으며, 2020년 감염증 확산으로 인해 예년에 비해 본인확인서비스 이용건수가 증가하였다. 2019년 한 해 동안 온라인 시장에서 가장 많이 사용하고 있는 대체수단인 휴대폰 기반의 본인확인서비스의 인증건수가 약 16억 건에 이르고 있으며 2020년 1월-06월까지 휴대폰 기반 본인확인서비스 인증 건수가 약 10억 건에 이루고 있는 것을 볼 때 2020년 한 해 동안 휴대폰 인증건수만 약 20억 건에 이를 것으로 예측할 수 있다. 본인확인서비스 인증 건수는 아이핀, 신용카드, 공인인증서를 제외한 인증으로써 사회활동 국민 약 4천만명당 평균적으로 연간 약 50회 이상 본인확인서비스를 이용한 것으로 추정할 수 있다. 이렇게 주민등록번호 대체수단을 통한 본인확인서비스 인증건수가 높은 이유는 본인확인기관이 제공하는 개인정보가 유일하게 이용자를 식별할 수 있으며 국가가 보증하고 대다수의 인터넷 서비스 사업자(ISP)들이 활용하고 있어 서로 연계가 가능하다는 이유에 기인한다. 표 3은 본인확인기관이 인증 시 제공하는 정보들이다. 이처럼 주민등록번호 대체수단 기반의 본인확인서비스를 ISP들이 활용하는 이유는 본인확인기관이 이용자의 진성 개인정보를 표와 같이 제공해 주고 있으며, 본인확인기관에게 제공하며, 인증비용 역시 건당 20-40원 선으로써 수집하는 개인정보가 그 이상의 가치가 있고, 공신력 있는 본인확인으로써 법적인 이슈 발생 시 법적 대항력을 가질 수 있어 활용하고 있다.

3. 본인확인기관 지정 제도

주민등록번호 대체수단 기반의 본인확인서비스 제공을 위해서는 「정보통신망법」에서 규정한 본인확인기관 지정심사를 방송통신위원회부터 받아야 한다. 앞 절에서 언급한 바와 같이 본인확인기관은 이용자 신원확인과 대체수단 발급을 위해 주민등록번호를 수집할 수 있는 근거 마련과 이용자가 제공한 개인정보의 수집, 저장 및 제공까지의 역할을 수행한다. 현재 국내에 본인확인기관으로 지정된 곳은 표 4와 같이 다양한 기관들이 존재하고 있으며 이들 중 휴대폰 기반의 본인확인서비스가 온라인에서 약 95%이상 차지하고 있다.

표 3. 본인확인서비스 인증 시 ISP에게 제공하는 정보
Table 3. Information provided to the ISP when personal identity proofing service

제공정보	제공내용
이름	신원확인 수단을 이용한 본인확인을 수행하여 검증한 이용자의 실명
생년월일	신원확인을 한 이용자의 주민등록번호에서 추출한 8자리 정보
성별	신원확인을 한 이용자의 주민등록번호에서 추출한 1자리 정보
내외국인	신원확인을 한 이용자의 주민등록번호(외국인등록번호)에서 추출한 1자리 정보
연령대	신원확인을 한 이용자의 주민등록번호에서 추출한 정보를 분류하여 제공하는 8단계의 법적 연령대 1자리 정보
연계정보	서비스 연계를 위한 웹사이트간 공동 식별자로 88byte 암호화 된 정보
중복가입 확인정보	웹 사이트 내에서면 유일하게 이용자를 식별할 수 있는 64byte 암호화 된 정보
휴대전화 번호	휴대폰 본인확인서비스 이용 시 제공하는 이용자 휴대전화 번호
가입통신 사정보	휴대폰 본인확인서비스 이용 시 제공하는 이용자 휴대전화 가입 통산 정보

본인확인기관 지정에 있어 가장 중요한 사항은 신뢰할 수 있는 이용자의 신원확인 업무이다. 대체수단 발급 신청자의 신원확인을 명확하게 수행하고 이를 근거로 본인확인기관은 발급신청자로부터 개인정보를 수집·저장하고, 이용자가 본인확인서비스 요구 시 사전에 저장한 개인정보를 ISP에게 전달하는 업무를 수행한다.

표 4. 본인확인기관 지정 현황
Table 4. Status of designation of personal identity proofing service agency

대체수단	본인확인기관명
민간아아핀	나이스평가정보, 서울신용평가정보, 코리아크레딧뷰로
공공아이핀	한국지역정보개발원 (2018년 10월 신규발급 중지, 2021년 10월 서비스 중지 예정)
휴대폰	SKT, LGT, KT
신용카드	국민, 신한, 롯데, 현대, 하나, 비씨, 삼성, 농협카드
공동인증서	한국정보인증, 한국전자인증, 금융결제원, 코스콤, 한국무역정보통신

따라서 본인확인기관 지정심사 시 주안점은 신원확인 업무의 정확성, 신뢰성, 안전성, 보안성 등이 주요한 사항이다. 또한, 본인확인기관 지정 이후 이용자의 권리보장, 본인확인 인증정보의 열람권 보장, 개인정보의 안전한 보호조치 이행 등을 요구하고 있다. 그리고 본인확인기관 지정 이후에도 사후관리를 위해 심사기준에 따라 정기적인 본인확인서비스 적합성 심사를 매년 진행하고 있다.

III. 전자서명 기반의 본인확인수단

1. 현황

전자서명 기반의 본인확인수단은 전자거래에서 이용자의 신원확인 목적으로 발행한 전자 신분증명서이다. 전자서명 생성 시 이용자의 개인키를 전자서명 생성정보를 사용하고, 전자서명 검증 시 이용자의 공개키를 전자서명검증정보로 사용한다. 인증서에는 소유자명, 이용자 공개키, 인증서 발급자명, 유효기간, 그리고 데이터 구조를 신뢰할 수 있는 기관에서 자신의 개인키로 전자서명하여 발급한 데이터들 저장하고 있다. 그동안 표 4의 인증기관들이 공동인증서(구. 공인인증서)를 발급하여 본인확인서비스에서 활용하고 있다. 지금까지는 공동인증서 발행 기관들은 대체수단을 사용한 본인확인업무를 수행함에도 방송통신위원회의 적합성 심사를 받지 않고 있었다. 하지만, 2020년 12월부터는 4개의 공동인증기관(한국전자인증, 한국정보인증, 금융결제원, 코스콤)이 본인확인기관으로 방송통신위원회의 지정심사를 통과하여 본인확인서비스를 수행하고 있다. 공동인증기관 중 한국무역정보통신은 현재 본인확인기관 지정이 조건부로 통과하여 모든 조건이 해소될 시 까지 본인확인서비스를 제공하지 못하고 있는 상황이다. 그림 3은 공동인증서 기반의 본인확인서비스 흐름도를 나타낸 그림이다. 사용자는 등록대행기관을 통해 신원을 확인받아 인증서 발급 정보를 인증기관으로부터 전달받아 공동인증서를 생성한다. 이후 인증서를 사용하여 온라인 사업자들에게 제시하고 온라인 사업자들은 해당 인증서에 대한 유효성 검증을 인증기관에게 요구하고 그 결과에 해당하는 본인확인정보를 서비스 요청 사업자에게 제공하는 구조이다.

2. 문제점

그림 3과 같이 공동인증서 기반의 본인확인서비스 제공이 있어 기존 본인확인기관들과 대비하여 이용자의 신원확인, 허무인 확인, 이용자 권리보장, 열람권 제동 등에 대해 직접 수행하지 않는 문제점이 있다.

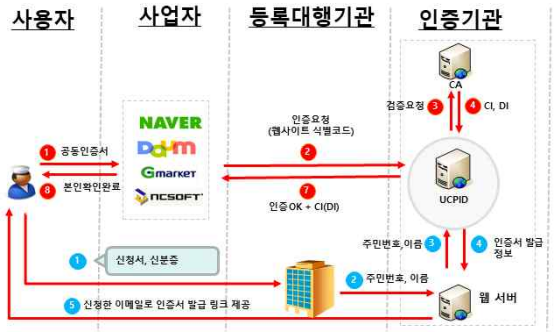

그림 3. 공동인증서 기반 본인확인서비스 흐름도
Figure 3. Flowchart of personal identity proofing service based on public certificate

1) 대체수단 발급 시 이용자 신원확인 기능 부재

전자서명 기반의 인증서 발급 시 이용자의 신원확인 업무를 인증서 발급기관이 직접 수행하지 않는 문제가 있다. 「전자서명인증업무준칙」에 따르면 인증기관의 신원확인 등의 등록업무를 등록대행기관에 위임할 수 있음을 규정하고 있다 [16]. 하지만, 본인확인기관 지정 기준에는 본인확인정보 발급 시 본인확인정보의 유일한지 검사 기능을 확보하도록 정하고 있다 [13]. 인증기관 업무 준칙상 신원확인 업무의 위임이 가능하나 본인확인기관 지정 기준상에서는 지정받고자 하는 기관이 직접 신원확인을 하도록 정의하고 있다. 현행 인증기관들은 인증서 발급 시 등록대행사가 대면을 통해 신원을 확인하고 이후 등록대행사가 전송한 발급 신청자의 이름, 주민등록번호만 수신하게 된다. 이처럼 인증기관은 실제 해당인이 발급 신청자 인지를 검증하기 위한 방안이 마련되어 있지 않는 상황이다.

2) 대체수단 발급 시 허무인 확인 기능 부재

인증서 발급 시 이용자의 신원확인을 직접 이행하지 않더라고 해당 이용자가 실제 존재하는 이용자인지 확인하는 과정이 요구된다. 본인확인기관 지정심사 기준상에 발급 신청자의 허무인 여부에 대한 검사 기능 마련을 요구하고 있다. 허무인은 사망자, 실종자, 국적상실자, 국적포기자 등과 같이 자신이 직접 본인확인을 수행할 수 없는 상황에 있거나 법적으로 실존하지 않는

사람을 의미한다. 본인확인서비스 요청자가 허무인인 경우 본인확인기관은 본인확인서비스를 제공할 수 없도록 정하고 있다. 이를 수행하기 위해서는 인증기관이 실시간 혹은 주기적으로 대체수단 발급자의 신원 상태 정보를 확인해야 함에도 이러한 절차가 마련되어 있지 않는 문제점이 존재한다. 다만, 대체수단 발급 과정에서는 사망자에 대한 여부를 실지명의 확인 과정에서 검증될 수 있으나 발급 이후 본인확인서비스 인증 시에는 검증하지 않고 있다.

3) 재외국민의 대체수단 발급 시 신원확인 기능 부재

재외국민이 대체수단 발급 시 해외 공관을 방문하여 여권을 통한 신원확인 과정을 거쳐 발급 서비스를 제공하고 있다. 해외 공관은 국가전산망 혹은 안전하게 보안 연결되어 있어 실시간으로 여권 소지자의 신원정보 확인 가능한 이점도 있으며 등록대행기관이 공공행정기관이고 신뢰성 있게 대체수단 발급자의 신원확인이 가능한 특징이 있다. 하지만, 실제 대체수단을 발급하는 인증기관에서는 발급신청자의 실물 신원확인 증표가 1년 이상 도래한 시점에 인증기관에 도착하는데 문제가 있다. 일반적으로 대체수단의 유효기간은 1년으로써 1년마다 갱신 과정을 거치게 된다. 재외공관에서 발급한 이용자의 경우, 갱신 시에는 자신이 직접 인터넷을 통해 별다른 확인 절차 없이 갱신이 가능함으로써 발급 시 신원확인이 이행이 중요한 상황이다. 또한 재외공관에서 대체수단 발급 시 범용으로 사용가능한 인증수단임에도 별도의 발급 비용을 징구하고 있지 않아 오·남용의 우려가 존재한다. 인증서 발급 기관인 공동인증기관에 실제 재외공관 발급 신청자의 실물 신원증표가 도달하는데 1년 이상 걸리는 원인으로는 재외공관에서 외교부 행랑을 통해 발송되고 이를 다시 한국인터넷진흥원으로 도달하여 각 인증기관에 송부함으로써 그에 소요시간이 1년 이상 발생하게 되어 발급 시점에는 신원확인이 불가능한 상황이다. 또한, 14세 미만의 아동이 인증서 발급 신청 시 법정대리인의 식별정보도 함께 전송되어야 하나 현재는 발급자의 식별정보만 인증기관으로 수신되어 법정대리인의 확인이 불가능한 상황이다.

4) 대체수단 이용자의 권리 보장 기능 부재

본인확인기관 지정 기준에서는 대체수단을 통해 본인확인서비스 중지 및 해지 기능 마련을 통해 이용자의 권리 보장 장치를 마련하도록 정하고 있다. 따라서 아이핀, 휴대폰, 그리고 신용카드 대체수단들에는 본인확인서비스의 중지와 해지 기능을 마련하여 해당 대체수단이 타인 등에 의해 오용되는 것을 차단할 수 있는 방안을 마련하고 있다. 그러나 전자서명 기반 인증서 대체수단은 본인확인서비스 중지 및 해지하기 위한 기능을 마련하고 있지 않아 이용자 스스로 권리를 추구할 수 있는 방안 마련이 부족한 상황이다.

5) 대체수단 인증이력에 대한 열람권 기능 부재

주민등록번호 대체수단을 사용한 본인확인서비스 이용 시 본인확인 인증 이력을 이용자에게 제공하도록 본인확인기관 지정 기준에서 정하고 있다. 그림 4와 같이 한국인터넷진흥원에서는 주민번호 대체수단이 아이핀, 휴대폰, 신용카드(2021년 하반기 연동 예정)를 사용한 본인확인 인증이력을 제공하고 있다 [17]. 인터넷 이용자들인 자신의 본인확인 인증이력을 확인하여 불필요한 인증이 존재하는지 혹은 특정 사이트에 가입되어 있는 등을 확인할 수 있으며 자신의 개인정보 보호를 위해 회원 탈퇴, 정보 파기 등을 요구할 수 있다. 하지만, 전자서명 기반의 인증서를 사용하여 본인확인서비스 이용 시 해당 정보가 연동되어 있지 않아 이용자는 자신의 인증 이력을 확인할 수 없는 상황이다 [1]. 설사 공공사이트에서 확인하는 것뿐만 아니라 인증기관에서 제공하는 본인확인 인증이력도 확인할 수 없는 상황이다. 이용자 입장에서는 대체수단 발급 후 미사용이나 혹은 노출에 의해 오·남용 될 수 있는 소지를 사전에 차단하기 위해 본인확인 인증 이력정보에 대해 확인할 수 있도록 방안 제시가 필요하다.

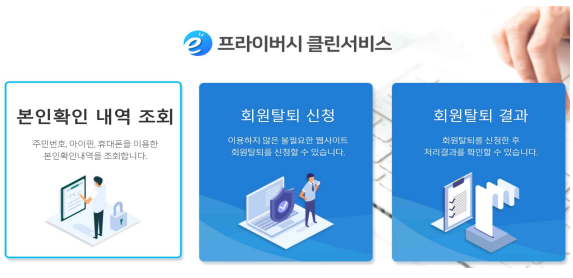

그림 4. 한국인터넷진흥원의 e프라이버시 클린서비스 화면
Figure 4. Korea Internet & Security Agency's e-privacy clean service screen

IV. 개선방안

전자서명 기반의 인증서를 활용한 본인확인서비스 제공 시 다양한 문제점을 개선하기 본 연구에서는 「정보통신망법」에서 정한 「본인확인기관 지정 기준」과 「전자서명법」에 따른 「공인인증업무준칙」을 비교하여 현실적으로 서비스 이용자의 혼란 없이 개선할 수 있는 방안을 제시한다.

1) 대체수단 발급 신청자의 신원확인 및 검사 수행

본인확인기관은 대국민 보편·타당한 본인확인서비스를 제공해야 한다. 이때 본인확인에 대한 신뢰성, 정확성, 신속성 등 보장되어야 한다. 실제 주민등록번호를 합법적으로 수집하고 이를 근거로 대체수단을 생성하여 본인확인서비스에 이용할 수 있도록 한 것은 국가 수행해야할 본인확인 업무를 민간 기관에게 위임한 것으로 볼 수 있다. 이로 인해 본인확인기관 지정심사 제도가 존재하고 있는 허가 제도로 유지하는 이유이기도 하다. 결국, 본인확인기관은 대체수단 발급 신청자의 신원을 직접 확인하고 실존인 인지를 검사해야 한다. 하지만, 현행 공동인증서 발급 시 이용자가 국내에 허가받은 5개의 공동인증기관 방문 후 대면확인을 통해 신원을 증명하는 것은 현실상 불가능한 일일 것이다. 또한 관련 법에 의거 등록대행기관이 신원확인 업무 수행이 가능함이 정의하고 있어, 신원확인과 인증서 발급 처리흐름상 오류가 발생하지 않도록 20년간 안정적으로 제도화된 것으로 인증기관이 직접 신원을 확인하도록 변경하는 것은 시스템 수정 비용과 사회적 비용이 과도하게 발생할 우려가 있다. 따라서 본 연구에서는 등록대행기관이 대체수단 발급 시 발급 신청자의 신원증표를 인증기관에 제공하여 직접 인증기관도 신원확인을 하도록 하는 절차 마련이 요구된다. 등록대행기관은 1차적인 대면확인을 통해 신원을 확인하고, 인증기관은 등록대행기관으로부터 전달받은 신원증표의 위·변조여부, 진위여부 등의 2차 신원확인을 수행한다. 이때 등록대행기관은 인증기관에서 신원증표 뿐만 아니라 이용자의 개인정보(연락처, 이메일 등)도 함께 전송하도록 한다.

그리고 이용자가 인증서 생성 시 인증기관 웹 사이트에 입력하는 참조번호와 인가코드를 등록대행기관에 제공하지 않고 이용자가 제공한 개인정보의 이메일 정보를 활용하여 인증기관이 직접 전달하도록 한다. 즉, 등록대행기관에게 이용자 인증서 생성 시 필요한 정보 제공을 최소화하는 것이다. 인증기관은 참조번호와 인가코드 열람 시 초기 이용자가 설정한 비밀번호 등으로 이용자 자신만이 식별 가능한 비밀정보를 활용하여 열람하도록 보안 조치 후 전송하는 개선방안을 제시한다.

2) 본인확인기관 간의 연계를 통한 허무인 확인 기능 마련

인증기관들은 현재 공식적으로 공공기관과 연계되어 실종자, 국적 포기자와 같은 허무인 여부를 실시간으로 확인하는데 한계가 있다. 즉, 행정안전부의 주민등록 DB, 출입국 정보 연동, 경찰청 정보 연동 등 대외 관련 기관들과의 개인정보 연동을 통해 허무인 여부를 지속적으로 확인하는 과정이 요구된다. 기술적으로는 어려운 일은 아니지만 현실적으로 여러 정부부처 및 공공기관들과 협의를 거쳐야 하며 공공의 이익과 개인 이익이라는 기준상에서 개인정보 제공에 대한 법적 이슈도 발생할 가능성이 있다. 현재 본인확인서비스에서 가장 중요한 정보는 주민등록번호와 일대일 매칭되어 생성하는 연계정보이다. 연계정보는 온라인상의 주민등록번호라고 언급한 바가 있다. 이처럼 연계정보를 생성할 수 있는 권한은 현재 아이핀 기관 3사만 보유하고 있다. 물론 과거 공동인증기관들도 보유하고 있었으나 본인확인기관 법적 의제기관에서 삭제됨으로써 연계정보 생성 모듈도 방송통신위원회가 회수하여 아이핀 기관과의 연계를 통해 연계 및 중복가입확인정보를 전달받도록 조치하고 있다. 이를 통해 통합한 정보 연동이 가능하고 향후 연계정보 변경 시 일괄적으로 정책을 적용할 수 있는 이점이 있다. 공동인증서 기반 본인확인기관들도 신규 본인확인기관 지정 심사를 통해 직접 연계정보 생성이 아닌 아이핀 기관에게 주민등록번호를 제공 후 연계 및 중복가입확인정보를 전달받도록 서비스 처리를 수행하고 있다. 이때 인증서 발급 시 허무인 여부를 아이핀 기관에게 확인하도록 하고 본인확인서비스 인증 시 아이핀 기관에게 허무인 여부를 확인 후 연계정보 제공을 받음으로써 일소에 허무인 검증 여부를 해결할 수 있다. 발급 신청자나 기존 서비스 처리 흐름, 대규모 변경 작업 없이 해결할 수 있는 개선 사항을 제시한다. 아이핀 기관들은 신용평가업무를 수행하고 있는 기관들로 신용DB 확인, 그리고 「정보통신망법」에 본인확인기관이 주민등록번호 DB 접근이 가능하도록 근거를 마련하고 있어 실제 주민DB를 통해 허무인 확

인이 가능하다.

3) 재외국민의 대체수단 발급 시 신분증표 실시간 전송 기능 마련

재외 공관에서 여권정보를 기반으로 대체수단 발급 신청 시 신청자의 신원정보(이름, 주민등록번호) 뿐만 아니라 신분증표도 함께 전송하도록 개선한다. 본인확인기관에서 직접 신분증표에 대한 진위확인을 실시간으로 수행하는 과정이 요구된다. 재외공관에는 인증기관간의 보안이 확보되는 팩스 등으로 전송함으로써 실현이 가능하다. 다만 해외 국가와 시차 차이로 인해 실시간 신분증표 검증이 현실상 어려울 것으로 판단된다. 그럼에도 불구하고 본인확인기관의 대체수단 발급 시 유일성에 대한 사후 검증을 위해서 수신 받는 것이 요구된다.

또한 만 14세 미만의 대체수단 발급 신청 시 인증기관과의 연동전문 상에 법정대리인의 개인정보(고유식별정보 포함)도 전송하도록 전문을 개선하도록 한다. 물론 개인정보수집 동의징구와 함께 신분증표도 함께 전송도록 개선할 필요가 있다.

4) 대체수단 이용자의 권리 보장 기능 마련

대체수단 이용자가 본인확인서비스의 중지 및 해지할 수 있는 기능을 인증기관 홈페이지 혹은 인증 앱 상에 구현하여 제시하는 방안을 마련하도록 한다. 대체수단의 기능이 신원확인과 같은 본인확인서비스에서만 이용하는 것이 아니라 부인방지, 전자서명 등에 활용하고 있기에 다른 서비스와 차별성을 가질 수 있도록 본인확인서비스의 중지 및 해지 기능 마련이 요구된다. 다만, 인증서의 경우 1년 혹은 3년 단위로 갱신 과정을 거쳐 장기간 미사용 시 자동으로 도태되도록 구현되어 있으나 실제 인증서를 통해 신원확인이 사회적인 파급력이 매우 높아 이용자가 본인확인서비스 중지 및 해지 기능을 마련함으로써 스스로가 자신의 권리를 확보할 수 있는 방안이 필요하다.

5) 본인확인 인증이력 정보의 열람 기능 마련

주민등록번호 대체수단을 사용하여 본인확인서비스를 제공받은 이력정보 제공은 본인확인기관 지정의 주요 요구사항 중에 하나이다. 그 이유는 얼마나 자신의 개인정보가 ISP 등에게 제공되었는지 확인할 수 있도록 본인확인 이력정보를 제공함으로써 회원 탈퇴 요구, 불필요한 개인정보 삭제 요구, 도용 등에 의한 부작용 최소화 등을 꾀할 수 있는 이점을 가지고 있다. 본인확인 인증이력정보에는 '언제, 어디서, 무엇을' 이란 정보들로 구성할 수 있으며, 예를 들어 어떤 인터넷 사이트에, 언제, 어떤 수단으로 본인확인을 시도하였는지 확인할 수 있다. 또한 본인확인 인증이력 정보에는 성공이력 뿐만 아니라 실패이력도 제공되어야 할 것이다. 본인확인서비스 실패이력을 통해 자신의 대체수단이 도용되었는지를 확인할 수 있으며 부정사용 시도에 대한 내역도 파악할 수 있는 이점을 가지고 있다. 이러한 본인확인서비스 인증이력 정보 제공은 각 대체수단을 발급하는 본인확인기관이 제공하는 것도 필요하지만 결국 연계 및 중복가입확인정보를 생성하는 아이핀 기관과의 정합성 검증에도 필요한 정보이다. 따라서 한국인터넷진흥원에 e클린서비스 [17] 연동을 통해 본인확인 인증이력 정보의 열람이 가능하도록 하고 대체수단을 제공하는 본인확인기관 자체 웹 페이지에서도 열람할 수 있는 방안을 제시한다.

Ⅴ. 결 론

본 연구에서는 주민등록번호 대체수단 중에서 전자서명 기반의 공동인증서(구. 공인인증서)를 사용한 본인확인서비스의 개선 방안을 제안한다. 전자서명 기반의 공동인증서는 방송통신위원회의 본인확인기관의 지정심사없이 법적인 의제에 따라 본인확인기관의 지휘를 부여받아 왔다. 그러나 「전자서명법」이 개정됨에 따라 공인인증서가 사설인증서로 전환됨으로써 법적 의제 조항에서 제외됨에 따라 전자서명 기반의 공동인증서를 사용한 본인확인서비스 제공 시 본인확인기관의 지정심사를 받아야하는 상황이다.

그동안 전자서명 기반의 공인인증서로 본인확인서비스를 제공하고 있었으나 「전자서명법」에 따른 법적 요구사항만을 준용하고 있어 주민등록번호 수집 근거 확보와 본인확인서비스 제공을 위해 「정보통신망법」에서 정의한 「본인확인기관 지정 고시」를 준용해야 한다. 따라서 전자서명 기반의 공동인증서를 사용한 본인확인서비스 제공 시 기존에 주민등록번호 대체수단들이 적용하거나 제공하고 있는 이용자 신원확인, 허무인 여부확인, 신원보증인을 통한 발급 시 절차, 이용자 권린 보

장, 그리고 본인확인 인증이력정보 제공 등의 대한 개선방안들을 제시한다.

본 연구를 통해 개선된 전자서명 기반의 본인확인서비스 제공으로 대국민 보편·타당한 역무를 제공하는 본인확인기관이 가능할 것이다. 또한 국내 주민등록번호 대체수단들이 준용하고 있는 법적 요구사항에 따라 본인확인서비스를 제공함으로써 이용자의 신뢰도 향상, 권리 보장, 안전성 강화 등을 꾀할 수 있을 것으로 사료된다.

References

[1] N. G. Kim and B. J. Cho, “A History Check System of Public Electronic Certificate using OCSP Service”, Journal of the Korea Institute of Information and Communication Engineering, vol. 20, no. 3, pp. 543-548, 2016. DOI: 10.6109/jkiice.2016.20.3.543

[2] https://www.law.go.kr/법령/전자서명법

[3] J. L. Zhang, “A study on application of digital signature technology”, Proc. of IEEE International Conference on Networking and Digital Society, vol. 1, pp. 498-501, 2010. DOI: 10.1109/ICNDS.2010.5479249

[4] E. Y. Lee, C. Shin, Baatdawa, “A study on the factors affecting the usage and diffusion of mobile easy payment services”. International Journal of Advanced Culture Technology, vol. 8, no. 1, pp. 38-43, 2020. DOI: 10.17703/IJACT.2020.8.1.38

[5] https://biz.chosun.com/site/data/html_dir/2019/10/11/2019101102528.html

[6] 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: 10.17662/ksdim.2019.15.2.029

[7] H. J. Lee, “The Improvement Plan of the Individual Information Protection of the Law on the Development of Cloud Computing and User Protection”, Journal of the convergence on culture technology, vol. 5, no. 1, pp. 219-226, 2019. DOI: 10.17703/JCCT.2019.5.1.219

[8] J. H. Kim, “A Legal Issues of Authentication and Electronic Signature on the Electronic Transactions,” Law Review, vol. 18, no. 2, pp. 59-103, 2018.

[9] J. W. Park, S. J. Kim, J. L. Lee, H. S. Lee, “Trend of standardization of identification technology using identification number in X.509 certificate”, Review of Korea Institute Of Information Security And Cryptology, vol. 14, no, 2, pp. 46-56, 2004.

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

[11]아이핀(i-Pin) 서비스 연계 정보 국가표준, KS X 3228-3, 방통통신표준심의회, 국립전파연구원 2012.

[12]J. B. Kim, “A Study on the Securing Technological Safety of Mobile 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. DOI: 10.7236/JIIBC.2020.20.4.7

[13]본인확인기관 지정 등에 관한 기준 고시, https://www.law.go.kr/LSW/admRulInfoP.do?admRulSeq=2200000038567

[14]The Reference Value/Secret Value Specification for Issuing Accredited Certificate, KISA, 2009.

[15]https://news.zum.com/articles/11356119?t=t

[16]전자서명인증업무준칙, https://www.rootca.or.kr/kor/accredited/accredited02.jsp

[17]e프라이버시 클린서비스, 한국인터넷진흥원, https://www.eprivacy.go.kr/mainList.do

[18]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: 10.7236/JIIBC.2020.20.2.201

※ 이 논문은 2021년도 산업통상자원부 규제샌드박스융합신제품인증기술개발사업의 지원(20016800)과 과학기술정보통신부와 한국연구재단 보조금에 의해 지원된 연구임 (NRF-2020R1F1A106890011)