The Journal of the Convergence on Culture Technology (JCCT)
Vol. 10, No. 5, pp.707-713, September 30, 2024. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2024.10.5.707
JCCT 2024-9-84

주민등록번호 대체수단별 발급·이용 시 이용자 신원확인 및 인증절차 분석 연구

A Study on the Analysis of User Identification and Authentication Procedures when Issuing and Using Alternative Means of Resident Registration Numbers

김종배*

J. B. Kim*

요 약 본 논문은 주민등록번호 대체수단의 발급·이용 시 신원확인 및 인증절차에 대해 현황을 분석하고 문제점의 개선 방안을 제안한다. 본인확인서비스 이용 과정에서 이용자의 개인정보보호와 권리보장이 필요하지만 근래에 만연해 있는 본인확인서비스의 확대로 인해 무분별하게 본인확인을 요구하고 있으며, ISP들도 신원확인 및 인증절차의 문제점 개 없이 활용에만 그치고 있다. 결국 온라인 서비스 이용자들은 자신의 개인정보가 과도하게 제공되고 있으며, ISP들은 본인확인서비스 요구에 따른 과금이 발생하고 있고 결국 온라인 서비스에 그 비용이 부가되고 있다. 따라서 본 논문에서는 주민등록번호 대체수단 발급·이용 시 이용자의 신원확인 및 인증 절차의 현황을 분석하고 문제점 개선방안을 제안한다. 제안한 방안을 통해 온라인 서비스 이용자들의 개인정보보호와 ISP들의 비용 절감, 그리고 온라인 서비스의 활성화를 꾀할 수 있을 것이다.

주요어 : 주민등록번호 대체수단, 본인확인, 본인확인서비스, 이용자 인증, 신원확인

Abstract This paper analyzes the current status of identity verification and authentication procedures when issuing and using alternative means for resident registration numbers and suggests measures to improve the problems. Users unconsciously use identity verification services by responding to identity verification requests from Internet service providers (ISPs). Ultimately, online service users are providing excessive amounts of personal information, and ISPs are charging fees for identity verification services, ultimately increasing online service costs. Therefore, this paper analyzes the current status of identity verification and authentication procedures for users when issuing and using alternative means for resident registration numbers and suggests measures to improve the problems.

Key words : Identity verification, Certification procedure, Alternative means, Personal identity proofing

Ⅰ. 서 론

정보기술이 고도화됨에 따라 오프라인이 아닌 온라인 서비스 제공 환경으로 변화하고 있다. 오프라인에서는 대면 확인으로 이용자 신원확인이 가능하였으나, 온라인에서는 신뢰할 만 한 제3자가 이용자의 개인신원에 대해 식별 및 인증해 주는 본인확인서비스가 등장하였다[1-4]. 본인확인서비스의 주요한 목적은 이용자 개인

*정회원, 세종사이버대학교 소프트웨어공학과 교수 (단독저자)
접수일: 2024년 7월 10일, 수정완료일: 2024년 8월 13일
게재확정일: 2024년 9월 10일

Received: July 10, 2024 / Revised: August 13, 2024
Accepted: September 10, 2024
*Corresponding Author: jb.kim@sjcu.ac.kr
Dept. of Software Engineering, Sejong Cyber Univ, Korea

의 신원을 확인하기 위함이다. 이때 개인 신원확인을 위해 이용자의 개인정보 수집과 검증 작업이 필수적이다. 개인정보는 개인을 식별하는 데 이용할 수 있는 정보로써, 대부분 국가에서는 정부가 국민에게 고유하게 부여한 식별정보(주민등록번호, 사회보장번호, 건강보험번호, 운전면허번호 등)를 활용한다. [5-7]. 이러한 개인식별증표 상에 표시되어 있어 정보는 개인을 식별할 수 있는 고유식별정보로써 다양한 곳에서 이용되고 있다.

사용자 식별이란 개인을 식별하기 위해 개인이나 혹은 제3자가 개인에게 부여한 정보이다. 대표적으로 사용자 ID, 계좌번호, 학번 등이 있다. 개인식별정보를 정당한 사람임을 증명하는 과정이 인증이다[8, 9]. 본인확인은 적법하고 합당한 절차에 따라 합의된 사용자라고 증명하고 인증하는 과정이고, 본인인증은 이용자의 전자적 정보를 통해 사용자가 실제 본인인지를 확인하는 과정이다. M. Zviran [10]과 Z. Erlich [11] 연구에 따르면 식별이란 "당신은 누구입니까?"라는 의미로 사용자 성명 및 ID를 의미한다. 하지만 이러한 식별정보만으로는 해당 사용자가 누구인지는 증명할 수 없다. 이는 해당 식별정보가 사용자 자신이 선택적으로 생성한 정보로써 실제 해당인인지에 대한 증명을 소유자 자신인 수행하는 것이 필요하고 이를 제3자가 확인하는 과정 혹은 검증하는 과정이 수반되어야 한다. 국내에서는 국민을 식별하는 수단으로는 주민등록번호가 있으나 온라인에서 법적인 수집 근거를 보유하지 않는 이상 수집이 금지되어 있어 온라인에서 이용자를 식별하기 위한 추가 수단이 필요하게 되었다[12, 13]. 더 이상 주민등록번호의 수집이 금지되고, 무분별한 사용 금지로 인해 2006년부터 새롭게 등장한 것이 주민등록번호 대체수단이다[14]. 이 대체수단은 정부가 허가한 본인확인 기관에서만 발급할 수 있는데, 이용자가 자신의 신원정보와 인증 방법을 본인확인기관에게 제공하고, 본인확인기관은 이용자에게 대체수단을 발급하여 온라인 서비스에서 이용자를 확인해 주게 된다. 현재 주민등록번호 대체수단들에는 아이핀, 휴대폰, 신용카드, 공동인증서, 그리고 전자서명 기반의 인증서 발급기관이다. 주민등록번호 대체수단 발급 업무를 수행하는 본인확인기관은 이용자로부터 주민등록번호를 수집 받아 일대일 매칭되는 연계정보와 중복가입확인정보를 생성하여 온라인 서비스 사업자(ISP)들에게 제공함으로써 이용자 신원확인과 인증을 수행한다[1]. 하지만, 국가가 허가한 주민등록번호 대체수단을 이용한 본인확인서비스로 인해 국내 ISP 사업자들의 온라인 서비스 제공 시 이용자 식별 및 인증 목적으로 온라인 서비스 이용자들에게 본인확인을 무분별하게 요구하고 있다[14]. 이로 인해 발생하는 문제점들은 다음과 같다.

이용자 측면에서는 과도한 개인정보 제공과 서비스 비용의 증가로 요약할 수 있으며, ISP 측면에서는 제공 서비스 이용 단가 증가와 본인확인 모듈의 관리 부재에 따른 보안 취약성을 들 수 있다. 그리고 정부 입장에서는 온라인 본인확인서비스 생태계의 다양한 기술 개발이 저해되고 본인확인기관에 대한 관리감독 비용 증가로 요약할 수 있다. 물론 주민등록번호 대체수단 기반의 본인확인서비스 제공으로서 ISP들이 중복으로 신원확인서비스 투자비용을 경감 할 수 있으며, 이용자들로 간편한 수단으로 손쉽게 신원을 확인받을 수 있는 이점도 존재한다. 최근에는 강화된 본인확인 요구에 따라 현행 본인확인서비스에서 이용자 신원확인에 대한 절차와 기술적인 문제점들을 개선하기 위한 요구사항이 증가하고 있다. 따라서 본 논문에서는 주민등록번호 대체수단 발급·이용 시 이용자 신원확인 및 인증 절차를 분석하고 문제점을 식별하여 개선 방안을 제안한다.

II. 주민등록번호 대체수단 서비스 현황 및 인증절차 분석

2.1 주민등록번호 대체수단의 정의

주민등록번호는 행정 목적상의 고유식별번호로서 해당 기관에서 사용자가 제시하는 주민등록증의 사진, 이름 등을 대조하여 본인확인 요소로 사용하고 있다. 그러나 주민등록번호의 무분별한 수집으로 인해 국민 대다수의 식별정보가 오·남용되는 문제점이 발생하자 더 이상 주민등록번호의 수집이 금지되어 사용자를 식별하기 위해 도입된 것은 주민등록번호 대체수단이다. 이러한 대체수단에는 아이핀, 공동인증서, 휴대폰, 신용카드가 있다.

2.2. 아이핀

아이핀은 인터넷상에서 대표적인 아이디와 패스워드를 사용한 지식 기반의 본인확인수단으로써 널리 활용되고 있다.

아이핀은 2005년 온라인상의 주민등록번호를 대체하

는 수단으로 신용평가기관을 통해 제공하게 되었다. 아이핀 발급·이용 방법은 인터넷 이용자는 아이핀 발급기관(본인확인기관)에 자신의 신원정보를 제공하고 휴대폰 또는 신용카드 인증을 통해 본인임을 확인받은 뒤 아이핀을 발급받을 수 있다. 표 1은 아이핀 기반 본인확인 서비스의 주요 현황이다.

표 1. 아이핀 서비스 주요 현황 분석
Table 1. Status of I-PIN service

항목	주요 현황
개념	ID와 PW를 이용한 본인확인서비스
확인방법	휴대폰, 공동인증서, 대면 확인
발급방법	발급 시 비대면, 방문을 통한 대면발급
관리기관	서울신용평가/NICE신용평가/코리아크레딧뷰로
신원확인 방법	아이디, 1차 / 2차 비밀번호 입력
장점	지식 기반의 서비스로 가장 간편한 접근
단점	• 온라인 대상자만 사용 가능 • 오프라인 발급 시 기관 방문에 어려움
고려사항	• 주민등록번호 수집(생성 시) • 변경 가능: I-PIN 아이디, 1/2차 비밀번호

2.3. 공동인증서

공개키 기반구조는 인터넷상의 거래 비밀을 보장하면서도 거래 당사자들의 신분을 확인시켜 주는 보안기술이다. 「전자서명법」에 근거하여 일종의 사이버인감증명서(서명용 개인키는 인감에 해당)로써 오프라인에서의 기명 서명과 동일한 법적 효력을 갖는다. 공동인증기관의 경우 전자민원, 연말정산, 주택청약, 전자세금계산서 등 비금융분야에서도 사용되고 있다. 하지만, 공동인증서 발급 시 특정 폴더에 저장하는 형태로 인해 해킹 등으로 폴더 복사를 통한 유출의 위험성이 존재한다. 그리고 해당 인증서는 항상 소지하고 있어야 하는 불편함이 존재한다. 현재는 소지하지 않고서도 서비스를 받을 수 있도록 클라우드 서버에 인증서를 저장하고 이를 활용하는 방식으로 편의성이 높아졌다. 현재는 간편인증 등을 통해 생체정보나 블록체인 기술을 접목하여 인증하는 서비스가 등장하고 있다. 표 2는 공동인증서 기반 본인확인 서비스의 주요 현황이다.

2.4. 휴대전화

휴대전화 인증은 휴대폰을 이용하여 일회용 숫자를 발송 후 입력하는 방법을 통해 본인여부를 확인한다. 최근에는 휴대전화를 이용한 본인확인 시 악성코드와 같은 해킹 링크가 포함한 SMS 인증문자를 발송하여 피싱이나 혹은 파밍 공격으로 본인확인서비스 이용자의 개인정보를 유출하려는 위험도 존재하고 있다. 최근에는 SMS 기반의 인증보다는 앱 기반 인증 서비스가 널리 활용되고 있는데 스마트폰의 탈옥 혹은 루팅 과정에서 악성앱들이 설치되고 본인확인서비스 시 개인정보 탈취가 되는 등의 위험성이 존재하고 있다. 표 3은 휴대전화 기반 본인확인 서비스의 주요 현황이다.

표 2. 공동인증서 서비스 주요 현황 분석
Table 2. Status of joint certificate service

항목	주요 현황
개념	사용자 신원확인을 위해 사용되는 증명서로 인증기관이 발행한 전자서명 인증서
확인방법	전자서명 인증서를 이용한 접속
발급방법	발급 시 대면확인, 갱신/이용 비대면
관리기관	한국정보인증/코스콤/금융결제원/한국전자인증/한국무역정보통신
신원확인 방법	전자서명 인증서와 개인키
장점	• 국제표준화 기술로 신뢰성 및 안전성 높음 • 금융거래 등에 활용 가능
단점	• 오프라인에서 적용 곤란 • 다양한 신원확인 수단 미제공 등
고려사항	• 주민등록번호 수집(생성 시) • 변경가능-년1회 갱신

표 3. 휴대전화 서비스 주요 현황 분석
Table 3. Status of mobile phone service

항목	주요 현황
개념	보유하고 있는 생년월일, 성명, 휴대폰번호를 이용한 인증 업무
확인방법	생년월일, 성명, 통신사, 휴대폰번호와 SMS 인증 문자 검증
주요정보	등록 시에 신청한 정보 활용
발급방법	발급 시 대면확인, 갱신발급 대면확인/비대면
관리기관	SKT, KT, LG U+
신원확인 방법	입력한 가입자 정보와 SMS 인증번호 입력
장점	• 언제, 어디에서나 편리하게 이용이 가능
단점	• 휴대폰 이용자에 한하여 활용가능
고려사항	• 주민등록번호 수집(등록 시) • 변경가능-신규 개설 시에만 변경

2.5. 신용카드

신용카드 기반의 본인확인서비스는 총 8자리 카드번

호를 입력하고 소유자의 휴대폰 번호를 입력한다. 이때 신용카드 소유자의 휴대폰 번호는 별도의 본인확인절차를 거친 정보가 아니라 신용카드 신청 시 신청자가 입력한 전화번호이다. 따라서 신용카드 기반의 본인확인서비스의 경우 신용카드번호와 결제용 카드 비밀번호의 함께 통신구간 상의 전송을 막기 위해 인증 창에는 신용카드번호 8자리, ARS를 통한 결제용 비밀번호 앞 두 자리만 입력받아 본인확인을 처리한다. 그리고 휴대폰을 소지하지 않은 이용자의 경우는 해당 신용카드사 홈페이지 회원가입을 통해 사전에 등록된 신용카드 정보를 사전 사용 등록 신청을 하고 이때 이용자는 홈페이지 ID와 PW를 입력하고 이후 사전에 등록한 신용카드의 유효기간, 결제 비밀번호, CVC 정보 입력을 통해 본인확인 처리가 가능한 방식을 적용하고 있다. 표 4는 신용카드 기반 본인확인 서비스 주요 현황이다.

표 4. 신용카드 서비스 주요 현황 분석
Table 4. Status of credit card service

항목	주요 현황
개념	보유하고 있는 신용카드정보를 이용하여 발급자 여부와 유효카드 여부, 앱카드 인증, ARS, 홈페이지 인증으로 검증하는 업무
확인방법	카드(카드번호 정보), 결재 비밀번호, 앱 인증, ARS 인증, 홈페이지 인증
발급방법	발급 시 대면확인 갱신발급대면확인/비대면
관리기관	카드발급업체(카드사 등)
신원확인 방법	카드번호, 비밀번호, 앱 인증, ARS 인증, 홈페이지 인증
장점	• 국내 카드사 대부분 처리 용이 • 별다른 단말기 소지 불필요 • 가입 및 유지 시 별다른 비용 미발생
단점	• 정보 노출 시 타인이용 가능 • 결제정보의 활용으로 유출 시 금전적 피해 가능성 높음
고려 사항	• 주민번호 수집(생성 시) • 변경가능-신규개설 • 성명, 주민번호, 카드번호, 비밀번호 • 금융거래에 활용 가능

2.6. 주민등록번호 대체수단 분석

주민등록번호 사용을 대신할 수 있는 본인확인수단 중 i-PIN은 가장 간편한 지식 기반의 인증 방법이다. i-PIN 기반 본인확인서비스는 주민등록번호를 사용하지 않고 ID와 패스워드를 사용하여 간편하게 본인확인을 수행하는 방법이지만 그만큼 보안의 위험성이 높은 문제점을 가지고 있다. i-PIN은 등록 후에 주민등록번호를 사용하지 않아 유출 위험을 줄일 수 있어 보안사고 대응이 용이하고, i-PIN ID 유출 시 재발급이 가능하여 안전한 인증이 유지되는 장점이 있다. 하지만 i-PIN 발급과정이 다소 불편하고, 타 시스템들과의 비연동에 따른 신원확인이 어려운 부분이 있어 불편하고, 사용자 특성에 따른 신원확인 방법 미 존재로 불편함이 존재한다. i-PIN 사용자의 등록 과정 및 절차상에서도 불편함과 패스워드 분실에 따른 문제도 대책이 부족하다. 이러한 문제해결을 방법으로는 패스워드 분실은 이차적인 패스워드를 지식 기반이 아닌 사용자가 선호하는 방법, 예를 들어 패턴, 문자, 그림, 숫자패드 등을 활용하는 방법, 신체정보 등 2차인증과 연계정보 활용, 간편한 등록 관리와 관리, 생체정보를 반영한 안전성 확보 및 사용상의 불편함의 해결 방안 마련이 필요하다.

휴대폰 기반의 본인확인서비스는 이용자의 생년월일, 성명, 휴대폰 번호, 그리고 가입통신사 정보를 기반으로 인증하는 수단으로써 사용이 다른 본인확인수단들에 비해 매우 편리하고, 전화 통화가 가능한 지역이면 언제/어디서나 이용이 가능한 장점이 있다. 또한 실시간 처리가 가능하고, 어린이와 어른들이 보편적으로 사용할 수 있고, 휴대의 안전성이 확보되고, 특별히 암기할 사항이 없는 장점이 있다. 그러나 도난 시에 타인에 의한 도용 우려가 예상되고, 휴대폰이 동작 시에만 사용할 수 있고, 분실 시에는 본인인증을 확인할 수 없으며, 불법적으로 타인 대신 본인인증이 가능한 우려가 있으며, 대포폰을 이용한 악용자들이 사용 시 적용 안 될 우려가 있다. 휴대폰 기반 본인확인서비스에 대하여 개선할 사항으로 도난/분실 시 신속히 불법 차단과 보안사고에 대비하여 본인확인을 위한 2차 팩터 인증 검토, 휴대폰 분실에 따른 위험 대비 필요 기능, 타인 도용에 따른 대비책 마련으로 보안성을 강화할 필요가 있다.

신용카드를 이용한 본인확인은 제화 결제용으로 발급받은 신용카드번호와 결제용 비밀번호를 이용하여 본인확인을 받는 서비스로써, 과거 신용카드 정보의 대량 유출로 인해 보안성을 강화한 방법으로 본인확인을 위한 대체수단으로 지정받았다. 신용카드 기반의 본인확인서비스의 보안성 강화 방안은 우선 ARS 인증을 통해 신용카드 정보의 일치성과 결제용 비밀번호의 입력을 위해 신용카드 가입 시 제시한 휴대폰으로 인증번호를 입력하는 방법으로 소지 여부 확인을 강화하였다.

그리고 스마트폰의 결재용 앱카드의 간편인증을 통해 Pin번호와 생체정보를 활용한 방식이 있으며, 추가로 휴대폰이나 인증서가 없이도 소지한 신용카드사 홈페이지 회원가입과 사전에 등록한 신용카드로 본인확인 서비스를 제공하는 방식이 있다. 지난해 확산했던 감염증으로 인해 전 국민 재난지원금 지급 시 신용카드 포인트 제공 시 인증 건수가 급격히 증가한 바 있다. 다만, 휴대폰 기반의 본인확인서비스에 비해 신용카드를 다시금 꺼내어 확인하는 등의 번거로움이 있으며, 또한 온라인 서비스 사업자들이 신용카드 기반의 인증 서비스 적용이 확산하지 못한 단점을 가지고 있다. 그러나 결제와 인증을 한 번에 처리함으로써 손쉬운 본인확인 방법이 될 수 있으며 신용카드 정보 역시 5년 단위에 재발급해야 함으로서 보안성이 높다고 할 수 있다.

전자서명 인증서는 인터넷상에서 본인의 신원확인을 위해 사용되는 증명서(인증서)로 인증기관이 발행한 인증서로 가장 안전한 본인인증 수단의 하나로 활용해 오고 있으며, 기업용, 개인용 등으로 구분하여 활용하고 있다. 기본적으로 대면을 전제로 안전하게 금융 업무를 처리하는 측면에서 다소 안전성이 있으며, 운영관리 기관의 공익성 있는 신뢰성이 있으며, 인증서/비밀번호로 이중적인 요소로 안전성을 확보하기 위한 강력한 본인인증, 명백한 본인인증 등 다양한 업무에 활용하고 있다. 한편, 전자서명 인증서는 인증서 휴대로 인한 불편요소와 유출에 따른 해킹으로 위험할 수 있으나 현재는 클라우드에 저장하여 소지의 불편함을 없앤 처리 방식도 서비스하고 있다. 또한, 1년마다 인증서 갱신에 따른 비용 발생과 패스워드 분실 시에 다시 발급받아야 하는 우려 사항과 별도의 저장매체를 이용하여 관리해야 하는 단점이 있다. 개선할 사항으로는 공인인증서의 안전/불편함을 극복할 수 있는 요소를 마련하고, 불법 유출에 따른 이용성을 배제하기 위하여 2차 3차 복합 인증을 이용한 개인정보 도용·유출에 대한 대책 및 2단계 인증과 결합한 대책을 마련할 필요가 요구된다.

2.7. 대체수단 발급·이용 시 신원확인·인증절차 분석

신원확인은 본인확인이 기본적으로 사항으로 일반적으로 대면확인을 통하여 이루어지고 있다. 공공 또는 민간 업무를 오프라인으로 처리할 때 목적에 따라 본인임을 확인하기 위해 국가가 발행한 신분증과 대면확인으로 신원을 확인한다. 신분증에서는 주민등록증, 운전면허증, 여권, 국가보훈증 등 신원확인 목적에 따라 활용하고 있다. 하지만, 대면확인 시 신분증을 항상 소지해야 하고, 만약 분실 시 타인에 의한 악용 가능성이 존재한다. 그에 반해 온라인상에서는 본인확인수단 즉 주민등록번호 기반의 대체수단들은 대면환경에서의 신분증표의 확인을 대체할 수 있어 많은 온라인 사업자가 활용하고 있다. 대표적으로 휴대폰 가입 시, 신용카드 발급 시, 전자서명 공동인증서 발급 시 등을 고려하면 신분증의 제시와 대면 확인을 전제로 한다. 하지만, 온라인 서비스의 급속한 확장으로 인해 온라인상에서 본인확인을 위해 대면확인에 준하는 수준으로 신원을 확인하는 것이 요구되고 있다. 대면확인에 준하는 사항이란 신분증과 주민등록번호 대체수단들을 복합적으로 인증하여 신원을 확인하는 것이다. 특히 금융업권에서는 계좌번호 인증, ARS 인증, OTP 인증, 거래내역 인증, 법정 대리인 인증 등을 복합적으로 적용하여 신원확인 및 인증에 활용한다. 표 5는 주민등록번호 대체수단 발급 및 이용 시 인증 절차를 분석한 것이다. 표 5은 본인확인수단별 발급과 이용 시 신원인증 및 인증절차를 정리한 것이다.

III. 결 론

본 논문은 주민등록번호 대체수단 기반의 본인확인서비스의 이용을 위해 본인확인수단의 발급과 이용 시 신원확인 절차와 인증 방법들에 대해 현황을 파악하고, 본인확인수단의 개선사항을 제시하였다. 아이핀 서비스는 지식 기반 본인확인수단으로써 간편한 인증과 더불어 발급 과정 역시 절차가 간단하다. 비대면 발급을 전제로 자신 명의 휴대폰만 있으면 발급이 가능한 상황으로 이제 더 이상 유효기간제 적용도 폐지되어 장시간 미사용 시 휴면계정 전환도 불가하고, 빈번하게 사용하지 않을 시 패스워드 분실에 따라 재인증 절차의 번거로움, 2차 인증의 번거로움으로 인해 그 활용 빈도가 점차 떨어지고 있다. 그럼에도 불구하고 사회적 약자들을 위해서는 꼭 필요한 본인확인수단으로써 문제점들을 개선하기 위한 노력이 필요하다. 지식 기반의 수단으로써 문자 기반의 아이디와 패스워드에 국할 필요가 없이 그림이나 패턴, 연상할 수 있는 도구, 음성, 몸짓 등 서비스 이용자가 기억하며, 편의성의 높은 본인인증 방법을 적용할 수 있는 방안 마련이 필요하다.

표 5. 대체수단 발급 시 신원확인 및 이용 시 인증 방법 비교
Table 5. Comparison of authentication methods for personal identity proofing and use when issuing alternative means.

인증절차 / 대체수단	발급		이용	
	신원확인	법적근거	일반인증	간편인증
i-PIN	이름, 주민등록번호 휴대전화, 전자서명, 신용카드	• 「본인확인기관 지정 등에 관한 고시」 • 「전자금융거래법」 제6조(접근매체의 선정과 사용 및 관리) • 「전자금융거래법 시행령」 제6조(접근매체의 갱신·대체발급 및 반환)	ID/PW/그림문자/2차PW	QR스캔+지문 / 앱인증+지문
휴대폰	이름, 주민등록번호 전자서명, 신용카드	• 「전기통신사업법」 제32조의4(이동통신단말장치 부정이용 방지 등) • 「전기통신사업법 시행령」 제37조의6(계약 체결 시 본인확인) • 「전자서명법」 제2조제2호(전자서명) • 「금융실명거래 및 비밀보장에 관한 법률 시행령」 제3조(실지명의)	이름, 생년월일, 성별, 전화번호, 가입통신사, SMS OTP	USIM / PIN / 지문
신용카드	이름, 주민등록번호 전자서명, 휴대폰	• 「여신전문금융업법」 제14조(신용카드·직불카드의 발급) • 「여신전문금융업법시행령」 제6조의7(신용카드의 발급 및 회원 모집 방법 등) • 「신용정보의 이용 및 보호에 관한 법률 시행령」 제30조제3항(신용정보 이용 미 제공사실의 조회 등) • 「전자금융거래법」 제6조(접근매체의 선정과 사용 및 관리) • 「전자금융거래법 시행령」 제6조(접근매체의 갱신·대체발급 및 반환)	발급회사, 신용카드번호, 유효기간, 비밀번호, ARS, 홈페이지 ID/PW	앱인증 / PIN / 지문
인증서	이름, 주민등록번호 휴대폰, 신용카드, 아이핀	• 「전자서명법」 제7조(전자서명인증업무 운영기준 등), 제14조(신원확인) • 「전자서명법 시행령」 제9조(신원확인의 방법) • 「전자서명법 시행규칙」 제5조(실지명의 기준의 신원확인 방법) • 「전자금융거래법」 제6조(접근매체의 선정과 사용 및 관리) • 「전자금융거래법 시행령」 제6조(접근매체의 갱신·대체발급 및 반환)	전자인증서/비밀번호	전자인증서/PIN / 지문

휴대폰 기반의 본인확인서비스에서는 비대면 발급 시 신원확인의 절차를 강화하는 것이 필요하다. 현재는 휴대폰 서비스 개통 시 필수적으로 본인확인서비스 가입을 동의하도록 규정하고 있다. 또한 휴대폰을 통한 본인인증 방법 역시 SMS 문자 인증 혹은 앱 인증만 존재하고 있어 다양화할 필요가 있다. 즉 본인확인서비스 이용자가 선호하거나 보안성이 강화된 방법으로 적용할 수 있도록 인증수단의 확대가 필요하다. 예를 들어 휴대폰 본인확인서비스의 사용자 인증 시 금융 OTP, 패턴, 음성, 얼굴, 사진인증 등으로 현행 SMS나 앱 기반의 인증 외 다른 수단을 사용자가 선택할 수 있도록 확대하는 것이 필요하다.

신용카드 기반의 본인확인서비스는 카드의 소지 번거로움, 카드정보 입력의 불편함, 신용정보 제공에 따른 위험성 등의 불편함이 존재한다. 이를 개선하기 위해 앱 카드 기반의 인증 방법을 적용하고 있으나 이 방법은 결국 스마트폰을 소지하고 모바일 앱을 설치하는 과정이 수반되어야 한다. 물론 신용카드와 스마트폰으로 지식과 소지라는 2차 인증의 강화라는 안전성은 있을지라도 사용의 불편이 가중되고 있어 이를 해소할 필요가 있다. 따라서 신용카드 기반의 본인확인수단 발급 시 비대면 발급 과정에서 강화된 인증 방법을 추가하는 것이 필요하다. 주민등록증 혹은 운전면허증 발급일자 대조와 더불어 얼굴인증, 계좌인증, 타 신용카드 정보의

유효성 검증 등을 수행하는 것이다. 그리고 인증 시에는 최근 카드승인 금액, 거래 업종, 납부은행 등 KYC 정보를 활용하는 것이다.

마지막으로 인증서 기반의 본인확인서비스는 다른 수단들에 비해 대체로 강화된 발급절차를 적용하고 있다. 발급 과정에서 대면확인이 필수적이나 일부 등록기관에서 신원확인 절차의 강화가 요구되고 해외 거주자들이 재외공관에서의 발급 시 신원확인의 강화가 요구된다. 그리고 인증 시에서는 현재는 인증서를 소지하거나 클라우드에 저장한 인증서로부터 비밀키를 입력하는 방법만 존재하고 있으나 비밀키 외의 사용자가 추가적 인증수단을 적용하여 다양한 방법들로부터 사용자의 신원확인 및 인증 방안의 확대가 필요하다.

본 연구를 통해 현행 주민등록번호 대체수단 기반의 본인확인서비스 이용 시 본인확인수단의 발급과 인증 현황을 분석하고, 수단별로 신원확인 및 인증 시 사용의 편의성과 보안성을 강화할 수 있는 개선 방안을 제시함으로써 안전한 본인확인서비스가 가능할 것이다.

References

[1] J. B. Kim, “A Study on Improvement of Personal Identity Proofing Service 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 : 10.17703/JCCT.2021.7.3.453

[2] G. 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”, M.S. Thesis, KunKook University, 2020.

[3] H. B. Jang, C. M. Lee, S. H. Cho, "A Proposal of Offline Identification Service using FIDO, NFC, and Blockchain", Pro. of Korea Institute of Information and Communication Engineering, Vol. 1, pp. 141-142, 2022.

[4] W. G. Jung, G. L. Han, H. C. Park, J. B. Kim, "A study on the analysis of usage status of personal proofing service based on resident registration number in the COVID era", Pro. of KIICE., Vol. 1, pp. 313-314, 2022.

[5] U. M. Kim, "Current status and future of Japan's personal identification and identity verification system", Local information magazine, Vol. 86. pp. 96-101, 2014. DOI : 10.17703/JCCT.2021.7.3.453

[6] L. J. Hwang, "Personal identification and authentication methods in the United States", Local information magazine, Vol. 86, pp. 78-81, 2014.

[7] L. H. Lee, "Germany, various methods for self-authentication and personal identification", Local information magazine, Vol. 86, pp. 82-89. 2014.

[8] J. O. Ha, H. J. Cho, K. S. Nam, J. K. Lee, CISSP notes from information security experts, Inforthebooks, 2016.

[9] H. J. Mun, "A Study on the User Identification and Authentication in the Smart Mirror in Private", Journal of Convergence for Information Technology, Vol. 9, No. 7, pp. 100-105, 2019. DOI : 10.22156/CS4SMB.2019.9.7.100

[10]M. Zviran and Z. Eflich, “Identification and Authentication: Technology and Implementation Issues”, Communications of the Association for Information Systems, Vol. 17, No, 4, 2006. DOI: 10.17705/1CAIS.01704

[11]H. D. Jun, et al., "Study on ways to activate i-PIN, a means of identity verification on the Internet", Journal of Korea Information Security Society, Vol. 19, No. 5, pp. 81-92, 2009. DOI: 10.13089/JKIISC.2009.19.5.81

[12]Y. J. Shin, "Research on personal information protection using Internet identity verification methods", Procedings of Korea Association for Puiblic Administration, pp. 1-15, 2010.

[13]H. Y. Yeon, "New National ID Infrastructure on the Internet", Journal of media law, ethics and policy research. Vol. 4, Mo. 2, pp. 83-110, 2005.

[14]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. DOI: /10.17703/JCCT.2022.8.3.559