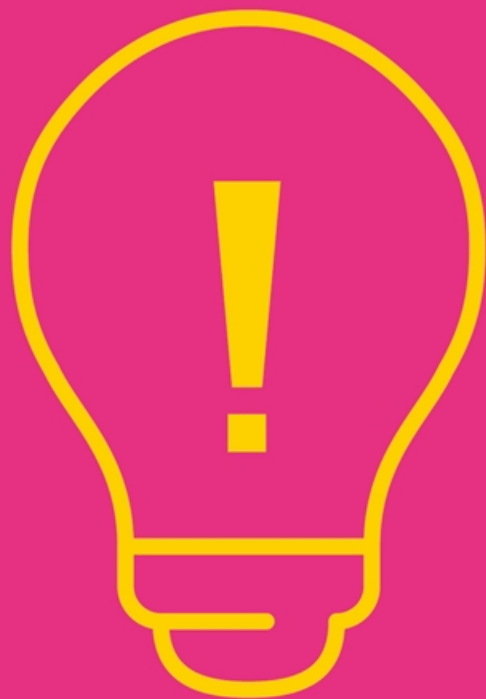


# D.gov

2023-2호

## 이슈분석



---

사용자 중심의 디지털정부 서비스 통합인증 추진현황



---

「D.gov 이슈분석」은 정부의 디지털 전환을 위한 다양한 이슈 분석과 향후 정책 방향을 모색하기 위해 한국지능정보사회진흥원에서 기획·발간하는 보고서입니다.

한국지능정보사회진흥원의 사전 승인 없이 본 보고서의 무단전제나 복제를 금하며, 가공·인용할 때는 반드시 출처를 명시하여 주시기 바랍니다.

본 보고서의 내용은 한국지능정보사회진흥원의 공식 견해와 다를 수 있으며, 문의 및 제안은 아래 연락처로 해 주시기 바랍니다.

---

- 발행처: 한국지능정보사회진흥원
- 발행인: 황종성
- 작성자: 한국지능정보사회진흥원 디지털정부본부 디지털정부기획팀  
- 이수인 책임(silee@nia.or.kr)
- 보고서 온라인 서비스: [www.nia.or.kr](http://www.nia.or.kr), [egov.nia.or.kr](http://egov.nia.or.kr)

## CONTENTS

### 사용자 중심의 디지털정부 서비스 통합인증 추진현황

|                                 |    |
|---------------------------------|----|
| I. 배경 및 필요성 .....               | 4  |
| II. 국내 통합인증 체계의 변천 .....        | 6  |
| III. 해외 통합인증 체계의 동향 .....       | 13 |
| IV. 통합인증 체계 구현을 위한 정책적 제언 ..... | 16 |

## I 배경 및 필요성

### □ 기관·업무별로 도입된 시스템의 인증수단이 제각기 달라, 사용자 불편 발생

- 민원 처리나 상거래가 온라인에서 확대될수록 신원인증의 법적·기술적 보장은 중요해지고, 더욱 안전하고 편리한 정부서비스에 대한 사회적 요구는 증대<sup>1)</sup>
  - 우리나라는 보통 주민등록번호를 통해 누구인지를 식별하며, 온라인에서 스스로를 증명(본인확인)하기 위해 특정한 방법을 활용<sup>2)</sup>
- 기관 및 시스템별로 상이한 인증·접근권한 관리는 디지털정부 서비스를 이용할 때마다 새로이 로그인 및 인증을 해야 하는 불편 유발
  - 일일이 아이디와 패스워드를 외워야 하는 불편뿐 아니라, 웹사이트별로 다른 본인확인 수단이 도입된 경우가 많아, 사용자의 불편과 혼란 가중
    - ※ 정부는 '통합인증체계 구축 및 적용'을 목표<sup>3)</sup>로 설정하고, 해결 노력 중

### □ 비대면 환경에서의 본인확인 수단이 점차 다양화

- ID/PW 기반의 로그인, 주민등록번호를 활용한 본인인증 등을 거쳐, 각종 인증 수단은 갈수록 다양해지고, 기술 발전을 제도가 뒤따르는 상황
  - 기술이 발전하더라도, 법적 보장이 뒤따라야 인증수단으로서 의미를 갖게 되므로, 신규 수단이 기존 수단과 대체(혹은 보완) 관계를 이루는 중
- 신원인증 및 편의성 향상은 미국, 영국 등 디지털정부 서비스 선진국가에서도 중요한 정책과제로 부상 중이며, 각국은 통합인증체계 구현을 위해 노력 중
  - 우리나라와 마찬가지로 이미 구현된 단일인증체계(SSO: Single Sign On)에 여러 인증수단의 법적·기술적 고도화를 통해 이용 편의성 향상을 목표

➔ 디지털정부서비스에 있어, 그간의 신원인증 변화와 함께 해외사례를 살펴보고, 향후 고려할 유의 사항 및 그 의미를 반추

1) 행정안전부. (2017). “대한민국 역사상 가장 위대한 도약 전자정부 50년.”, 서울.

2) 소프트웨어정책연구소. (2021). “본인확인 수단의 변천과정 분석.”, 월간 SW중심사회 2021년 6월호.

3) 디지털플랫폼정부위원회. (2023). “디지털플랫폼정부 실현계획.”

## 참고

## 디지털정부 서비스를 위한 개인식별(본인확인)의 중요성

### □ 국가는 개인을 보호하고 혜택을 제공하기 위해 신분을 등록하고 개인을 식별

- 개인식별은 민원인이 관공서 방문을 통해 여권을 신청하거나, 디지털정부 서비스에 가입·접속한 주체가 본인이 맞는지 반드시 확인
  - 보편적인 정부 서비스는 국민의 접근 및 요청(시스템·현장) → 개인식별 → 인가 → 서비스 제공이라는 점은 큰 틀에서 모두 동일
- 국가는 개인을 식별하기 위해 신분을 등록·관리하며, 등록된 신분은 주로 신분관계를 증명하는 목적으로 활용
  - 국민 개개인을 식별할 수 있는 정보(예: 주민등록번호)와 국가가 인정한 자격(예: 운전면허)이 맞물리는 경우 신분을 증명하는 용도로도 인정
- 국가가 국민에게 서비스를 제공하는 시스템을 구축하는 데에 있어, 기술적으로 필수적인 것이 데이터 식별자(Identifier)이며 기본키(Primary key)에 해당<sup>4)</sup>
  - 기본키란 데이터베이스에서 값이 변경될 일이 극히 적은 경우에만 적합하고, 개인식별정보가 해당 역할을 하는 데에 적합
  - 한국에서는 주민등록번호가 국민을 식별하는 데 활용되는 데이터 식별자로, 대표적인 개인식별번호로 활용되고 정착<sup>5)</sup>되었던 경험

### | 데이터 식별자(기본키와 후보키)의 예시 |

| 데이터 식별자 |     |    |    |    |
|---------|-----|----|----|----|
| 기본키     | 후보키 |    |    |    |
| 학생 ID   | 성명  | 학과 | 성별 | 나이 |
| 9634001 | 홍길동 | 전산 | 남  | 22 |
| 9634002 | 홍길동 | 물리 | 여  | 23 |
| 9634003 | 한라산 | 화학 | 남  | 19 |
| 9634004 | 태백산 | 통계 | 여  | 20 |
| 9634005 | 묘향산 | 전기 | 남  | 21 |
| 9634006 | 지리산 | 전자 | 여  | 22 |

4) 기획재정부, 경희대학교. (2015). “2015 경제발전경험모듈화사업: 한국의 주민등록제도 발전과정.”

5) 행정자치부. (2007). “주민등록제도 발전방안 연구.”

## II

## 국내 통합인증 체계의 변천

## 1 주민등록번호와 아이핀

## □ 주민등록번호 유출로 인한 피해를 방지하고자, 인터넷 개인식별번호 도입

- 우리나라는 개인의 고유 식별자, 즉 범용적인 개인식별정보로 주민등록번호를 활용하였으며 이는 전자정부서비스의 빠른 발전과 효율적인 민원처리로 연결
- 온라인상의 본인확인 방법으로 주민등록번호가 널리 활용됐었으나, 유출 시에 피해가 발생하는 등 개인정보 보호의 필요성에 대한 공감대 형성

## | 온라인 환경에서의 본인확인 및 인증에 관한 주요 변화 |

| 시기        | 내용                                                      |
|-----------|---------------------------------------------------------|
| 1962년 6월  | · 주민등록법 제정                                              |
| 1999년 7월  | · 전자서명법 시행과 함께 공인인증서가 등장하여, 법적 효력 근거 마련                 |
| 2008년 8월  | · 공공아이핀 도입과 함께 온라인에서의 주민등록번호 활용 최소화                     |
| 2011년 4월  | · 본인확인기관 지정 제도 도입을 통해 주민등록번호 대체수단 활성화                   |
| 2012년 8월  | · 영리 목적의 주민등록번호 수집을 전면 금지                               |
| 2020년 12월 | · 전자서명인증사업자 인정·평가 제도 도입을 통해 공동인증서 (구, 공인인증서) 외의 서비스 활성화 |

- 새로운 개인식별정보의 필요성이 대두되었으며, 대체수단으로 인터넷 개인식별번호(Internet Personal Identification Number: 이하 아이핀) 도입
- 아이핀은 식별수단인 동시에 인증수단이었으나, 공공아이핀은 개인식별번호로서 가치가 부족하고, 인증수단으로서의 효용성이 떨어져 폐지를 결정
- 아이핀 2.0 도입 당시 생성된 연계정보가 개인식별정보로 활용됨으로써, 주민등록번호나 아이핀을 직접 활용하지 않고도 개인식별 가능

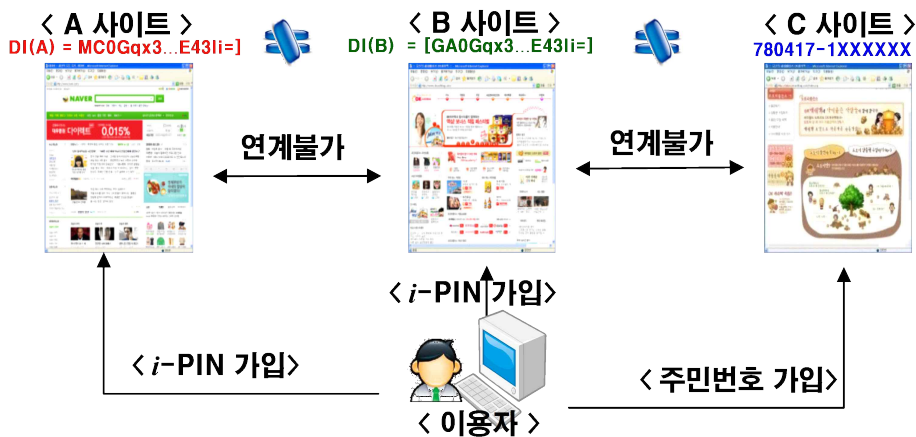
## | 국가별 개인식별정보의 예시와 활용 |

| 국가  | 개인식별번호 여부        | 비고                             |
|-----|------------------|--------------------------------|
| 영국  | X                | 개인식별을 지양                       |
| 미국  | X                | 사회보장번호, 운전면허증 번호 등을 활용         |
| 일본  | △ (마이넘버)         | 최근 적극 도입 중으로, 무작위 번호로 민감정보 미포함 |
| 중국  | ○ (공민신분번호)       | 행정구역, 생년월일 등 민감정보 포함           |
| 스웨덴 | ○ (Personnumber) | 행정구역, 생년월일 등 민감정보 포함           |

## □ 개인정보 노출 위험이 큰 주민등록번호의 대체수단으로 공공아이핀 활용

- 아이핀은 개별 웹사이트 간 한 사용자의 동일인 여부 확인의 어려움, 온라인 서비스의 오프라인 연계가 어렵다는 2가지 문제점을 보유<sup>6)</sup>
  - 오프라인에서는 주로 주민등록번호를 활용하고 있어 본인확인이 어려우며, 일례로 온라인에서 구매한 정보를 오프라인에서 확인 불가
- 아이핀을 고도화할 때, 연계정보(Connecting Information; 이하 CI)를 도입하였으며, CI는 주민등록번호와 같이 개인에게 부여된 유일무이한 식별정보

### | CI의 역할①: 웹사이트 간 연계 |



출처 : 한국인터넷진흥원(n.d.)

### | CI의 역할②: 온-오프라인 간 연계 |



출처 : 한국인터넷진흥원(n.d.)

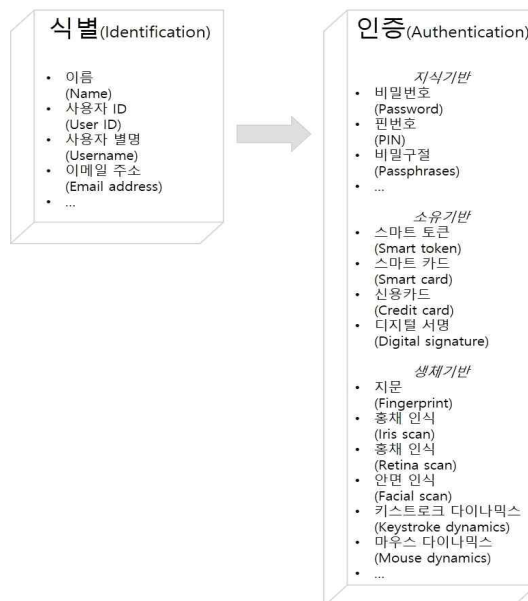
6) 한국인터넷진흥원(n.d.) “아이핀 연계정보(CI) 생성 모듈 안내서.”

## 2 고유식별번호로서의 CI

### □ 주민등록번호 수집이 금지되면서, CI가 활용 가능한 고유식별정보로 대두

- 고유식별정보란 “개인을 고유하게 구별하기 위해 부여된 식별정보”로, 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 등에 해당
    - CI는 본인확인기관이 주민등록번호를 일방향 암호화(Hash)하여 만든 88바이트 길이의 값이며, 고유식별정보 중 하나로 해석<sup>7)</sup>
  - 어떤 본인확인 서비스를 이용하든, 본인확인기관이 생성한 CI를 활용하여 개개인을 식별한다는 점에서는 동일
    - 우리나라의 본인확인 서비스는 개념상 식별과 인증의 의미를 모두 포함하며, ‘본인인증’이란 용어와 엄격히 구분되지 않은 채로 혼용
- ※ 식별이 이름, 생년월일, 주민번호 등을 통해 사용자를 고유하게 확인하는 것을 의미하는 데 반해, 인증은 사용자와 인증기관 간 약속된 방법(ID/PW, 생체정보 등)을 통해 인가된 자임을 증명하는 것<sup>8)</sup>

### | 식별과 인증의 구분 |



출처: Zviran & Erlich(2006)

7) 개인정보보호위원회. (2021) “사례중심 개인정보 보호법령 해석 실무 교재.”

8) 본인확인 지원포털(n.d.)



### 3 공인인증서의 등장과 공동인증서로의 변화

#### □ 전자서명 '인증' 시장의 민간 경쟁이 활성화되고, 사용자의 서비스 선택권 확대

- 전자서명법에 따른 공인인증서는 사실상 유일무이한 독점적 지위를 가지고 있었으나, '20년 12월 전자서명법 개정과 함께 공인인증서 제도는 폐지
- 전자서명법 개정을 통해 민간의 각종 인증서가 경쟁할 수 있는 환경이 조성 되었으며, 공동·금융·민간인증서가 자리를 차지

#### | 인증서의 구분 |

| 분류    | 내용                                           | 예시                                                          |
|-------|----------------------------------------------|-------------------------------------------------------------|
| 공동인증서 | 기능상으로는 공인인증서와 동일하며, 관련 법령 개정에 따른 명칭 변경       | 공동인증서<br>(구. 공인인증서)                                         |
| 금융인증서 | 은행 및 카드사 앱 등을 통해 연계된 서비스에서 이용 가능             | 금융인증서비스,<br>KB국민인증서,<br>NH원패스,<br>하나원큐 등                    |
| 민간인증서 | 개별 서비스 앱에서 인증서를 발급하며, 각 플랫폼에 연계된 서비스에서 이용 가능 | PASS 인증서,<br>카카오페이 인증서,<br>네이버 인증서,<br>페이코 인증서,<br>토스 인증서 등 |

출처 : 금융위원회(2020)를 수정

- 법령상 전자서명은 서명자가 해당 문서에 서명한 사실을 나타내는 걸 의미 하며, 이를 위해 공개키 기반 구조의 인증서 보안 기술이 활용
- 전자서명에서의 '인증(Certificate)'은 보안 방식으로서 데이터 자체의 무결성을 보장<sup>9)</sup>하며, 해당 데이터가 위·변조되지 않았단 사실을 확인
- 전자서명에서의 인증 자체는 보안상의 검증을 의미하는 것이므로, 해당 인증을 수행하는 개인식별을 위한 정보(CI)는 본인확인기관을 통해 취급
- 법률상 본인확인기관이 정보제공자라면 전자서명인증사업자는 개인식별정보 (CI)를 활용한 서비스 제공자로 비유 가능

9) 이대기, 김희선, 조영섭, 진승현, 정교일, 조현숙. (2001). “국내·외 전자서명 및 인증제도 동향 분석.” 정보보호학회지, 11(4), 44-60.

## 참고

## 전자서명인증사업자와 본인확인기관의 비교

- 전자서명인증사업자는 본인확인기관을 통해 개인식별정보(연계정보)를 제공받아야 하지만, 2개 자격을 동시에 취득한 경우는 홀로 서비스 가능

## | 본인확인기관 및 전자서명인증사업자의 구분 |

| 정보통신망법에 따른 본인확인기관<br>(본인확인이 가능한 기관) |              | 금융실명법에 따른 전자서명인증사업자<br>(본인인증이 가능한 기관) |             |
|-------------------------------------|--------------|---------------------------------------|-------------|
| 주민등록번호를<br>취급할 수 있는 기관              | (주)KB국민카드    | 보안 기술의<br>안전성·신뢰성이<br>검증된 기관          | (주)코스콤      |
|                                     | (주)국민은행      |                                       | (주)국민은행     |
|                                     | (주)신한은행      |                                       | (주)드림시큐리티   |
|                                     | (주)엘지유플러스    |                                       | (주)비바리퍼블리카  |
|                                     | (주)우리은행      |                                       | (주)신한은행     |
|                                     | (주)카카오뱅크     |                                       | (주)엘지유플러스   |
|                                     | (주)케이티       |                                       | (주)우리은행     |
|                                     | (주)코스콤       |                                       | (주)케이티      |
|                                     | (주)하나은행      |                                       | (주)한국무역정보통신 |
|                                     | (주)한국무역정보통신  |                                       | (주)한국정보인증   |
|                                     | 금융결제원        |                                       | NH농협컨소시엄    |
|                                     | 나이스평가정보(주)   |                                       | 금융결제원       |
|                                     | 롯데카드(주)      |                                       | 네이버(주)      |
|                                     | 삼성카드(주)      |                                       | 에스케이텔레콤(주)  |
|                                     | 신한카드(주)      |                                       | 엔에이치엔페이코(주) |
|                                     | 에스씨아이평가정보(주) |                                       | (주)뱅크샐러드    |
|                                     | 에스케이텔레콤(주)   |                                       | (주)카카오      |
|                                     | 엔에이치농협은행(주)  |                                       | (주)카카오뱅크    |
|                                     | (주)비바리퍼블리카   |                                       | (주)하나은행     |
|                                     | 코리아크레딧뷰로(주)  |                                       | 한국전자인증(주)   |
|                                     | 하나카드(주)      |                                       | 한국정보인증(주)   |
|                                     | 한국전자인증(주)    |                                       |             |
|                                     | 한국정보인증(주)    |                                       |             |
|                                     | 현대카드(주)      |                                       |             |

출처 : 본인확인 지원포털(n.d.), 한국인터넷진흥원(n.d.)을 참고하여 수정

## 4 통합인증을 위한 시도

### □ 디지털정부 서비스를 위한 인증 프레임워크 개선 추진

- 신기술 도입, 서비스 다변화 등에 따라 새로운 전자정부 인증체계에 대한 수요에 대응하고자 2016년부터 ‘전자정부인증 프레임워크 사업’을 착수
  - 제1차 전자정부 기본계획(2016~2020) 및 실행계획이 수립되면서 정보보호, 개인정보보호에 대한 논의가 활발하게 이루어지기 시작

#### | 전자정부인증 프레임워크 사업 경과 |

| 시기        | 내용                                                    |
|-----------|-------------------------------------------------------|
| 2016년(1차) | · 인증관리제 수립, 디지털원패스 시범 구축, IoT 시범 인증 등                 |
| 2017년(2차) | · 인증관리제 확대, 디지털원패스 구축, G-FIDO(Fast IDentity Online) 등 |
| 2018년(3차) | · 디지털원패스 확대, G-FIDO 개선 등                              |
| 2019년(4차) | · 디지털원패스 확대(계속), 정보보호 강화 등                            |

- 전자정부인증 프레임워크의 하나이자, 공공부문 인증 서비스로서 디지털원패스가 시범 구축되고, 이후 여러 가지 신기술을 반영하여 확대되는 과정에 돌입
    - 디지털원패스란 하나의 아이디로 본인이 선택한 인증수단을 사용하여 안전하고 편리하게 다양한 전자정부 서비스에 로그인, 이용할 수 있는 인증 서비스
- ※ 2023년 현재 254개 정부서비스(포털)에서 사용 가능하며, 전자정부인증 프레임워크 사업을 통해 인증관리제 수립, 공공부문 FIDO 공통기반을 구축하여 디지털원패스에 적용

#### | 디지털원패스 소개 및 로그인 화면 |

##### 디지털원패스란?

하나의 아이디로 본인이 선택한 인증수단을 사용하여 안전하고 편리하게 여러 전자정부 서비스를 이용할 수 있는 인증 서비스입니다.

전자정부 서비스 이용 시 웹사이트/앱/아이디를 달달히 기억할 필요 없이 하나의 디지털원패스 아이디를 통해 여러 전자정부 서비스들을 이용할 수 있습니다.

디지털원패스에서는 편리하게 전자정부 서비스를 이용할 수 있도록 모바일 인증(자문, 연필, 패턴, PIN, 공동인증서(자문)), 공동인증서(PC), SMS 등 다양한 간편 인증수단을 제공하고 있습니다.



디지털원패스 이용시 편리한 전자정부 사이트 로그인

##### 디지털원패스 로그인

디지털원패스 아이디

☐ 아이디 저장

이전

로그인

회원가입

인증수단 재설정

아이디찾기

※ 이용문의 : 1533-3713

(월~금 9:00~18:00, 점심시간 12:00~13:00, 공휴일 제외)

출처: 디지털원패스(n.d.)

## □ 디지털정부서비스를 위한 통합인증 체계인 'Any-ID(가칭)' 구축 시작

- 기존에 구축·운영 중인 디지털원패스의 진화된 단계인 Any-ID에 대한 논의가 시작되어 준비하기 시작
  - 로그인 서비스는 기본적으로 '식별 → 인증 → 인가'의 과정을 거치며, Any-ID 서비스는 해당 과정 전반에 관한 사항을 포함
- Any-ID 서비스 구현 목표 중 하나는 정부의 모든 로그인 수단을 통합·연계하는 데 있으며, 타 정부 웹사이트 이동 시에도 다시 로그인을 요구하지 않도록 개선
  - 민간 SNS ID 또는 디지털원패스로 로그인하거나, 간편인증을 사용해도 동일한 사용자로 식별하여 서비스를 이용할 수 있도록 지원

### | Any-ID 서비스 구현을 위해 필요한 시스템 |



출처: 한국지역정보개발원(2023)

- 모든 공공부문 서비스의 사용자 인증에 있어, 동일한 사용자경험을 제공하고자 하며, Any-ID는 인증체계 전반을 포괄하는 개념

### | 디지털원패스와 Any-ID의 비교 |

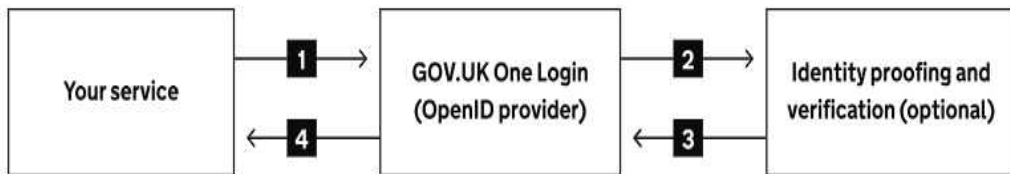
| 구분                | 디지털원패스                                                                 | Any-ID |
|-------------------|------------------------------------------------------------------------|--------|
| 인증수단 간 연계         | O                                                                      | O      |
| 인증등급 정책<br>(권한관리) | X                                                                      | O      |
| 웹사이트 간 연계         | X                                                                      | O      |
| 특징                | 디지털원패스는 그 자체로 독립적인 인증 서비스에 불과하나, Any-ID는 인증등급 정책을 토대로 여러 웹사이트 간 서비스 연계 |        |

### III 해외 통합인증 체계의 동향

#### □ 영국 GOV.UK One Login

- **(배경)** 영국은 기존의 사용자 인증 서비스인 ‘GOV.UK Verify’의 한계를 느껴 서비스를 중단하고 보완된 통합 인증 시스템인 ‘One login’ 개발에 착수
  - GOV.UK Verify의 주요 실패 원인은 ①비현실적인 목표, ②충분한 테스트 부족, ③ 이해관계자들 간의 소통 부족이었으며, ‘23년 4월부터 서비스 종료<sup>10)</sup>
  - ‘디지털 미래를 위한 전환: 디지털 및 데이터를 위한 2022-2025 로드맵<sup>11)</sup>’을 통해 One Login 서비스 강화를 핵심 목표 중 하나로 제시
    - ※ 모든 부처가 2023년 4월까지 정부를 위한 One Login의 적용 전략과 로드맵을 확정하고 2025년까지 서비스를 시작할 것을 미션으로 제시
- **(특징)** 현재 베타버전을 개발하여 보완 중인 단계로 여권 사진, 운전면허증 등을 통해 신원을 증명하고, 현재 해당 앱의 신원 증명 성공률은 80% 이상<sup>12)</sup>
  - ※ 영국은 국민에 대한 고유식별번호를 수집·관리하지 않아 본인확인·인증 등에 어려움
  - 여권 사진과 셀프 촬영 사진을 대조하여 증명할 수 있는 등 생체인증, 지식 기반 인증을 웹·앱을 통해서 할 수 있도록 인증수단을 다양화
- **(도입지원)** 민간 혹은 공공기관이 해당 로그인 시스템에 연계할 수 있도록 전체 흐름과 설명을 제공 중
  - 기관 혹은 기업이 담당하는 서비스가 접속 혹은 계정 생성을 요청받으면, 원 로그인 시스템과 연계하여 본인확인을 위한 지원 제공

#### | One Login과 개별 인증 서비스의 연계 흐름 |



출처 : Government Digital Service(n.d.)

10) 한국지능정보사회진흥원(2022), “민관협력을 통한 공공서비스 고도화 사례 : 해외 주요국 사례를 중심으로.” 디지털플랫폼정부 시리즈 2022-03.

11) Central Digital & Data Office. (2023). “Transforming for a digital future: 2022 to 2025 roadmap for digital and data – updated September 2023.”

12) UKAuthority News. (2023). “GDS promotes the prospects for GOV.UK One Login.”

## □ 미국 Login.gov

- **(배경)** 미국 디지털 서비스와 총무청이 추진한 18F 혁신프로젝트 중 하나였으며, 하나의 계정과 암호로 모든 웹사이트에 접속할 수 있도록 지원
- '17년에 시작되었으며, '23년 3월에 로드맵 발표를 통해 중기 추진방향, 서비스 적용에 따른 대국민·부처의 기대효과 등을 소개<sup>13)</sup>

### | Login.gov 로드맵 |

|                   | 2023년 7~12월<br>(진행 중인)                                                                                                               | 2024년 1~6월<br>(명시적으로 처리 예정된)                                                                                                      | 7월~2024년 12월<br>(예정된 방향성)                                                                                                                          |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 최종 사용자에게<br>대한 영향 | <ul style="list-style-type: none"> <li>· 인증률 향상</li> <li>· 접근성 개선</li> <li>· 플랫폼 인증자</li> <li>· 언어 추가</li> <li>· 계정 복구 개선</li> </ul> | <ul style="list-style-type: none"> <li>· 새로운 신원 인증 채널(전체 대면 또는 원격 감독)</li> <li>· 새로운 근거 유형 및 데이터 소스를 통해 지원되는 새로운 활용 사례</li> </ul> | <ul style="list-style-type: none"> <li>· 추가적인 신원 인증 채널</li> <li>· 추가적인 근거/데이터 소스/이용 사례</li> <li>· 내재된 증명 처리</li> <li>· "비밀번호 없음"으로 가는 중</li> </ul> |
| 파트너 지원            | <ul style="list-style-type: none"> <li>· 새로운 가격 책정 개발</li> <li>· 향상된 보고 기능</li> </ul>                                                | <ul style="list-style-type: none"> <li>· 초기 셀프 서비스 대시보드</li> <li>· 신원 실무 그룹</li> </ul>                                            | <ul style="list-style-type: none"> <li>· 셀프 서비스 대시보드 증가</li> <li>· 데이터 공유 개선</li> </ul>                                                            |
| 정책 및 규정           | <ul style="list-style-type: none"> <li>· 신뢰할 수 있는 심사 정책</li> <li>· 국립표준기술연구소의 조정</li> </ul>                                          | <ul style="list-style-type: none"> <li>· 규정(NIST 800-63-4) 준수</li> <li>· 사기 방지 운영 확대</li> </ul>                                   | <ul style="list-style-type: none"> <li>· 연방정부 위험 및 인증 관리 프로그램으로 가는 중</li> </ul>                                                                    |
| 기타                | <ul style="list-style-type: none"> <li>· 형평성 조사</li> <li>· 부가적인 ID 공급업체</li> </ul>                                                   | <ul style="list-style-type: none"> <li>· 생체 인식 경로 전달</li> <li>· 주와 지방에 걸쳐 더욱 완전한 확장</li> </ul>                                    | <ul style="list-style-type: none"> <li>· 지속적인 플랫폼 개선</li> </ul>                                                                                    |

출처 : General Services Administration(2023)

- **(특징)** 신원 증명을 위해 모든 50개 주, 콜롬비아 특별구, 기타 미국 영토에서 발급한 운전면허증이나 이에 준하는 주·영토에서 발급한 신분증 활용
- 미국 시민권이 없거나 이민자가 아닌 경우도 미국 주에서 발행한 ID, 사회보장번호 및 미국주소만 있으면 본인확인 가능하도록 조치
- **(도입지원)** Login.gov 프로젝트는 부처들이 활용할 수 있는 공통 기반 플랫폼을 제공하며, 접근하는 정부 서비스에 따라 두 가지 수준의 보안을 적용<sup>14)</sup>
- 낮은 보안 수준에서는 전자 메일 주소, 암호 및 전화번호를 사용하며, 상위의 보안 수준에서는 전체 이름, 주소, 생년월일 및 사회보장번호를 포함
- 사용자의 신원을 확인하기 위해 FIDO Alliance 등 민간의 ID 서비스를 활용하며, 이를 통해 확인 불가능할 경우 추가적인 사용자 데이터를 요청
- ※ 미국의 웹 디자인 시스템 설계원칙을 준수하고 범정부 통합 배포를 위한 엔지니어의 기술 지원하며, 'developers.login.gov'을 통해 단계별 개발자용 문서를 제공

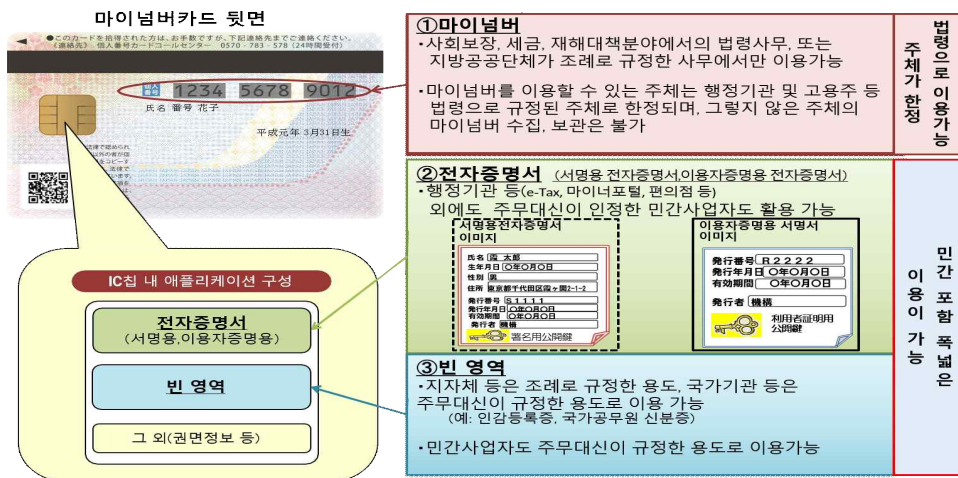
13) General Services Administration. (2023). "Roadmap."

14) Nextgov/FCW. (2017). "The bid to establish a single login for accessing government services is moving again on the last full day of the Obama presidency."

## □ 일본 마이넘버

- **(배경)** 일본은 2015년 10월부터 마이넘버(개인번호) 제도를 도입하였으며, 2016년 1월부터 신분증 및 전자증명서 기능을 하는 실물카드 발행 시작<sup>15)</sup>
  - 영역별 다른 개인식별번호를 활용함으로 인해 이를 확인·연계하는 데에 상당한 시간이 소요되는 것과 같이 행정 효율성 및 국민 편의성 저하<sup>16)</sup>가 이유
- ※ 2017년 12월 기준, 10.2%에 불과하였던 마이넘버카드의 보급률은 2023년 7월 말을 기준으로 71.0%까지 상승한 것으로 발표<sup>17)</sup>
- **(특징)** 한국의 마이핀은 공개 용도로 사용할 개인식별정보였다면, 일본의 마이넘버는 주민등록번호처럼 사실상 비공개를 전제로 활용
  - 앞면에는 성명, 주소, 생년월일, 성별, 본인의 얼굴 사진, 유효기간 등이 표시되어 있으며, 뒷면에는 개인식별번호와 IC칩 소재
- **(도입지원)** 도입 초기 단계에서 발생하는 오류(타인 명의의 연금, 계좌정보와 연동)에 취약점을 드러냈으며, 문제 해결을 위해 노력 중<sup>18)</sup>
  - 2024년 가을까지 기존 건강보험증을 폐지하고, 마이넘버카드를 건강보험증 대신에 활용하도록 하는 마이넘버보험증 제도를 시행 예정<sup>19)</sup>

### | 마이넘버카드 뒷면 |



출처: 일본 총무성(n.d.); 대한무역투자진흥공사(2023)에서 재인용

15) 일본 히로시마시청. "사회보장·조세번호제도 (마이넘버제도)."

16) 이희훈. (2017). "일본 마이 넘버 제도의 개인정보 보호에 대한 시사점 연구." 비교법연구, 17(3), 263-294.

17) 일본 총무성. (n.d.) "マイナンバーカード 交付状況について."

18) 와이티엔. (2023). "채면구진 日 '디지털 행정'...신분증 '마이넘버카드' 곳곳 오류."

19) 뉴시스. (2023). "日記시사, 4일 기자회견...마이넘버카드 추진 계속."

## IV

## 통합인증 체계 구현을 위한 정책적 제언

## □ 고유식별정보로서 CI의 실태조사 확대 및 CI 버전 변경 주기화 필요

- 정부는 매년 '고유식별정보 안전조치 관리실태 조사'를 수행하고 있지만, 이때 고유식별정보의 점검 대상에 CI는 미포함되므로, 기관별 CI 보유량 조사 필요
  - CI를 활용한 본인확인 자체는 본인확인기관을 통해 수행하지만, CI값 자체는 고객 정보와 함께 각 기관의 데이터베이스에 저장되고 있으므로 유출 시 위험
  - 고유식별정보는 비공개를 전제로 하는데, CI는 고유식별정보로 해석됨에도 불구하고, 다른 고유식별정보만큼의 보안 관리 대책이 마련되지 않은 상황
- ※ CI 저장·관리 시, 주민등록번호와 반드시 분리 저장하라는 지침 외에는 권고사항<sup>20)</sup>
- 사회적 비용 발생을 감수하더라도, 지속적으로 신규 버전의 CI 생성·배포를 통해 고유식별정보의 노출로 인해 발생할 수 있는 국민 피해 가능성 최소화
  - 본인확인기관의 역할은 사용자의 개인정보를 보호하고, 고유식별정보의 노출 없이 본인확인 방법을 제공하는 것이므로, 적절한 투자를 계속하도록 유도
  - '23년 11월 현재 정보통신망법에 따른 본인확인기관은 모두 민간사업자로, CI 이용 시 별도 수수료를 수취하고 있으므로 투자 여력은 충분한 것으로 추정
- ※ 본인확인 서비스의 시장 규모는 연간 200~300억 원 규모로 추정<sup>21)</sup>

## | 2017~2021년 본인확인기관(이동통신 3사)의 서비스 처리 누적 건수 |

(단위: 백만 건)

| 구분    | 2017년 | 2018년 | 2020년 | 2021년 9월 |
|-------|-------|-------|-------|----------|
| SKT   | 543   | 614   | 724   | 822      |
| KT    | 338   | 391   | 462   | 547      |
| LG U+ | 283   | 340   | 405   | 502      |

출처: 시사저널e(2021)

- 한편, CI를 활용한 본인확인·데이터 연계 등에 있어, 정부가 과도한 비용을 꾸준히 지출할 가능성이 크므로 '특정 목적을 위한 본인확인기관'으로 공공기관 지정 검토
  - 공공기관의 본인확인기관 지정을 통한 시스템 운영으로 발생하는 비용과 현행의 본인확인기관(민간사업자)을 통한 수수료 지출 간 경제타당성 분석 선행 필요

20) 금융보안원(2022). "인증서 본인확인 기반 통합인증 절차 및 규격."

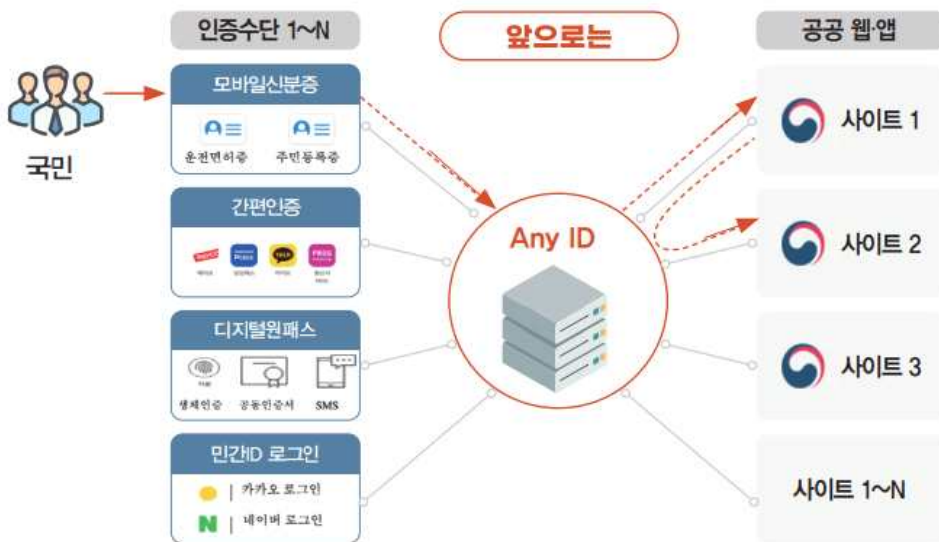
21) 디지털데일리. (2017). "[국감2017] 이통3사 본인확인서비스 수익 5년간 1000억원 육박."



## □ 사용자를 우선시하는 네거티브 규제 방식의 통합인증체계 구현방안 마련 필요

- Any-ID를 적용할 공공서비스의 범위에 대한 고려가 필요한데, 특히 정부가 직접 서비스를 운영하지 않는 경우(비영리법인, 협회 등 위탁)에 대한 논의 필요
  - 공공기관은 아니지만 정부 업무를 위탁받아 수행하는 비영리기관의 경우도 마찬가지이며, SSO로 연계되지 않는다면 결국 국민의 불편은 가중
    - ※ SSO는 '97년 개발된 이래로 20년 이상 각광 받은 기술이며, 한번 인증된 토큰을 시스템 간 주고받음으로써 사용자의 추가인증이 불필요한 원리<sup>22)</sup>
- '제2의 공인인증서 사태'를 막기 위해서는 통합인증 체계 이용기관 간 논의를 통해 서비스의 목적에 맞는 인증등급 정책을 적용할 수 있도록 준비
- 만족스러운 서비스 이용경험을 제공하기 위해서는 통합인증 체계 이용기관 간 논의를 통해 충분한 Any-ID 유지시간(세션시간)을 갖거나, 입력내용 유지 방안 마련
  - 디지털 소외계층이 Any-ID를 통해 서비스를 옮겨 다닌 후, 다소 복잡한 민원 신청을 하게 되었을 때 보안상의 이유로 입력된 내용을 모두 소실할 가능성
    - ※ 민원 신청을 위해 입력한 정보가 시스템으로 인해 소실되는 경우, 서비스 이탈률 및 불만족 증가

### | Any-ID를 통한 통합인증 서비스 경험 |



출처: 디지털플랫폼정부위원회(2023)

22) 유재형. (2007). “다중 도메인간 SSO 실현을 위한 통합 Identity 관리기술 분석.” KNOM Review, 10(1), 16.

## 참/고/자/료

## 국내

## 〈 논문 및 보고서 등 〉

기획재정부, 경희대학교. (2015). “2015 경제발전경험모듈화사업: 한국의 주민등록제도 발전과정.”



개인정보보호위원회. (2021). “사례 중심 개인정보 보호법령 해석 실무 교재.”



디지털플랫폼정부위원회. (2023). “국민은 편리하게, 정부는 똑똑하게 세상을 바꾸는 디지털플랫폼정부.” 한국경제매거진. 서울.

소프트웨어정책연구소. (2021). “본인확인 수단의 변천과정 분석.”, 월간 SW중심사회 2021년 6월호.



유재형. (2007). “다중 도메인간 SSO 실현을 위한 통합 Identity 관리기술 분석.” KNOM Review, 10(1), 16.



이대기, 김희선, 조영섭, 진승현, 정교일, 조현숙. (2001). “국내·외 전자서명 및 인증제도 동향 분석.” 정보보호학회지, 11(4), 44-60.



이희훈. (2017). “일본 마이 넘버 제도의 개인정보 보호에 대한 시사점 연구.” 비교법연구, 17(3), 263-294.



한국지능정보사회진흥원(2022), “민관협력을 통한 공공서비스 고도화 사례 : 해외 주요국 사례를 중심으로.” 디지털플랫폼정부 시리즈 2022-03.



행정자치부. (2007). “주민등록제도 발전방안연구.”



행정안전부. (2017). “대한민국 역사상 가장 위대한 도약 전자정부 50년”, 서울.



## 〈 뉴스/웹사이트/기타 〉

금융보안원. (2022). “인증서 본인확인 기반 통합인증 절차 및 규격.”

금융위원회. (2020). “공인 인증제도가 폐지되더라도 금융분야에 편리하고 안전한 인증서가 사용될 수 있도록 하겠습니다.” Retrieved from <https://www.fsc.go.kr/no010101/74917?srchCtgry=&curPage=&srchKey=sj&srchText=%EC%9D%B8%EC%A6%9D%EC%84%9C&srchBeginDt=&srchEndDt=>



뉴스시스. (2023). “日記시다, 4일 기자회견…마이넘버카드 추진 계속.” Retrieved from [https://newsis.com/view/?id=NISX20230803\\_0002401167&cID=10101&pID=10100](https://newsis.com/view/?id=NISX20230803_0002401167&cID=10101&pID=10100)



디지털데일리. (2017). [국감2017] 이통3사 본인확인서비스 수익 5년간 1000억원 육박 Retrieved from <https://ddaily.co.kr/page/view/2017101810450667080>



디지털원패스. Retrieved from <https://www.onepass.go.kr/>



시사저널e. (2021). “이통3사, 온라인 본인확인시장 98% 장악...5년간 3200억원 수익?” Retrieved from <http://www.sisajournal-e.com/news/articleView.html?idxno=240755>



와이티엔. (2023). "체면구긴 日 '디지털 행정'...신분증 '마이넘버카드' 곳  
곳 오류." Retrieved from [https://www.ytn.co.kr/\\_ln/0104\\_202306100432379238](https://www.ytn.co.kr/_ln/0104_202306100432379238)



본인확인 지원포털. Retrieved from <https://identity.kisa.or.kr/>



한국인터넷진흥원. Retrieved from <https://www.kisa.or.kr/>



한국인터넷진흥원. “아이핀 연계정보(CI) 생성 모듈 안내서”

한국지역정보개발원. (2023). “2023년 Any-ID 구축” 제안요청서

행정안전부. (2022). ‘행정안전부의 디지털플랫폼정부 추진계획(2023년~2027년)’ Retrieved from <https://www.mois.go.kr/frt/sub/a06/b04/egovVision/screen.do>



해외

< 뉴스/웹사이트 >

Central Digital & Data Office. (2023). "Transforming for a digital future: 2022 to 2025 roadmap for digital and data - updated September 2023" Retrieved from <https://www.gov.uk/government/publications/roadmap-for-digital-and-data-2022-to-2025/transforming-for-a-digital-future-2022-to-2025-roadmap-for-digital-and-data>



Government Digital Service. "How GOV.UK One Login works." Retrieved from <https://docs.sign-in.service.gov.uk/how-gov-uk-one-login-works/#how-gov-uk-one-login-works>



General Services Administration. (2023). "Roadmap." Retrieved from <https://login.gov/partners/roadmap/>



Nextgov/FCW. (2017). "The bid to establish a single login for accessing government services is moving again on the last full day of the Obama presidency." Retrieved from <https://www.nextgov.com/digital-government/2017/01/loggingov-moving-ahead/228515>



UKAuthority News. (2023). "GDS promotes the prospects for GOV.UK One Login." Retrieved from <https://www.ukauthority.com/articles/gds-promotes-the-prospects-for-govuk-one-login/>



Zviran, M., & Erlich, Z. (2006). Identification and authentication: technology and implementation issues. Communications of the Association for Information Systems, 17(1), 4.



일본 총무성. "マイナンバーカード交付状況について." Retrieved from [https://www.soumu.go.jp/kojinbango\\_card/kofujokyo.html](https://www.soumu.go.jp/kojinbango_card/kofujokyo.html)



일본 히로시마시청. 사회보장·조세번호제도 (마이넘버제도). Retrieved from <https://www.city.hiroshima.lg.jp/site/korean/15249.html>

