One ID 본인인증과 FIDO2.0 거래인증 활용

Application of One ID Certification and FIDO2.0 with Transaction Certification

유 미 영*, 이 재 형*, 강 민 구**

◈ 목 차 ◈

1. 핀테크와 본인확인 및 인증방식 분석

최근. 금융과 ICT 기술이 융합된 핀테크 기술은 지문과 홍채 등의 생체인증을 위한 스마트 디바이스 제조업체와 플랫폼 기반의 단말기 인증을 통한 지불, 결제수단 등에 활용되고 있다[1].

생체인증을 통한 다양한 컴퓨터 등 스마트 단말의 정보보안과 로그인의 본인 인증을 받는 5G 등의 모바일 인터넷 전자 상거래에 활용되고 있다.

1.1 핀테크 성장과 생체인증 및 단말인증 동향

스마트 디바이스의 단말 인증을 통한 비대면 전자거래에서 생체인증 기반의 본인 인증 등 빅 데이터 및 인공지능 활용을 통한 핀테크(IT·금융 융합, Fintech)가 발전하고 있다[1][2].

〈표 1〉 생체인증 기반의 핀테크 적용 사례 비교

분야	세부 활용
금융	ATM · 키오스크(KIOSK)[1], 스마트뱅킹, 전자(간편)결제 등
컴퓨터	PC · 노트북 · 스마트폰 · 네트워크 로그인 및 접근 제어 등
의료 · 복지	환자신원확인, 원격진료, 전자 처방전, 진료기록 관리 등
출입통제	주요 시설물 출입관리, 근태관리 등
공공 부문	출 · 입국심사, 증명서발급, 전자신분증, 선거관리, 범죄자관리 등
사회 복지 부문	연금지급관리, 기타수당관리 등

자료 : 바이오인식정보시험센터 자료 재구성

특별히, 블록체인과 생체인증 등 다양한 인증수단이 확산 및 생체인증 수단의 지문인식을 활용한 삼성 페이는 단말기에서 홈 버튼 지문인증을 통한 핀테크 기반의 거래가 활발해 지고 있다.

스마트 단말기의 생체정보를 활용한 사용자 인증을 통한 무인점포용 디바이스가 활용되고 있다.

이러한 핀테크 기술의 발전과 생체인식기술을 적용을 통한 다중 인증방식 도입을 통해 비대면 계좌 개설용 실명확인 방식으로 금융권에 빠르게 도입되고 있다[1][2].

〈표 2〉 바이오 정보유형에 따른 인증방법과 특징분석

분야	바이오정보	인증 방법	특징
신체적 특징	지문	지문의 형상적 특징을 비교	• 편의성, 센서 소형화 수준 높음 (스마트폰 내장) • 땀, 먼지 등에 의한 인식률 저하
	홍채 · 망막	홍채의 무늬 · 형태 · 색, 망막의 모세혈관 분포 패턴 비교	• 낮은 오인식률 • 위조가 어려움 • 눈을 뜨고 있어야 하는 불편함
	정맥	손바닥, 손가락 등의 정맥 분포 패턴 비교	• 위조가 어려움 • 높은 시스템 구축 비용
	얼굴	눈, 코, 입 등 3차원 얼굴 형상 비교	• 낮은 시스템 구축 비용 (스마트폰 카메라 및 웹캠 등 활용가능) • 주변 환경, 노화 등에 의한 인식률 저하
행동적 특징	서명	서명과제(속도, 필압 등), 형상 비교	• 낮은 시스템 구축 비용 (스마트폰 터치스크린 활용가능) • 서명 복제 및 위조 가능
	음성	개인 고유 음성패턴 비교	• 전화 · 인터넷 등으로 원격 인증 가능 • 복소리 및 주변 환경에 의한 인식률 저하 • 녹음을 통한 도용 가능

* 옥타코주식회사
** 한신대학교 IT콘텐츠학과

〈표 3〉 생체인증 인식률(거부율FRR/수락율FAR) 분석

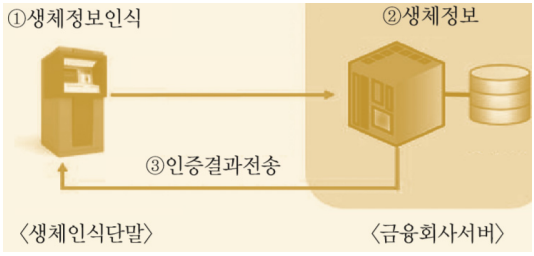
구분		본인거부율(FRR)	타인수락률(FAR)
지문		0.1%~0.5%	0.001%~0.01%
홍채		0.0001%~0.1%	0.000083%~0.0001%
정맥	손바닥	0.01%~0.1%	0.00008%~0.0001%
	손가락	0.01%~0.3%	0.0001%~0.001%
얼굴		1%~2.6%	1%~1.3%

자료 : 금융결제원, 바이오인식 기술의 금융서비스 적용 현황 및 발전과제, 2014.7.

스마트 고객을 위한 바이오 생체 인증방식은 스마트폰에서 금융서비스에 사용할 때, 패스워드 입력 등 불편함을 해소할 수 있으며, 높은 보안성과 빠른 검증속도로 사용자 편의를 극대화할 필요가 있다[1][2].

1.2 비대면 생체인증 방식의 활용과 비교분석

핀테크를 위한 모바일 기반의 비대면 확인과 신용카드 및 계좌 확인 없이도 이용할 수 있는 서버 저장방식과 생체인식 단말에 저장되는 FIDO (Fast Identity Online) 방식 등을 통한 단말인증 등의 핀테크가 급격히 발전하고 있다[1][2].

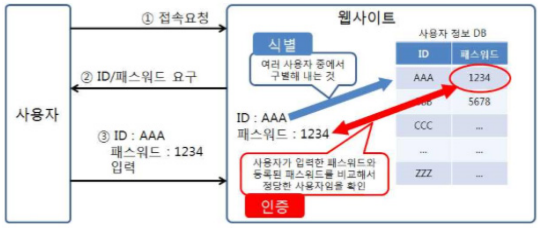


〈그림 1〉 생체인증 정보의 서버 저장 및 비교 방식분석

〈그림 2〉 생체인증 단말저장 및 FIDO서버 연계분석

2. One ID 인증과 디지털원패스 활용

최근까지 공인인증서의 복잡한 본인확인/인증방식과 단말인증 및 액티브 X 사용 등으로 인한 핀테크의 금융거래로 인한 고객 불편했지만, 개인인증을 위해 휴대폰 SMS와 OTP, 생체인증 등 인증수단 다양화하고 있다[3].



〈그림 3〉 본인인증과 식별ID저장 및 본인확인 절차분석

1999년에 도입된 공인인증서는 금융·상거래·민원행정의 전자서명 등에 활용하게 되었다. 그러나 공인인증서가 공공분야의 로그인 등 본인인증에 사용하게 됨에 따라, 민간인증 발전의 저해와 액티브 X 설치 등으로 어려움이 고조되었다.

이에 국민의 인터넷 이용환경 개선을 위해 2020년까지 액티브 X 제거 및 불필요한 공인인증 절차를 폐지할 예정이다. 안전한 온라인 거래를 위한 사용자의 식별(Identification)방식과 인증기관을 통해 발급된 인증서 및 개인키 형태의 OTP 단말 등이 활용되고 있다. 사용자 본인확인의 정의와 방식 및 FIDO의 정의는 아래와 같다[3].

○ 본인확인 : 전자적인 온라인 방식으로 제시된 이용자 신원확인에 대한 신뢰성을 확인절차
(휴대폰인증, 공인인증서, 아이핀, 카드인증 등을 이용한 이용자의 신원을 확인함)
- 본인확인 방식 : 대면 확인과 비대면 확인
1) 대면확인 : 주민 센터와 은행창구 등에서 서면작성에 자필증거로 사용자 확인
2) 비대면 확인 : 전자금융서비스, 온라인 거래 등 안전한 온라인 서비스를 위한 사용자 식별(Identification)과 인증(Authentication) 필요함

○ 본인(사용자) 인증 : 사용자 확인을 위한 하나로 된

인증방식, 로그인하는 사용자가 웹사이트에 등록된 사용자 여부를 확인하는 방법 및 절차

○ FIDO(Fast IDentity Online) : 사용자의 편리성을 위한 국제표준 생체인증 기술규격이며, GFIDO는 FIDO 기술 규격에 따라 구축한 정부 생체인증 공통기반 서비스

○ 디지털원패스(Digital Onepass) : One ID로 사용자 본인이 선택한 인증수단으로 여러 전자정부 서비스를 이용할 수 있는 사용자 인증 서비스

아래 [표 4]처럼 사용자 인증을 위한 본인 인증수단 인증 특성에 따라 지식기반과 소지기반, 생체기반 및 행동기반 으로 분류하고 있다[3].

〈표 4〉 인증수단과 요소별 특징과 예시 분석

분 류	설명	예시
지식기반	- 사용자가 알고 있는 지식을 활용하여 사용자를 인증하는 방법	- ID/PW 또는 식 인증 등
소지기반	- 사용자가 소지하고 있는 인증수단을 활용하여 사용자를 인증하는 방법	- OTP, 휴대폰SMS, 공인인증서 등
생체기반 (특성기반)	- 사용자의 생체정보를 활용하여 사용자를 인증하는 방법	- 지문, 홍채, 정맥 등
행동기반 (습관기반)	- 스마트폰, 스마트패드 등을 통해 서명을 하거나 키보드를 통해 정보를 입력할 때 사용자의 행동 패턴을 분석하여 인증하는 방법	- 키보드 타이핑 행위 - 서명패턴 등
단일인증	- 한가지의 인증요소를 이용하여 식별자의 신원을 검증하는 방식	- ID/PWD 등
다중인증	- 두가지 이상의 인증요소를 함께 사용하여 안전성 및 보안성을 높여 인증하는 방식	- ID/PWD+OTP - ID/PWD+ARS 등

2.1 국내 사용자 본인인증 방식과 활용분석

공인인증서를 사용하는 이용자가 PC에 액티브 X 등의 설치가 필요 없는 노플러그인(No-plugin) 방식인 카카오페이의 사용자 본인인증 절차를 대표적이다.

이러한 카카오톡 앱 사용자가 모바일(스마트폰)앱 기반의 카카오 톡으로 전달된 인증요청 메시지를 이용자가 확인 후 인증할 수 있다.

이때, 노플러그인 인증서는 카카오 톡 모바일 앱 내 저장 되며, 사용자 본인인증이 필요할 때 마다 호출하여 사용자를 ID를 인증할 수 있다.

이러한 카카오의 노플러그인 인증서는 워크넷, 한국교통안전공단 자동차검사고지안내 서비스 등의 공공분야에 활용되고 있다. [표 5]는 노플러그인 기반의 브라우저와 모바일 및 클라우드 인증기술에 관한 사용현황을 분석하고 있다[3].

〈표 5〉 국내 노플러그인 인증기술과 사용현황 분석

기술	내용	적용사
브라우저 인증서	공인인증서를 브라우저의 저장공간에 발급 받아 인증하는 방법 ※ 금결원에서는 브라우저 공동저장소를 만들어 여러 인증서 공유기능 제공	금결원, 코스콤, 한국정보인증, 한국전자인증, 이니텍
모바일 인증서	공인인증서를 모바일의 안전한 저장소에 발급 받아 인증하는 방식	금결원, 코스콤, 한국정보인증, 한국전자인증, 이니텍
클라우드 인증서	공인인증서를 클라우드 저장공간에 발급받아 인증하는 방식	한국전자인증, 한국정보인증

2.2 글로벌 사용자 본인인증 표준과 활용분석

글로벌 주요 국가의 사용자 인증수준 분류방법과 국제 표준방식은 무인증과 기관 내부용 수준을 포함한 4단계로 분류하며, 운영하고 있다.

대국민의 공공 서비스 인증의 보안수준은 인증오류 위험도와 요구되는 본인확인의 신뢰도에 따라 3단계로 분류하고 있다.

사용자 인증의 보안관리 대상은 국가별 공공기관의 업무용 수준을 제외한 대국민 공공서비스를 관리범위로 정하고 있다[3].

〈표 6〉 글로벌 사용자 인증표준과 공공서비스 레벨분석

※ LoA(Level of Assurance, 이용자 신원의 신뢰도)

보안수준	구분	내용
매우높음	수준4 (LoA 4)	• 하드웨어 암호화기반 인증수단 (전자서명 적용) • 대면인증 필수 또는 이에 준하는 수준의 신원확인
↑	수준3 (LoA 3)	• 지식인증과 소지인증 필수 • 일반적인 수준이상의 엄밀한 신원확인
	수준2 (LoA 2)	• 소지기반 인증 또는 이에 준하는 보안수단 필수 • 신원의 신뢰성있음(일반적인수준의 신뢰수준)
낮음	수준1 (LoA 1)	• 아이디/패스워드, 싱글팩터 • 신원확인절차가 없거나 신원의 신뢰성을 요하지 않음

사용자 인증을 통한 본인 인증수단으로 스마트 UI와 사용자 경험(UX, User experience)은 이용자의 용이성과 효율성, 기억성, 오류성, 및 사용자 만족성 등을 고려한 아래와 같은 디자인 요소를 고려한다[3].

○ 로그인용
1) 전체화면 : 탭(Tab)형, 나열형
2) 화면일부 : 탭(Tab)형

○ 본인확인용 : 나열형

○ 전자서명용 : 나열형, HTML5 툴킷형

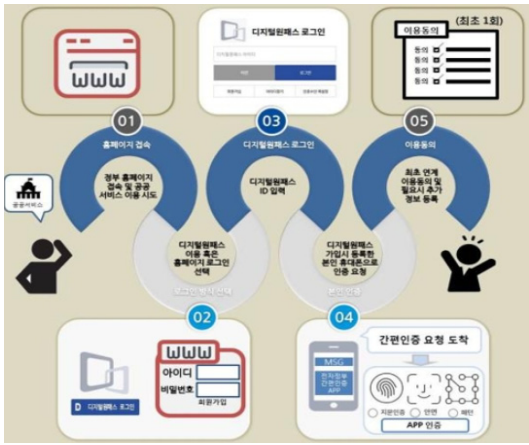
2.3 디지털원패스 기반의 본인인증과 공공활용

정보통신망법 제23조의2에 따라 정보통신서비스제공자는 본인확인과 본인인증 절차에 따라 공공서비스가 가능하다[3][4].

하지만, SMS나 ARS 등 2채널 다중인증 방식의 허점이 드러나면서 사용자의 본인인증 기술이 발전하고 있다. 그동안 USIM과 통신사의 단말정보를 활용한 인증방식 및 V3 Mobile Plus기술 등이 모바일 금융거래 보안 솔루션에 활용되고 있다.

행정안전부는 금년6월 온라인 공공서비스를 위한 본인인증으로 '디지털원패스'를 발표했다[4].

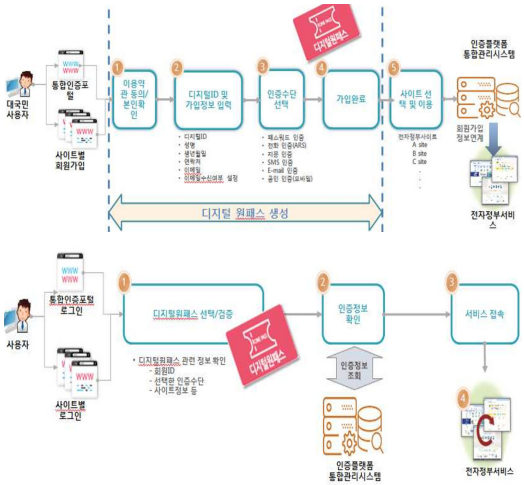
[그림 4]와 같은 디지털원패스의 간편 본인인증 절차와 서비스는 네이버나 카카오, 구글처럼 홈페이지 마다 별도의 회원을 가입할 필요 없이 하나의 아이디(One ID)로 본인이 선택한 인증수단인 비밀번호와 공인인증서 및 지문·안면인식·패턴 등 을 사용해 여러 공공서비스가



〈그림 4〉 디지털원패스의 간편 본인인증 절차와 서비스

가능하다.

[그림 5]는 다양한 공공서비스를 하나의 디지털원패스를 활용하기 위한 회원가입과 본인인증 절차에 관한 블록도이다[3].



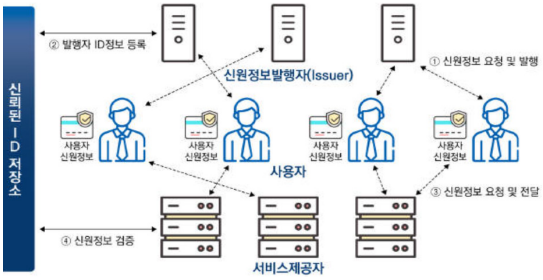
〈그림 5〉 디지털원패스 회원가입과 본인인증 절차분석

3. 블록체인 DID와 FIDO2.0활용분석

3.1 블록체인 기반 분산ID(DID)와 본인인증

금융위원회는 최근 6월에 블록체인 기반 분산ID(DID,

Decentralized ID) 서비스로 아이콘루프와 파운트의 비대면 본인인증으로 계좌개설 과정에 실명을 확인하는 절차를 간소화하기 위한 본인확인 방식을 발표했다[4].



〈그림 6〉 블록체인 기반 DID 서비스 절차분석〔4〕

DID를 통한 비대면 계좌 개설시 다음 5가지 방법 가운데 두 가지 이상의 본인확인 방법으로 고객의 실명을 확인해야 한다[4].

1. 실명확인증표 사본 확인
2. 영상통화
3. 위탁기관을 통한 실명확인증표 확인
4. 이미 개설된 계좌와의 거래
5. 1~4외의 새로운 방식

이러한, 전자신분증 하나만으로 로그인 절차와 배송지 입력 등 번거로운 절차 없이 전자상거래가 가능하다. 또한, 은행, 카드, 증권 등 각종 금융서비스도 손쉽게 이용할 수 있다.

아울러, 삼성전자 휴대폰에 디지털신원인증·모바일 신분증(DID)을 내장함으로서 어제, 어디서나 쉽게 금융거래가 가능하다.

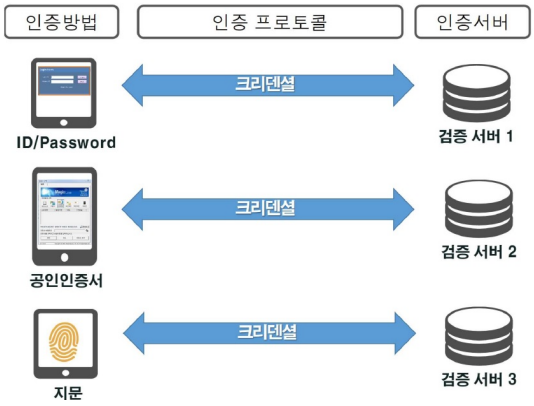
이로서, 미래의 신분증은 주민등록증 및 운전면허증 등 실명확인징표와 통신사의 휴대폰 본인 인증 정보, 전자서명을 위한 각종 인증서, 금융회사별 계좌번호와 같은 각종 금융정보를 휴대전화 앱에 저장하는 방식이 존재할 수 있다.

3.2 블록체인/생체 본인인증 및 FIDO2.0활용

생체 인증정보를 이용한 사용자를 인증기술은 블록체인 사용자 ID 관리기술과 접목을 통해 블록체인 상에서 FIDO2.0 및 블록체인 활용한 차세대 인증서비스로 확장될 전망이다[5][6].

이때, 다양한 다중생체 인증 수단을 결합한 '복합인증'을 통한 사용자 본인인증 방식을 거래인증 수단인 FIDO2.0의 다양한 생체인증 수단을 활용할 수 있다. 이로서, 고객이 스마트 청구서를 조회할 때 거래인증 상황에서 사용자 본인확인 및 인증을 FIDO인증으로 진행할 수 있다[5][6].

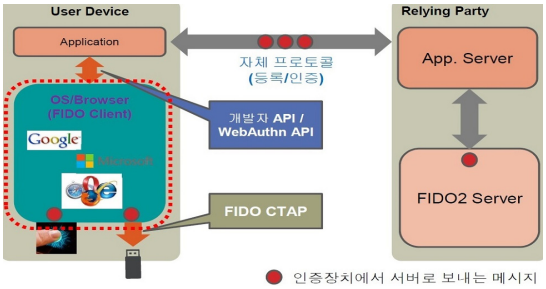
'FIDO2'에 포함된 '웹 인증'을 W3C(World Wide Web Consortium)에서 웹 표준으로 지정되W3C는 웹 API(Application Programming Interface) 사양을 기반으로 온라인 서비스 제공자와 웹 개발자에게 '웹 인증'의 도입이 가능하게 되었다[6].



〈그림 7〉 FIDO 인증이전의 인증방법 분석(출처:ETRI)

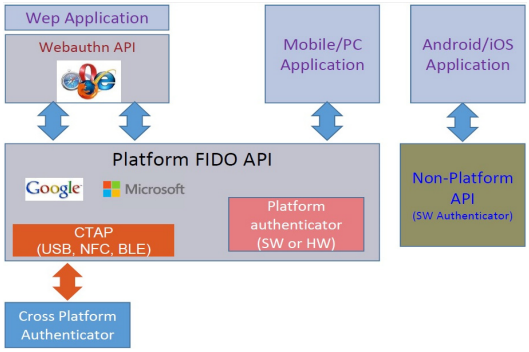
이러한 '웹 인증'은 인터넷 사용자들이 여러 웹 사이트 및 디바이스에서 안전하게 생체인식, 모바일 인증, 블록체인 등 고객이 원하는 인증방법으로 인증할 수 있다. 특별히, 웹 브라우저 및 연계된 웹 플랫폼 인프라에 표준화된 API 정의를 내려 사용자 본인인증 기능이 가능하다[6].

[그림 7]처럼 FIDO는 아이디와 비밀번호 조합한 사용자 본인인증 대신 지문, 홍채, 안면인식, 목소리, 정맥 등 생체인식과 OTP 등의 인증 체계를 지원하는 사용자 본인 인증 시스템이다[6].



FIDO2.0 구조(출처: ETRI)

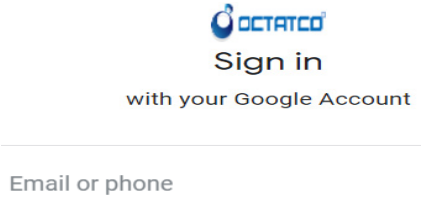
〈그림 8〉 'FIDO2.0'에 포함된 '웹 사용자 인증구조[6]



〈그림 9〉 FIDO2.0 사용자인증 장치분석(출처:ETRI)

특별히, FIDO는 사용자 본인인증 기법과 인증정보를 주고받기 위한 인증 프로토콜을 분리한 것이다. 이로서 분리된 생체정보 전송의 위험성과 저장된 생체의 사용자정보에 대한 해킹 가능성을 원천 차단할 수 있다. FIDO2.0이 적용될 경우 생체인증의 활용범위가 확대될 것 이다.

스마트폰에 한정됐던 FIDO 1.0에 비해 FIDO2.0은 PC나 웹 브라우저 등 모든 플랫폼에서 사용한다. 또한, 온라인 이외에 오프라인까지 확장될 것이며, IoT 환경에서 사용자 본인인증 기술로 활용 범위가 크게 확대될 것이다[5][7][8][9].



https://fido2.octatco.com:9492/webauthn/login-google.html

〈그림 10〉 FIDO2.0인증서버(옥타코) 사례(화면캡쳐)

4. 고찰 및 결론

본 연구에서는 스마트 핀테크 시대에 맞는 사용자 본인 인증의 중요성이 확대됨에 따른 다양한 본인확인 및 사용자 인증방식을 비교 검토하였다. 아울러, 안전한 온라인 공공 서비스를 위한 사용자 식별과 디지털원패스(Digital Onepass)에 의한 하나의 아이디(One ID)로 본인이 선택한 인증수단의 활용 및 민간분야 사례를 분석하였다.

블록체인 분산ID(DID)와 생체인증 등 핀테크 기반의 다양한 사용자 인증수단의 확산에 따른 FIDO는 아이디와 비밀번호 입력보다 강력한 보안성을 제공방안의 서버구축 사례를 분석하였다.

이로서 본인인증과 인증정보가 다른 거래인증 방식인 FIDO2.0 기반의 생체인증을 활용한 사용자 본인인증 서비스는 금융거래에 필요한 통합 결제시스템의 활성방안이 확산되길 기대한다.

ACKNOWLEDGMENT

본 연구는 산업통상자원부의 디자인혁신역량강화사업(#10065273, 생체인증 기반의 생활밀착형 스마트 기기 선행디자인 및 표준 프로세스 개발) 결과의 일부입니다.

참 고 문 헌

[1] 금융위원회,"핀테크 혁신 활성화 방안," 2018. 3.
[2] 김동진, "바이오인증 최신 활용 및 보안 동향", 전자금융과 금융보안, 2016.07.
[3] 행정안전부 정보기반보호정책과,"공공웹사이트 인증수단 소개서," 2018. 9.
[4] http://www.ipnomics.kr/news/articleView.html?idxno=72276
[5] https://fido2.octatco.com:9492/webauthn/login-google.html
[6] http://www.comworld.co.kr/news/articleView.html?idxno=49477
[7] 김석현 외, "단말 장치, 서버 장치 및 블록체인을 이용한 FIDO 범용 인증 방법," 대한민국특허출원번호 1020180080792, 2018.07.11
[8] 유미영 이재형 강민구, "접근통제형 장비를 위한 생체인증 로그데이터의 블록체인 공유 기반의 액세스

보안관리 시스템," 대한민국특허등록번호 101868589, 2018.06.11
[9] 유미영 이재형 강민구, "생체인증형 리모콘을 이용한 블록체인 기반의 홈쇼핑 정보처리 시스템," 대한민국특허등록번호 101925147, 2018.11.28

◐저 자 소 개 ◑

유 미 영
2007년 홍익대학교 국제경영학과
2007년~2010년 삼에스코리아 해외영업 주임
2013년~2015년 달스코리아 해외영업 팀장
2016년~현재 옥타코주식회사 대표이사

이 재 형
2004년 충남대 국제경영학과(학사)
2005년~2017년 달스코리아 대표
2017년~현재 옥타코 기술전략책임

강 민 구
1986년 연세대학교 전자공학과(공학사)
1989년 연세대학교 전자공학과(공학석사)
1994년 연세대학교 전자공학과(공학박사)
1985년~1987년 삼성전자 연구원
2000년~현재 한신대학교 IT콘텐츠학과 교수