

디지털ID와 스마트키 2030



최운호

서강대학교 전자공학과 초빙교수
choiunho360@gmail.com



현재 글로벌 ICT환경은 구글, 애플 그리고 MS 등이 국제생체표준을 만들어서 이미 'No Password, your Body is Password' 환경으로 변화되었다.

4차산업혁명의 기본 요소인 사물인터넷, 스마트홈, 스마트아파트 등은 기본적으로 글로벌 IT공룡인 애플, 삼성 그리고 구글 등의 주도로 음성인증으로 통제 가능하다. 따라서 정부는 DIGITAL ID의 핵심요소로 가능한 빠른 시일 안에 'Smart Key'의 기능을 정책적으로 제공해야 한다. 특히, 온라인과 지진/재난 등의 상황을 대비해 오프라인에서도 가능해야 한다.

한국 전자정부의 디지털신원인증 정책실패 요인 분석

한국은 유엔이 선정한 전자정부 1위를 수성하면서, 제 4차 산업혁명의 선두주자로 가는 길을 지난 30년간 법과 정책으로 만들어 놓고도 활용을 못했다. 대표적인 부분이 90년대에 전국민 지문DB를 아날로그에서 디지털로 전환하여, 전국의 무인민원발급기와 주민센터에서 온라인으로 18세 이상 전국민 '지문DB'를 활용하면서도, 플라스틱 주민등록증에 지문을 인쇄하여 아날로그 형태로 사용하는 것이다. 생체정보를 IC칩에 넣는 것을 주저했으며, 추가로 혈액형 등 건강정보 등을 사용하는 시점을 실기했다.

또한, 전자서명법에 전자서명의 범위가 공인인증서에서 출발해서 현재 2021년 사설인증서, 금융인증서 등으로 확장되어 가고 있는데, 과거에 법령으로 공개키 기반구조(PKI, Public Key Infrastructure) 이외에도 생체정보인 '지문·음성·홍채 인식' 등으로 확대하여 사용할 수 있다고 정하고도 실제 적용하는 시점에서는 전문가들의 충고를 무시했다.

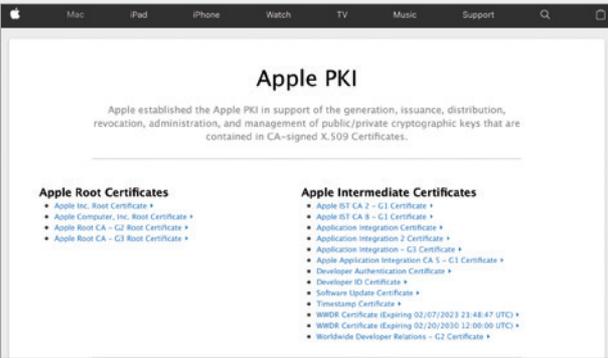
현재 일반인이 사용하는 2015년 이후 스마트폰이라 판매된 모든 디바이스에 '지문, 홍채, 얼굴인식 등'이 광범위하게 사용되고 있고, 생체정보를 암호화해서 보호하기 위하여 애플, 구글, 삼성전자 등이 스마트폰 보안영역에 사설인증서(PKI)를 기본 탑재하여 사용하고 있는데도 말이다. 스마트폰 '설정/생체인증과인증서' 영역에 가면 몇백 개의 인증서가 기본 탑재되어 있다.

또한 사물인터넷, 스마트홈, 스마트시티 그리고 Digital Car Key 등에 미국, 유럽연합 등이 국가적 정책과 애플, 구글 등 글로벌 IT 기업이 사설인증서(PKI)기술을 확장해서 사용하고 있는데도, 국가 전반적으로 사물

인터넷, 스마트시티 등에 도입하는데 주저하고 있다. 게다가 일부 무분별한 전문가들이 '공인인증서에 사용된 인증서(PKI)기술'을 한국만 사용하고 있다는 여론몰이에 넘어가서, 인증서기술을 없애야 한다는 국가적인 청산작업까지 하고 있었다.

- 주민등록법 제24조(주민등록증의 발급 등)
②주민등록증에는 성명, 사진, 주민등록번호, 주소, 지문(指紋), 발행일, 주민등록기관을 수록한다. 다만, 혈액형에 대하여는 대통령령으로 정하는 바에 따라 주민의 신청이 있으면 추가로 수록할 수 있다. (이하 생략).
- 전자서명법
2002년 4월부터 시행된 개정 '전자서명법'에는 전자서명의 범위가 공개키기반구조(PKI) 암호방식에서 지문·음성·홍채 인식 등으로 확대되었다.

[그림 1] 애플과 주요 글로벌금융기관의 최상위인증기관(ROOT CA)



VISA PKI
<http://enroll.visaca.com>
<http://enroll.visaca.com/VisaPublicKeyInfrastructureCertificatePolicy.pdf>

Master card PKI
<https://ssl-tools.net/subjects/9d9950aa2be51a2bdc1e749c9eb9f24a9ad046e8>

EMV PKI(신용카드 국제표준)
<https://www.cryptomathic.com/products/emv/emv-ca>

SWIFT PKI(국제 외화 송금네트워크)
<https://www.swift.com/our-solutions/interfaces-and-integration/swift-certificate-centre/swiftnet-pki-evolution>

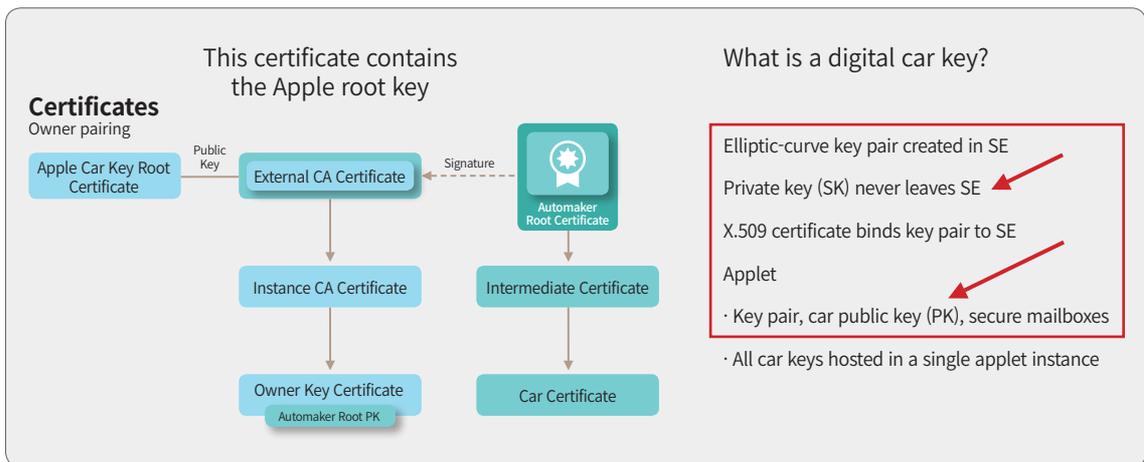
Apple PKI
<https://www.apple.com/certificateauthority/>

주요 사례를 들면, 2014년 지문센서를 처음으로 휴대폰에 도입한 애플이 사설인증서(PKI)기술을 가장 많이 쓰고, 2020년에는 스마트폰으로 차량도어를 열고, 시동을 걸며, 발레파킹에 사용하는 ‘Apple Car Key’에 어떻게 사설인증서(PKI)를 사용하는지를 살펴보면 된다. 애플은 아이폰, 애플페이, 애플시계, 애플TV 등 모든 영역에 사설인증서를 사용하며, 애플, 구글, MS 그리고 아마존 등이 세계 최대 규모의 최상위 인증기관(ROOT CA)을 운영하고 있으며, 비자카드, 마스터카드 등 금융기관의 주요 최상위 인증서 사이트를 보면 알 수 있는데, 누가 한국만 인증서 쓴다고 거짓말을 한 건지 생각해 보아야 한다.

애플이 2020년 야심차게 발표한 Smart Car key는 애플의 최상위인증기관이 발행한 인증서로 내부보안구조를 설명하고 있으며, 전세계 공유차들의 표준화 단체인 CCC(Car Connectivity Consortium) 표준에도 적용되었으며, 실제적인 구현모습에 한국과 같은 사설인증서(PKI) 기술이 사용되었다.

애플, 현대차, 벤츠 등 전세계 25개 자동차 회사들이 참여한 CCC 표준의 ‘Digital Car Key’에 사설인증서(PKI)기술이 적용된 것을 보면, 앞으로 사설인증서(PKI) 기술을 어떤 분야에 활용할지 정책적으로 검토해야 한다.

[그림 2] 애플 아이폰으로 Smart Car Key에서의 사설인증서(PKI) 사용사례



출처: <https://developer.apple.com/videos/play/wwdc2020/10006/>

[그림 3] 국제공유차컨소시엄(Connected Car Consortium)의 Digital Key와 PKI

02

The Digital Key architecture uses standards-based public key infrastructure to establish end-to-end trust. Mobile devices create and store Digital Keys in Secure Elements-embedded technology that provides a tamper-resistant secure implementation - to provide the highest-level of protection from the plethora of known hardware- and software-based attacks, including tampering, storage intrusion, cloning, and unauthorized access as well as side- channel, interface, and many other forms of attack.

출처: https://global-carconnectivity.org/wp-content/uploads/2020/04/CCC_Digital_Key_2.0.pdf

전자정부의 문제점

- 한국 전자정부는 유엔이 선정한 ‘전자정부 1위’라는 한 상에서 깨어나야 한다.
- 지난 10년간 지속적인 예산삭감으로 급속하게 노후화 되어서 향후 전면 개편되어야 한다.
- 국제기구(OGP)의 보고서는 한국의 정보공개수준 및 정부투명성은 낙제점을 기록한 바 있다.
- 산업 4.0시대에 시민들의 편의를 위해서, 스마트홈 / 사물인터넷 / 핀테크 등에 연결이 불가능하며, 향후 ‘메타버스’ 등 VR/AR/MR 가상공간 활용 등에 대한 대비가 부족하다.
- 북한의 핵 고출력 전자기파(EMP)공격에 정부전산센터와 국가기반구조인 금융/통신/전력 등 무방비여서 ‘재난 시 전자정부 구축’에 대한 준비가 부족하다.
- 전시적 정보공유로 ‘칸막이 행정’과 주요 정부자료가 빅데이터 활용에 불가능한 구조이다.
- 정권마다 홍보차원의 새로운 구호나 개념에 전자정부가 희생을 당해서는 안된다.

전문가들이 아래와 같이 3.0도 걱정했는데, 현재는 앞으로 10년이 더 걱정스러운 수준이다.

‘데이터정부, 디지털정부, 사이버정부 및 플랫폼정부 등 수없이 많은 용어들이 등장하기 때문에, 시류에 휩쓸려서 새로운 것을 찾아서 작명을 하고, 세계에 하나밖에 없는 것을 정권 임기 중에 추진한다고 정치적 수사(Political Rhetoric)를 내세우고 싶겠지만, 근본으로 되돌아가는 것만이 성공의 지름길이라는 것을 명심해야 한다.’
- ‘정부3.0은 왜? 실패했는가’, 정충식(경성대학교) -

2020년 이후에 대표적인 몇 가지 기술변화를 살펴보고, 이를 도입 시 필요한 구성을 제시한다.

[그림 4] MS 노트북 접속시, “ID/패스워드없이, 지문USB, 지문카드”로 컴퓨터 접속” 2021년



MS가 2021년 봄에, 향후 MS의 모든 서비스에 접속 시 ‘No Password’를 선언하면서 도입한 방식이다. 즉, 지문카드나 지문USB, 얼굴 그리고 음성으로 접속한다. 이러한 방식은 구글, 페이스북 등이 모두 도입 중이어서 전자정부에 접속할 때 기본수단으로 검토되어야 한다.

현재는 재택근무 시 줌이나 MS 팀즈 등을 활용해서 원격회의에 참가하지만 VR/AR/MR 환경에서 참여하는 방식은 아래와 같이 다를 수 있으며 이에 대한 ‘전자정부 환경’을 새로 갖추어야 한다. 물론, 전자정부 참가자에 대한 “사용자 인증”을 별도로 구성해야 하며 이를 ‘지문, 얼굴, 홍채 그리고 제스처 등과 인증서(PKI)’ 등이 멀티 인증으로 사용되어야 한다. 적절한 인증과 보안등급별로 참여자를 구별하는 것은 당연하다.

스마트전자정부와 스마트시티에 접속하는 '디지털ID 열쇠(Smart Key)'

5G 시대에 생체 인증을 이용한 '스마트키(Smart Key)', 즉 DIGITAL ID를 도입해야 한다. 정전·지진·해킹으로 인터넷이 끊겨도 본인 인증이 가능하기 때문이다. 2018년부터 본격적으로 시작한 사물인터넷(IoT) 기반 스마트 홈, 스마트 카, 스마트 시티 등에 적용할 스마트키 시스템을 구축해서 스마트시티 보안으로 제공해야 한다.

인터넷이 마비돼도 사용자 본인을 인증할 수 있는 전자 신분증과 'Digital Identities'를 발급해 운영해야 하는 것이 필요하기 때문이다. 스마트키를 사용하려면 보안과 인증을 빼놓을 수 없다. 하지만 국내 대기업이나 전자정부 그리고 지자체의 스마트시티의 경우 모든 서비스에 보안 설계가 부실하다는 지적이 많다. 생체 인증의 경우 국제표준을 무시하고 부처 간, 회사 내부부서 협력도 미약한 편이다.

2018년 KT 통신구 화재는 생체 인증과 스마트키를 설명하기에 좋은 사례로 볼 수 있다. KT 통신구 화재는 '일시적인 통신 불통-정전-인터넷 단절' 등이 얼마나 중요한 것인지 보여줬고 '오프라인 서비스 대책'이 필요하다는 것을 알게 해줬다.

통신구 화재는 전화-인터넷-IPTV 사용 불가, 은행 영업점 전용회선과 현금 자동 입출금기(ATM, Automated Teller Machine) 수백 곳 장애, 신용카드 결제 마비, 의료기관 의료진 전화 불통으로 응급상황 교신을 병원 내 방송 사용, 경찰 통신망 장애 등 불편을 낳았다.

IoT 시대에서는 온·오프라인을 넘어 모든 것을 연결해 다양한 서비스에서 사용할 수 있는 멀티인증을 만들어내고, 편리하고 보안성이 높으면서 경제성도 갖춰 가장 활발히 사용할 수 있는 방법이 생체인증, 특히 지문·음성인증이며, 안전한 방법을 지원하는 것이 바로 국제표준에 근거한 사설인증서(PKI) 기술로 구현할 수 있다. 생체 인증은 온라인은 물론 오프라인에서도 모두 사용할 수 있기 때문이다. 생체 인증은 스마트폰, PC, 노트북, 태블릿,

브라우저에 이르기까지 다양한 곳에서 이미 상용화되어 판매 중이다.

2021~2023년은 스마트폰 화면에 지문 인식 기능이 탑재되어 사용할 수 있을 것으로 예상되는데 삼성전자, 애플, 구글 등 모든 스마트폰이 화면지문 인증을 도입하고 있고, 지문을 여러 개 등록할 수 있어서 그 중 특정 등록 지문은 경찰 신고 전용이나 오프라인용으로 지정해서 사용할 수도 있다.

지문 등 생체정보를 안전하게 사용하도록 암호화하고 서명하는 기술인 '사설인증서(PKI, Public Key Infrastructure)'는 국제통신연합표준(ITU X.509)으로 우리말로 '공개키 기반구조'라고 번역한다. 1989년 ITU 국제표준으로 정한 후 전 세계에서 정부, 금융, 국제결제망(SWIFT), 우체국 등에서 사용하고 있다. 한국은 2001년부터 인터넷으로 금융 거래를 할 때 비밀을 보장하면서도 거래 당사자 신분을 확인할 수 있게 해주는 보안 기술로 적용해 사용하고 있는데, 일반적으로 금융용 공인인증서에 사용하며, 데이터를 암호화하는 방법은 크게 '공개키'와 '개인키' 방식으로 구분할 수 있고, 2020년부터 전국민이 사용하는 사설인증서도 동일한 기술이다.

세부 기술은 키를 구분하는 것, 그러니까 '공개키'는 은행에 보관하고 '개인키'는 개인의 스마트폰이나 PC 등에 보관해 보안을 강화하기 위해 쓰는 방식인데, 공개키 방식은 데이터를 암호화하고 이를 다시 풀 수 있는 열쇠가 다르기 때문에 거의 완벽한 보안이 가능하고 정보 유출 가능성을 줄일 수 있다는 이점이 있다. 공개키 암호의 상용화를 위해서는 키의 생성과 인증이 필요하다. 이런 과정을 안전하게 관리할 수 있는 체계가 사설인증서(PKI)이고 ITU 국제표준을 따르는 기술이다.

애플페이, 구글페이, 카카오페이 그리고 요즘 시 스피커나 사물인터넷, 암호화폐, 블록체인 등도 모두 사설인증서(PKI)를 사용하고 있다. 뿐만 아니다. 온라인 신원 확인, 전자서명, 사물인터넷 기기인증도 이 기술을 이용한다. 특히 차세대 인증 기술로 손꼽는 국제생체표준(FIDO) 기반 생

체인증도 사설인증서(PKI)가 융합돼서 구현되었다.

2017년 7월 애플은 애플 사물인터넷 연결서비스인 홈킷(Apple HomeKit)에 생체인증을 지원한다고 발표했다. 애플 홈킷은 2014년에 처음 공개한 개발자 도구 중 하나로, 연결된 가전제품을 애플의 모바일 OS에 통합시켜 스마트 홈을 위한 통합 제어장치로 활용할 수 있도록 하는 제품이다. 2017년에 애플 홈킷에 추가된 새로운 기능 중 하나가 생체인증 지원이다. 애플사는 HomeKit 코드 혹은 QR코드로 사물인터넷 장비를 등록시켜, 주인의 명령만 듣게 하는데, 국내 회사들의 서비스와 가장 큰 차이는 국내 사업자들은 장비 몇 대를 빌려주는 IoT 무제한 요금제로 플러그, 에너지미터, 스위치, 오픈센서, IoT 허브, 스피커 등 기기를 무료로 제공하고, 월별 통합요금을 부과하는데, 사설인증서(PKI)와 결합된 서비스 없이 단순한 네트워크 통신 기능만을 제공하고 있어서 수많은 해킹의 위협에 노출되고 있다.

2021년에 애플, 구글, 아마존 등이 사물인터넷 누적 연결대수가 1억대에서 많게는 10억 대 이상을 연결하여 판매했는데, 특히 2020년 11월에 애플은 시스피커로 ‘스마트홈의 모든 사용자의 목소리 별로 각각 조작하는 시연을 보여주면서’ 스마트폰과 스피커 그리고 공유차(Connected Car) 등을 연결하여 통제되는 것을 보여준 바 있다. 이에 따라 각각의 스마트폰 생산회사들은 각각 ‘애플은 홈킷 그리고 안드로이드 폰은 Things’라는 메뉴에 연결되는 사물인터넷 제품 메뉴를 서비스하고 있으며 이는 보편적으로 사물인터넷은 스마트폰과 시스피커 모두에 구현되었다.

우려되는 점은 국내 가전사인 삼성전자, LG전자 등의 최신 TV제품에 탑재되어, 시장을 내주었다.

유럽기반 방산업체인 Thales(2017)는 글로벌 트렌드 보고서에서 ‘기업에서 IoT의 부상과 공개키 기반구조(Public Key Infrastructure, PKI)를 설계하고 구축하는 방법에 미치는 영향을 2017년 발표하고, 특히 IoT는 인증서(PKI)를 활용한 서비스로 사물인터넷 장비의 등록을

가속화하는 가장 중요한 요소가 될 것¹⁾이라고 언급했다.

이렇듯 사물인터넷(IoT) 환경에서 ‘생체정보와 사설인증서(PKI)의 결합’은 2020년에 전세계 가전제품 선두주자인 삼성전자, LG전자의 TV 등 전제품에 탑재되어 본격적으로 추진되고 있는 것으로 보인다. 애플뿐만 아니라, 구글, 아마존, 삼성 등 다양한 글로벌 기업들이 스마트폰과 지문, 홍채, 안면, 음성 등 생체인증을 결합한 서비스를 빠른 속도로 내놓고 있다. 이는 ‘사물인터넷+사설인증서(PKI)+생체정보’를 결합하여 스마트 아파트 혹은 스마트시티와 개개인을 안전하게 연결하려는 움직임이라고 할 수 있으며, 각국의 지능형 정부서비스에도 연결되고 있다.

사물인터넷(IoT) 환경이 복합적으로 연결되는 환경에서, 이제 기존의 인증기술인 인증서(PKI)만으로는 보다 확장되고 융합된 새로운 인터넷 환경에서 안전할 수 없다. IoT 환경이 구체화 된 스마트시티에 빠르게, 그리고 안전하게 접속하기 위해서 생체인증과 결합은 필수적인 요소라고 하겠다. 또한, 각국 정부가 경쟁적으로 도입하고 있는 초기 단계의 전자신분증을 넘어서서 종합적인 ‘Digital ID, eID’ 그리고 ‘Digital Identities’는 4차산업혁명을 준비하는 지능형국가나 스마트시티에서 새로운 스마트키(Smart Key)로 부각되고 있다.

한국에서 통신사업자가 운전면허증 등 일부 신분증 기능을 스마트폰에 탑재하거나 코로나 백신 여권을 추진하는 것은 이러한 국제표준이나 동향에 기반해서 만드는 것보다는 대중의 수요를 일부만 도입하는 사적인 신분증 통합현상이다. 삼성/애플 등 스마트폰 제조사들이 추진하는 신분증 통합은 보다 구체적이지만 국제표준과 지침이 어느 정도 제정되어야 시범사업 추진이 가능한 수준이기도 하다.

1 The rise of the Internet of Things(IoT) in the enterprise and its impact on how organizations design and build their public key infrastructure (PKI) is a key theme in this year's study. Specifically, IoT is the fastest trend driving the deployment of applications using PKI.

최근 영국정부는 ‘UK Gov, The UK digital identity and attributes trust framework(Feb 2021)’에서 생체 인증과 한국의 공인인증서/사실인증서 기술에 쓰이는 공개키기반구조 인증서(Public Key Infrastructure, PKI)를 사용하는 것을 보여 주었고, 비영리 국제기구인 ‘Secure Identity Alliance’도 유럽, 아시아, 아프리카 등 많은 나라의 ‘Digital ID, Digital Identities’ 등의 진행사항을 요약하여 ‘GIVING VOICE TO DIGITAL IDENTITIES WORLDWIDE(Feb. 2021)’에서 보여 주고 있는데 대표적인 용어 정의를 [표 1]에 정리해 보았다.

전자신분증과 ‘Digital Identities’

최근 지능형 정부서비스의 일환으로 운전면허증, 공무원증, 연금, 보험 등 각종 신분증 등이 스마트폰에 탑재되어 가는 추세지만 이는 한정적인 신원확인 서비스에 국한되어 적용되고 있으며, 글로벌 동향은 신원확인 이외에도 금융업무, 주택 구매, 신용 조회 등이 일괄적으로 해결되는 ‘Digital Identities’의 정의를 대폭 확장한 개념으로 진행되고 있어서 지능형정부 정책의 조정과 일괄적인 법제도 정비가 필요하다.

또한 많은 나라는 ‘IC칩 형태의 스마트카드’에 생체 정보로 인증하는 카드를 사용하는 국가와 국가주도의 eID 나 Digital ID 등을 제공하는 여러 형태로 구분되는데 한국이 지능형 정부의 신분증으로 앞서가려면, 신분증 검

[표 1] 주요 Digital Identities 용어 및 기술 정의

Biometrics

A measurable physical characteristic or personal behavioral trait used to recognize an applicant’s identity, or verify their claimed identity. Facial images, fingerprints, and iris scan samples are all examples of biometrics

Digital ID wallet

A secure mobile wallet app which hosts a range of digitized identity documents and credentials, which is based on ISO 18013-5 standard, put the end user in control of his data and can be checked through an ID verifier app.

Electronic signature

The result of a cryptographic transformation of data that, when properly implemented, provides origin authentication, assurance of data integrity and signatory non-repudiation.

Public Key Infrastructure (PKI)

A set of hardware, software, policies, processes, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and public-keys. PKIs are the foundation that enables the use of technologies, such as digital signatures and encryption, across large user populations. PKIs deliver the elements essential for a secure and trusted business environment for e-commerce and the growing Internet of Things (IoT)

출처: Secure Identity Alliance ‘GIVING VOICE TO DIGITAL IDENTITIES WORLDWIDE(Feb. 2021)’
<https://secureidentityalliance.org/news-events/news/entry/global-identity-report-launched-by-secure-identity-alliance>

용 ‘전자신분증+신용카드’ 같은 형태로 ‘One Card’ 기능을 지문 등 생체기술과 사설인증서로 융합하여 제공해야 한다. 이는 다중보안이 구현되는, 세계 최고의 IT시스템과 핀테크 결제를 제공할 수 있고, 메타버스에서 신분증 용도로 활용이 가능하다.

실제로 지문인증기능을 탑재한 전자신분증용 스마트카드가 제작되고 있어서, 60여 개 국가가 다목적 생체전자신분증을 발급하고 있으며, 신용카드와 병합하는 현상도 나타나고 있다. 대표적으로 마스터카드(Mastercard)사는 지문센서를 탑재한 신용카드를 제작하고 향후 5년간 약 33억장의 신용카드 교체를 발표하였으며(2017), 이는 세계 신용카드 1위 유니온페이(2019)와 2위인 비자카드(2018)도 동일하다. 2021년 3월 삼성전자는 마스터카드사와 제휴하여 ‘지문신용카드’의 글로벌서비스 전략을 발표했다.

이러한 전자신분증을 활용하면 간편하게 민원을 처리할 수 있다. 무인 민원처리 기기 혹은 온라인 민원 홈페이지에서 개인정보를 입력하고 사설/공인인증서를 설치하여 로그인하는 번거로운 절차를 거치는 대신, 전자신분증과 생체인증을 통해 좀 더 간단하면서도 안전하게 본인인증이 가능해진다. 이는 해당 스마트시티 주민들의 공공서비스에 대한 만족도를 높여 줄 것으로 기대된다.

특히, 복지비가 증가 추세이고 각 부처와 지방자치단체의 복지바우처 카드도 대상자가 확대되면서 초기 연 3조원에서 현재는 12조 원대나 되는데 횡령이나 대리수령 등이 언론에 보도되고 있으며, 정책적으로 이를 지문인식 카드로 바꾸면 수령확인을 생체인증 및 바이오서명으로 문제를 해결할 수 있으며, 해외 관광객들을 대상으로 지문인식 원카드(One Card)를 도입하면 편리한 교통과 쇼핑, 관세 환급, 자동 환전 등의 혜택을 원스톱으로 제공할 수 있다.

군인신분증이나 공무원카드도 지문 카드로 교체하면 컴퓨터 접속과 비밀문서 접근 관리는 물론 전이나 사이버전에서 인터넷·통신이 두절돼도 오프라인 접속이 가능하고 여러 가지로 행정 효율성도 제고할 수 있다.

4차산업혁명시대의 전자정부 접속시스템

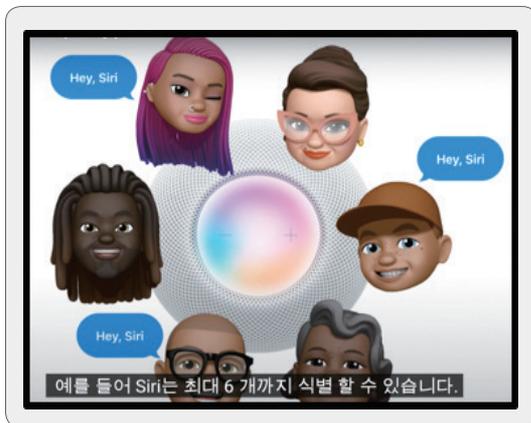
■ 글로벌 ICT환경 변화로 ‘정부 생체인증 + 혼합현실(XR)’ 도입이 전면 실시되어야 한다.

- 생체정보기반 본인 인증 수단인 지문인식이 스마트폰을 넘어 PC와 키보드, 노트북 등 IT(정보기술) 기기 전반으로 확대되고, 금융권도 가세해 지문인식 신용카드 개발에 나서며 시장은 더욱 커지고 있다.
- 가상환경에서 전자정부서비스와 디지털신원인증은 새로운 차원의 서비스가 계획되고, 안전한 환경으로 구현되어야 하며, 메타버스에서 아바타의 Digital ID 이슈는 국가적으로 검토되어야 한다.
- 생체인식은 기존 잠금 해제나 개인정보 보호용으로 쓰던 수준을 넘어 결제 수단이나 공공기관·기업의 내부 시스템 접근을 위한 인증 수단으로 쓰임새가 많아지고 있다.
- 스마트폰 등에 지문 / 홍채 / 음성 / 안면인식이 보편화 대중화 되고 있다.
- 미국 MS는 지문인식센서를 탑재 키보드, 삼성전자 등 100여 사 지문노트북 출시(2019년)
- PC·노트북에 꽂는 지문인식 보안USB키도 대중화되고 있다.
- 금융권도 서명·비밀번호를 대체하는 인증 수단으로 생체인식을 도입하고 있다.
 - : 마스터카드와 삼성전자가 하반기 ‘지문신용카드’를 출시할 방침이고 향후 200억 장 교체
 - : 중국은 ‘디지털 위안’이라 불리는 국가발행 암호화폐(CBDC)에 지문카드 시범사업을 진행 중이어서 향후 IC카드를 지문카드교체로 되는 것이 인민은행 승인으로 진행 중이고, 한국은행도 2021년 시범사업을 발표
- 유엔과 59개 산하기관은 지문 스마트카드 한 장으로 출입과 컴퓨터에 접속할 수 있는 신분증을 도입, 15만 명 사용 예정, 한국업체가 공급업체로 선정 (2017년 9월)
 - ✓ 단순한 결제수단을 넘어 자율주행차, 공유차, 스마트 홈, 사물인터넷(IoT)에서도 지문 등 생체인증을 통한

본인인증 수단으로 활용됨을 의미하면, 전자정부에 접속되는 수단이 다양함을 의미

- ✓ 이미 애플이 홈킷이라는 사물인터넷서비스를 제공하고 있고, 국제표준(FIDO)도 PKI를 이용한 새로운 사물인터넷 표준을 제안하고 있는 상태(2021년)
- ✓ 구글, 페이스북, 드롭박스는 10억~20억 명의 서비스 이용자가 겪는 패스워드 관리 어려움을 해결하기 위해 2017년 2월 ‘No Key, No Access’ 정책을 발표, 지문 USB 도입
- ✓ 마이크로소프트는 윈도우10에서 헬로우(Hello) 생체인증지원 스마트Key로 작동
- ✓ 인터넷 익스플로러(IE), 크롬 등 모든 인터넷 브라우저도 이를 지원한다.
- ✓ 문제점 : 정부에 보급된 MS Window 7(구형)이 현행 ‘Winow 10’등 최신형으로 신속히 교체중이나 단계적 교체로 되어 있어, 관련된 전자정부지원 S/W가 이미 경쟁력 상실 중
- # 국제생체표준(FIDO: Fast Identity Online) :
구글 / MS / 삼성 / LG 등 Global 생체산업표준

[그림 5] 애플, 스마트홈 시스피커에서 ‘가족 모두의 음성을 구별’ 2020년

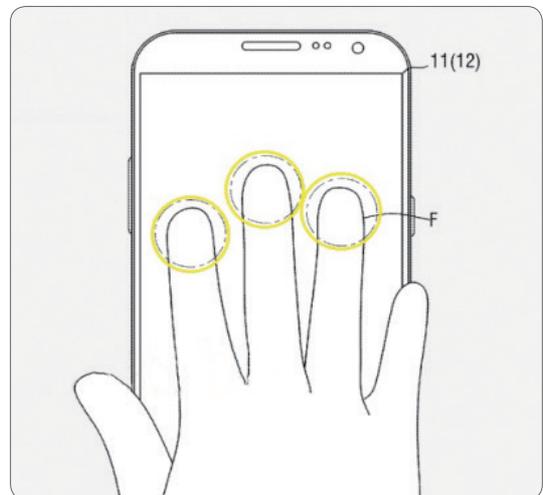


출처: <https://developer.amazon.com/en-US/alexa/voice-interoperability/members>

■ 집에서 인공지능(AI) 스피커로 전자정부에 접속하는 상황에 대응해야 한다.

- 삼성전자 등 주요 가전사와 지자체가 공급중인 스마트 아파트가 폭발적으로 증가하고 있으며, 집안의 모든 사물인터넷은 음성으로 제공되고 있지만, 주인을 구별 못하고 있는 수준이어서 아무나 명령하면, 검색이나 날씨 정보 등을 제공하는 수준이다.
- 애플, 아마존, 구글 등은 ‘본인의 음성을 인증하여 본인에 맞는 서비스’를 2019년부터 구성하여 제공하고 있으나, 국내 시스피커들은 이에 비해 아마추어 수준의 서비스만 실시 중이다.
- 각각의 시서비스의 음성에 대한 호환성을 보장하는 표준을 결성하여, 집안에 복수의 회사가 제공한 음성서비스를 ‘한 개의 음성’으로 통합하여 제공하는 기능도 제공한다. ‘Voice Interoperability Initiative’에는 아마존, 페이스북, 인텔, 퀄컴, 카카오 등 100여 개의 기업이 음성인증에 대한 호환성 개발자 지침을 가지고 공동 대응 중이다.
- 2021년 하반기부터 생산되는 주요 스마트폰은 지문을

[그림 6] 스마트폰 ‘스크린 지문 2-3개’ 채택 예정 (2022년 발표 예상)

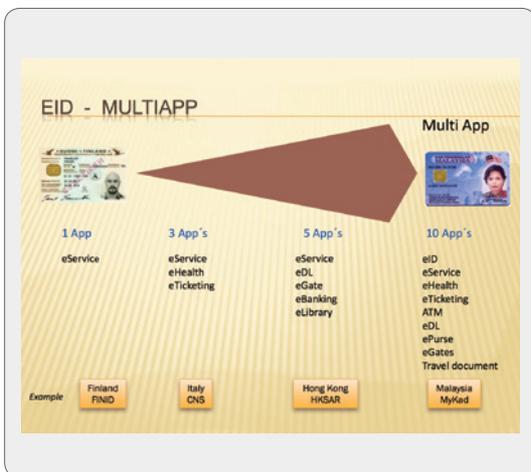


동시에 2~3개로 활용이 가능해지면서 이에 따라 '지문 1개 혹은 동시에 3개 혹은 지문을 순서대로'하는 인증이 가능해진다.

전자주민증 vs 전자신분증(스마트Key) 논란 요약

- 한국은 과거 '전자주민증'을 시도했으나 전자주민증을 도입한 60여 개국 보다 뒤쳐져 있다.
- 인도정부는 2010년 11월부터 '아드하르' 프로젝트를 추진했다. 아드하르는 전 국민에게 지문·홍채·얼굴 등의 정보를 담은 신분증, 즉 생체인식카드를 발급하는 프로젝트다. 약 10억 명의 지문과 홍채인식정보 등이 들어가는 '세계 최대 생체 빅데이터 플랫폼'이다.
- 에스토니아도 'e-ID' 발급을 통해 200개 민원업무를 전자신분증으로 해결한다.
- 미국정부는 2021년까지 '비밀번호 사용 금지'(No Password)를 선언했다.

[그림 7] 다목적 전자신분증
(주민증 +운전면허증+연금+의료 등, 2015년 기준)



- ✓ 인도, 말레이시아, 유럽각국 등이 '다목적 전자신분증 (Smart Key)' 사용 전자정부접속(2010-15)
- ✓ 인도정부는 전자신분증으로 'Digital India와 송금, 핀테크 플랫폼 운영'
- ✓ 나이지리아는 '주민등록증+운전면허증+의료보험증+연금+선거+전자여권+신용카드'(2010-18)
: 4천만 장 이상이 발행되어 'Anytime, Anywhere+핀테크를 구호로 아프리카 선도주자'이다.

DIGITAL ID는 재난/전쟁시에도 활용

■ 전자 정부의 연속성을 보장하기 위한 시스템을 갖추어야 한다.

- 전자정부는 지진/재난/홍수/급변사태 등 어떤 상황에서도 해킹이나 인터넷 연결 끊김, 본인 확인 등 '전자신분증'으로 된 스마트Key를 활용할 수 있는 시스템을 먼저 갖춰야 한다.

: 스마트키(Smart Key)를 온라인은 물론 오프라인, 특히 전쟁·지진이나 재난 같은 상황 구현

- 지문 등 생체인증을 통한 스마트 보안 기술은 결제는 물론 자율주행차·스마트홈·스마트시티·사물인터넷(IoT) 등에서 필수여서, 사물인터넷(IoT) 기반 스마트홈, 스마트 카, 스마트 시티 등에 적용할 '스마트Key' 시스템을 구축해야 한다.

: 대규모 정전 및 지진이나 해킹 등으로 인해 모든 인터넷이 마비돼도 시민 본인을 인증할 수 있는 '전자신분증과 Digital ID'를 발급해 운영해야 한다.

- 전쟁, 재난에도 무너지지 않아야 한다.
✓ 군인 신분증이나 공무원 카드도 지문 카드로 교체하면 컴퓨터 접속과 비밀문서 접근 관리는 물론 전시나 사이버전에서 인터넷·통신이 두절돼도 오프라인 접속이 가능하고 여러 가지로 행정 효율성도 제고할 수 있다.

[그림 8] 인도와 나이지리아의 다목적 생체전자신분증(2015년 기준)



• 정보통신기술(ICT) 융합이 핵심인 4차 산업혁명 시대에 모든 것이 연결된 사회에서 ‘블랙아웃(대규모 정전 사태)’ 이나 사이버 테러가 발생하면 어떤 상황이 벌어질까를 준비해야 한다.

✓ 당장 본인을 인증할 수 있는 수단이 모두 차단된 이용자는 인터넷이 복구될 때까지 집안 생활자전이나 자율주행차 등을 제어할 수 없게 될 것이란 관측이 나왔다.

: 이에 따라 온라인은 물론 오프라인 환경에서도 지문, 홍채, 안면인식 등 강력한 생체정보를 기반으로 이용자 스스로를 입증할 수 있도록 ‘오프라인’에 대한 사회적 시스템을 구축해야 한다.

DIGITAL ID의 급변사태 대비 활용

지능형 정부에서는 4차산업혁명의 서비스 구현과 스마트시티 같은 부분은 중요하지만 국제 정세를 감안, 재난 및 급변사태에 따른 대비책도 동시에 수립해야 하며, DIGITAL ID도 동시에 제공되어야 한다.

미국과 중국이 코로나바이러스로 무한 충돌의 움직임을 보이고, 최근 북한 지도부의 ‘사망설, 중병설 등’으로 한반도의 정세가 일촉즉발의 위기를 보이고 있으며, 최근 북한이 잠수함 핵무장과 장거리 미사일 도발이 예측되면서 한반도 상공에 각종 미국 정찰기들이 24시간 감시를 하고 있고, 중국과 대만의 대립으로 4개의 미국 항공모함 전단이 동북아로 몰려오는 상황이 매년 발생하고 있다.

각종 분야의 국제정치 분석보도를 보면, 북한의 (피)난민의 유입을 봉쇄한다는 ‘중국 정부의 정책으로 북한과 중국의 국경지대에 군대가 배치되고, (피)난민을 수용할 준비를 하고 있다’라는 외신도 나오고 있다. 특히, 북한 핵무기와 화생방 무기 등의 2/3 이상이 북중 국경에 배치되어 있으며, 중국은 군사력을 가진 북한군 탈영 병력 등의 중국 국경유입을 걱정하고 있지만, 본질은 ‘핵무기 통제력을 상실하거나 핵물질 유출 사고가 발생하면 최대 피해자는 중국이 될 수도 있다’라는 계산도 하고 있다.

이에 비해, 정부는 중무계획으로 알려진 ‘전시 피난민 구호 및 수용 대책’을 위해서 매년 을지연습 기간 동안 부처별 대응 등으로 훈련을 하고 있고, 일본 아베 내각은

한반도에서 밀려오는 피난민들에 대해서 ‘선별적 수용’을 밝혀, 한국인들의 분노를 산 적도 있다.

통일부는 정책상 기밀로 분류하면서 훈련 내용을 취급하지만, 주요 내용은 ‘유사시 북한에 머무는 우리 국민의 철수와 북한 피난민 수용 계획’을 주 내용으로 하는 ‘총무 3300 계획’과 유사시 북한 수복 통합 계획인 ‘총무 9000계획’을 발전시키고 있다”고 일부 언론에 알려진 바 있다.

지능화정부는 급변사태에 대비하여 피난민 규모가 1백만 명 정도가 아닌 예상보다 많은 5백만 명~1천만 명 이상으로 단기 1~2개월 간에 폭발적인 증가를 보인다는 전제 하에 유엔 등 국제기구와의 협력관계를 사전에 준비해야 하며, 한국 전쟁 시 ‘거제도 포로수용소’ 운영사례 등 대규모로 복수의 난민촌 설치 및 건설같은 신속한 이행계획 부분에서 인터넷, 피난민 등록 등 지능화 정부와의 연계를 고려해야 한다.

독일은 분단된 1949년부터 90년 통일되기까지 동독에서 서독으로 넘어온 피난민은 520만 여명이었다. 서독은 당시 동독주민 수용법을 제정, 동독을 탈출한 주민 전원을 수용하기로 했다. 서독은 80년대에 동독 주민의 서독 이주를 조건으로 동독에 경제지원을 실시하기도 했다. 지구상에 유일한 분단국가인 한국도 동·서독의 사례를 하나의 교훈으로 하고 있지만 이에 더해 급변하고 있는 2021~ 2025년도의 현실에 맞는 정책을 수립해야 한다.

실례로 유엔은 시리아전쟁으로 발생한 시리아난민을 최초 50만~백만 명으로 예측하고 준비하던 중, 전쟁의 확산으로 10배 이상인 5백만 명 이상으로 불어나면서, 유엔은 사상 초유의 혼란을 겪고, 미국/EU등 주요 예산 지원국들과 정책적인 대립을 했던 경험을 바탕으로, 한국 지능형 정부가 대비할 필수 교훈으로 삼아 ‘정책 대안’을 제시해야 한다.

일단, 한반도의 현실로 보면, 시리아 난민은 요르단 등 사막지역에 배치하는 장소가 마련될 수 있었지만, 하루 저녁에 2~3만 명 혹은 1주일에 10만 명 이상이 늘어나

는 시기에 ‘난민 캠프’를 신규로 확장하고 난민들을 배치 하는데 모든 혼선과 운영 불편 등 예상 밖의 상황이 노출 되는 상황에서, 지능화 정부가 제공하는 인터넷 및 대규모 등록에 제공하는 서버 등이 ‘정부통합전산센터 등’에 안전하게 연결되어야 한다.

주요 사례중, 언론에도 잘 알려진 요르단 자타리캠프는 1년도 안돼 10만 명에서 70만 명 이상으로 늘어나고, 몇년 뒤에는 난민캠프 수용을 포기하고, 도시 내에서 방을 빌려서 월세바우처 등을 지원하는 다양한 정책을 급조해서 적용한 바 있다.

국내에는 주로, 산악 지역인 경기/강원도는 1백만 명 단위의 (피)난민캠프를 10여 개 이상 설치할 장소나 필요 부지와 인프라를 수용할 만하지 아니면 어디가 좋은지를 네트워크 인프라와 캠프 단위의 ICT 용량 등 적정성을 고려해서 준비를 해야 하며, 피난민 정보에 대한 해킹 등을 대비하여, 보안관제센터를 24시간 가동해야 한다.

가. 미국 클린턴 대통령이 세운 ‘재난 시나리오..’를 참조

- 2시간 후, 시민은 버스/전철/기차에서 하차
- 4시간 후, 주유소는 정전으로 문을 닫는다
- 6시간 후, 슈퍼마켓은 현금만 받는다
- 8시간 후, 은행ATM을 가보지만 닫았다
- ‘성난 시민들은 거리를 배회, 야간이 되자..일부 굶주린 시민이 폭도가 된다.’

나. 국내 재난대책/급변사태 수립시 ...망각하는 주요 현상

- 전기와 인터넷 전면 중단 시 대책
- 시민은 식량/식수가 필요..그러나 슈퍼마켓은 현금만 취급
- : 슈퍼마켓에 식량은 있지만 카드를 안 받고, 은행 ATM에 현금은 있지만, 카드는 안되고.. 스마트폰은 먹통이며, 앰불런스는 오지 않는다.

지능화정부는 ‘난민 1인당 식권 등을 담은 바우처 지원예산과 이를 제공하는 안전한 바우처 생체카드를 제공하기 위한 세부 설계와 배포시스템’을 산정해야 한다. 시리아난민 사태에서, (피)난민들은 지원하는 미국/영국/캐나다/EU는 ‘난민 발생 초기부터 시리아 (피)난민’은 5백만 명을 제시하는 유엔난민기구에 2백만 명 정도로 인정한다면, 자금을 일부만, 혹은 50% 이하만 지원한 바 있어서, 난민 전체 인원 및 이를 증명하는 ‘생체난민 등록시스템’이 설계되어야 하고, 최근 유엔난민기구는 파키스탄에서 이를 시행한바 있다.

이는 유엔난민기구(UNHCR)과 세계식량기구(WFP) 등에서 전세계에 제공하고 있는 ‘Biometric’시스템과 연동되어야 한다. 유엔은 20여 년간 난민들의 지문 2개를 수집한 데이터베이스를 운영하다가 2014년부터 ‘지문, 홍채, 얼굴 등’ 멀티생체 인증사업을 미얀마, 아프리카 등에서 진행했고 이를 위한 ‘생체지문카드’도 2021년 2월 결제시스템을 지원하는 용도로 도입 중이다. 세부적인 내용은 2021년 중 파키스탄의 난민캠프에 체류 중인 아프간 난민 140만 명에 대한 생체카드발급을 목적으로 현재 8천 명에 대한 시범사업을 진행 중이다.

유엔난민기구가 예산 산정에 필요한 근거가 필요한 이유는 그 동안 (피)난민에게 지급한 것은 ‘종이로 된 흑백 난민 증명서’로 지급하다가 현재는 플라스틱카드를 지급하고 있지만 소지만으로는 난민 지위를 인정받는데 한계가 있다. 문제는 플라스틱카드는 난민캠프에 도착 후, 안정적인 단계에서 단계별 등록절차와 인터뷰 후, 사진 등을 넣어 발급하기에 초기 1~2개월 대응에서는 사용할 수 없다는 한계가 있다.

난민캠프 운영에 대해 전반적인 재정을 지원하는 각국은 유엔이 운영하는 난민캠프에서 총인원에 대한 산정근거가 부족하다고 지적하면서, 예산을 삭감하고 유엔은 은행에서 대출을 받아 (피)난민 살림을 유지하고 있으며, 얼마 전 신임 유엔사무총장은 ‘유엔의 재정 부도를 경고하며, 전세계 국가에 밀린 유엔분담금’을 내라고 촉구한 바 있다.

유엔은 (피)난민캠프에 도달한 난민들에게 사용하는 식량과 비누, 식용유 등을 받을때 사용하는 종이카드를 사용 중인데, 배급 시 명단대조와 지급 확인을 하느라 줄을 하루 종일 서서 식량 배급을 받아야 하고, 편칭으로 구멍을 내서 구별한다

불행하게도, ‘임시 수용시설’ 혹은 ‘(피)난민 캠프’에서 가장 문제가 되는 것은 ‘식량, 생필품, 텐트, 생수’ 등을 지급받았는가와 중복지급을 증명할 방법인데, 유엔은 ‘종이식권’에 날짜별로 구멍을 내고, 명단목록에서 표시하는 것으로 하고 있다.

이를 통해 지능화 정부는 어떤 ‘디지털 신분인증’을 준비해야 하는지를 예측해야 한다.

밀려오는 이재민, (피)난민에게 지능화 정부는 어떤 디지털 증명서를 무엇에 담아 발급할 것인가와 이에 대한 효력을 국제적인 표준으로 공인받을 지에 대한 검토가 필요하며, 요르단, 케냐 등 많은 국가는 자국민과 구별을 위하여 별도의 ‘(피)난민 플라스틱 카드’를 발급하기도 한다.

한국은 기존의 주민등록증을 (피)난민에게 발급할 것인지 검토가 필요하다.

- (피)난민에게 필요한 식량, 텐트, 식수, 담요, 의료 지원 등을 하면서 “중복지급”에 대한 대책은 어떻게 세워야 하는 지를 민간산학중심으로 논의해야 한다.
- 간단한 의료지원이나 코로나 등 전염병주사 등 조치 완료된 난민대상을 구별할 방법과 최근 코로나 바이러스 ‘Health Passport’ 같은 전염병 증명서도 제공되어야 한다.

최근 유엔은 2014년부터 ‘(피)난민 생체DB’를 구축하고 있는데 ‘지문 10개+홍채+안면’의 멀티 생체데이터베이스를 구축하고 있다. 유엔이 검토중인 생체지문카드는 ‘자신의 지문을 스마트카드의 IC칩에 저장하여, 본인이 Matching On Card’ 방식으로 본인 증명을 할 수 있으며, 2017년 30개 유엔회원기관의 공인을 받은 ‘물리적 생체출입증’은 2019년 국제통신연합(ITU)를 시작으로 단계별로 30여개 유엔기관에 실시할 것을 공표하였으나 ‘(피)난민 생체카드’는 예산을 이유로 아직 적용되지 못하고 있다.

결론

급변사태, 지진/홍수 등 어떤 상황에서도 전자정부서비스와 ‘DIGITAL ID’는 제공되어야 한다.

유엔 등 60여 개국이 실시하고 있는 생체정보를 이용한 다목적 스마트 Key(전자신분증)를 구축해서 국민이 전자정부접속시 ‘One Card’에 DIGITAL ID를 발급해 모든 민원을 해결해야 한다.

일반 공무원증 / 경찰 신분증 / 군인 신분증 / 전자신분증이 발급돼서 카드 1장으로 ‘출입증 + 컴퓨터 접속 + 전자정부’ 이용이 가능해야 한다. 최근 스마트폰의 모바일 공무원증, 운전면허증 등은 인터넷이 두절되면 무용지물이다.

한국의 장점을 활용해야 한다. 한국은 전국 주민센터에서 지문만으로 주민등록등본 등 100여 가지를 발급하는 유일한 국가이다. 전국 기차역, 터미널 그리고 쇼핑센터 등에 설치된 5,000여 대 무인민원발급기로 100여 가지 정부공식문서를 발급하는 최고의 지문인증 선진국이다.

사이버전쟁으로 인터넷이 중단돼도, 전자정부는 ‘무정지 운영’이 가능해야 한다.

오프라인에서 국민이 ATM에서 현금인출, 슈퍼마켓에

서 POS로 물건구매가 가능하다. 블록체인 방식으로 복수의 전산센터에 저장된 ‘전자정부시스템’이 재난 후 신속히 연결되어 급변사태 이전의 시스템으로 신속히 복구 및 시민 서비스가 제공되어야 한다.

시민불편 해소를 위해 전자정부는 ‘재난 시, 슈퍼의 식량을 구입할 방법’을 제공해야 한다.

급변사태시 주변의 슈퍼마켓에서 인터넷 / 통신이 두절되도 물건을 사고, 온라인으로 돌아갈 때 정산할 방법을 제공해야 한다(기술적으로 가능하기에 정책만 변경된다면 실현 가능할 것이다.).

유럽연합은 6월 1일 ‘디지털 신분증 지갑’을 발표하면서, 모든 공공/민간 서비스에 사용을 선언했다.

한국이 최근 운전면허증 등 신분정보를 스마트폰에 담는 것은 초기 단계의 서비스이지만 유럽연합의 발표는 한국은 플라스틱 주민등록증을 쓰는 원시적인 형태에 남아 있고, 유럽은 디지털 신분증 지갑으로 메타버스에서 사용할 수 있음을 의미하는 바, 국가적인 논의가 필요한 시점이다.

참고문헌

최운호(2020). 급변사태(통일 등)에 대비한 유엔 지원과 (피)난민 정책 국가미래연구원 News Insight

최운호(2019). 4차산업혁명, 한국만 첫 단추를 잘못 끼웠다 국가미래연구원 News Insight

최운호(2018). ‘생체인증은 오프라인과 온라인에 모두 사용할 수 있다.’ - KT 통신구 화재나 지진시, 대책에 활용 - News Insight

최운호(2018). “5G 시대에 생체인증 ‘스마트 키(Smart Key)’ 도입하자” - 정전·지진·해킹으로 인터넷 끊겨도 본인인증 가능- 국가미래연구원 News Insight

최운호(2017). 스마트시티의 Smart Key. 지역정보화 이슈 리포트, 9호

최운호(2017). ‘블록체인 전자정부 2030과 스마트Key(전자 신분증)’ - Anytime Anywhere based Online & Offline - News Insight

UK Gov, The UK digital identity and attributes trust framework(Feb 2021)

Secure Identity Alliance GIVING VOICE TO DIGITAL IDENTITIES WORLDWIDE(Feb. 2021)

Apple Car Key <https://developer.apple.com/videos/play/wwdc2020/10006/>

CCC Standard 2.0 https://global-carconnectivity.org/wp-content/uploads/2020/04/CCC_Digital_Key_2.0.pdf

EU to step up digital push with digital identity wallet -The digital identity wallet "can be used anywhere in the EU to identify and authenticate for access to services in the public and private sectors
<https://www.reuters.com/business/finance/eu-step-up-digital-push-with-digital-identity-wallet-2021-06-01/>

저자 소개

최운호(전 유엔난민기구 최고정보보호책임자)

최운호박사는 유엔 등 글로벌 정보보호 전문가이고, WSIS 2015 / ID World 등 글로벌 컨퍼런스에서 기조강연(Key Note Speaker) 등 국내외 조직에서 경험을 쌓은 페이먼트, 사이버전쟁 전문가이다.

최근까지 한국인으로는 최초로 유엔난민기구(UNHCR) 최고 정보보호책임자를 역임했으며, 이전에는 도로교통공단에서 정보보호단장(CISO), 금융결제원, 인터넷진흥원 등 정보보호 관련 주요 직책을 역임했다.

‘One UN Card’라는 유엔신분증과 유엔난민카드를 개발했고, FIDO 국제 생체표준보다 앞서서, 2012년 유엔 최고정보보호 책임자(CISO)회의에 기술을 설계/제안했다.

글로벌IT 공동들이 시행중인 생체인증, 생체페이, AI로 연결된 사물인터넷 그리고 스마트자동차Key 등의 관련 기술에 대한 국제/국내 특허를 개인적으로 50여개 보유한 핀테크, 전자화폐, 메타버스 등의 전문가이다.