FNSVALUE

EASY · FAST · SAFE

BSA

“가장 쉽고· 빠르고· 안전한
블록체인 기술 기반 사이버 보안 인증 솔루션”

Jun 2023 | (주)에프엔에스밸류

DISCLAIMER

- 본 자료는 투자 대상사업에 대한 예비투자자의 이해를 돕기 위하여 작성된 자료로서 이와 관련하여 향후 추가 보완 및 수정사항이 발생 할 수 있습니다.

- 본 자료는 독립적인 검증절차를 거치지 아니하였으며, 잠재적 투자자에게 필요한 모든 자료를 포함하고 있지는 아니하므로 잠재적 투자자는 본 프로젝트에 대하여 자체적인 조사와 분석을 하여야 합니다. 또한, 본 자료에서 제공된 정보는 어떠한 계약의 근거로도 사용될 수 없습니다.

- 본 자료는 잠재적 투자자의 투자의사결정을 지원하기 위하여 작성된 것으로 귀사의 의사결정 과정에서 어떠한 책임도 부담하지 아니합니다. 이에 따라 회사 및 회사의 관계자는 본 자료와 관련한 어떠한 보증이나 보장도 제공하지 아니하며, 모든 의사결정은 의사결정자의 판단과 책임하에 이루어져야 합니다.

- 본 자료는 잠재적 투자자의 투자의사결정 지원 목적 이외의 다른 용도로 사용될 수 없습니다. 본 자료가 잠재적 투자자 이외의 자에게 공유 또는 배부될 경우에는 회사 및 회사 관계자로부터 서면동의를 얻어야 하며, 이에 반하여 본 자료가 사전 서면동의 없이 다른 목적으로 사용되는 경우 회사나 제3자에게 발생한손실에 대하여 책임을 질 수 있습니다.

Contents

INVESTOR RELATIONS 2023

Executive Summary

기술

① 쉽고 빠르고 편리한 사용자 가입과 사용

② 완벽한 보안성

③ 기술진입장벽 : · 미국, 영국, 중국, 일본, 말레이시아, 대만, 싱가폴 특허 등록/ 국내 특허 4건 등록 - 총 8개 국가 13건 등록 완료

· OIC-CERT 글로벌 사이버보안 대상 수상(국외), 조달청 우수제품지정 인증, 대한민국 우수기업 우수기술대상 수상(국내)

· MAIN-BIZ 인증 & INNO-BIZ 인증, ISO 27001:2013 보안인증 솔루션에 대한 정보보호경영인증,

· CCRA(Common Criteria Recognition Arrangement) : 정보보호시스템 국제 공통평가기준

· 한국정보보안기술원 기술시험성적 인증 및 GS 1등급 인증

경쟁력

① 높은 신규 진입 장벽 : 블록체인 검증기반 탈 중앙서버, Passwordless, 모바일 정보 기반 보안인증 솔루션으로서의 완벽한 보안성

② Legacy 경쟁 : 기존 생체정보 중앙 서버 저장, 주요 개인정보 중앙 서버 저장 등 FIDO/FIDO2 방식과 전혀 다른 솔루션

③ 요구 정보 최소화로 고객 정보 탈취에 대한 영향 없음 : 휴대폰 번호/이메일 주소/ID

확장성

적용 가능 대상 : ① 사용자 계정 인증이 필요한 서비스(쇼핑/게임/신원정보 확인 등)

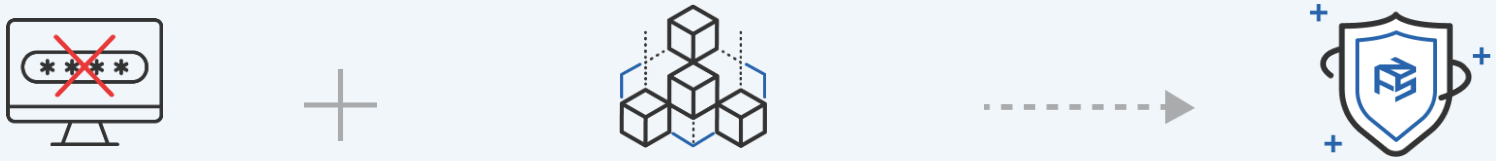
② 기업 사내 직원용 인증

③ Defi custody : Wallet 인증, 탈 중앙 거래소 보관서비스

④ IoT 보안 : 월패드 해킹 방지, 모든 사물기기와 사용자간 인증 보안

⑤ 커넥티드 카 : 사용자 접근 권한 인증 / 차량 애플리케이션

Executive Summary



로그인 실패 문제 해결

로그인 실패로 인해 보안 알림을 처리해야 하는 시간이 줄어들 뿐만 아니라 더 이상 새로운 비밀번호 요청에 대응할 필요가 없습니다.

사용자의 앱 도입 및 충성도 제고

로그인 프로세스를 긍정적인 경험으로 만들어 줌으로써 사용자가 앱을 지속적으로 사용하도록 유도하며 **사용 고객의 충성도를 높여 재방문 사용자를 늘리는** 데도 효과적입니다.

간편한 로그인으로 구매율 증가

상품 판매 시 **로그인 프로세스의 간소화**가 제공하는 편의성으로 구매를 포기하는 고객이 줄어들어 **웹과 모바일 환경 모두에서 구매율이 증가**할 수 있습니다.

계정·데이터 등 기업 공격 위험 감소

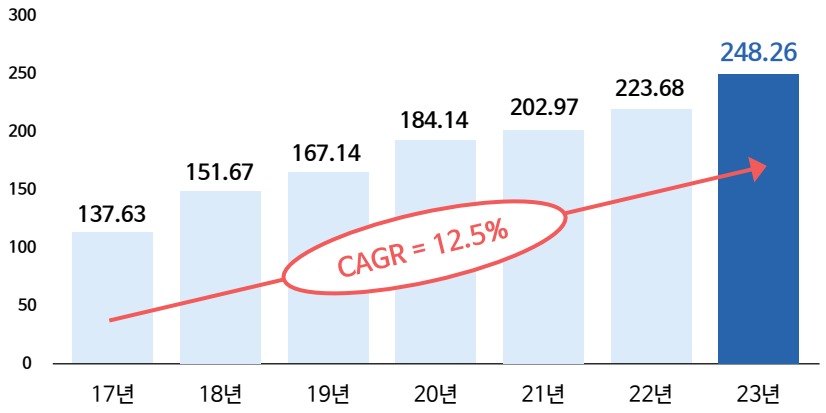
취약하거나 재사용되는 Password 중심의 자격 증명은 공격에 항상 노출됨으로써 기업의 허점으로 작용합니다. **비밀번호 없는 로그인**이 가능해지면 자격 증명 유출로 인한 **계정 탈취 및 데이터 침해 위험을 줄일 수** 있습니다.

Executive Summary

글로벌 사이버 보안 시장 규모

(단위: 십억$)

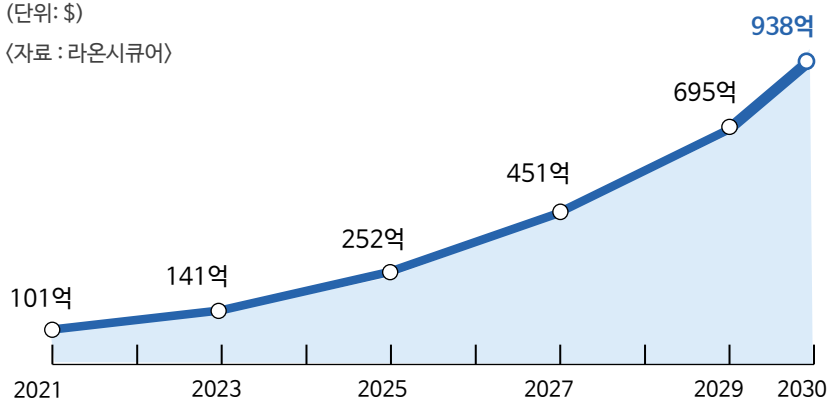
〈자료 : Statista (2020)〉



블록체인 기반 신원인증 글로벌 시장 규모 전망치

(단위: $)

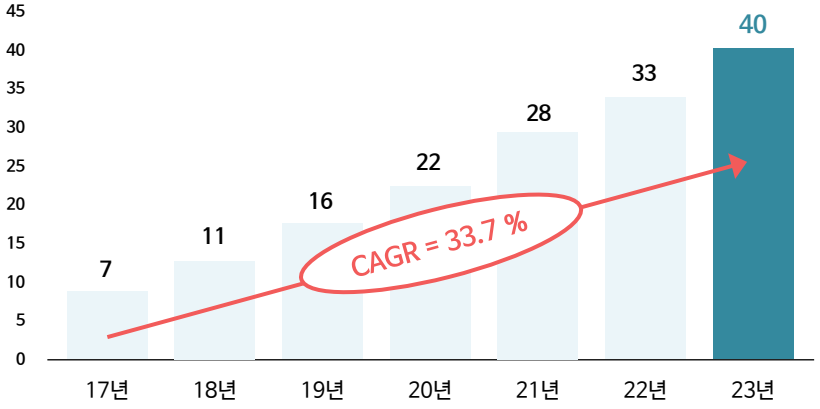
〈자료 : 라온시큐어〉



말레이시아 사이버 보안 시장 규모

(단위: 백만$)

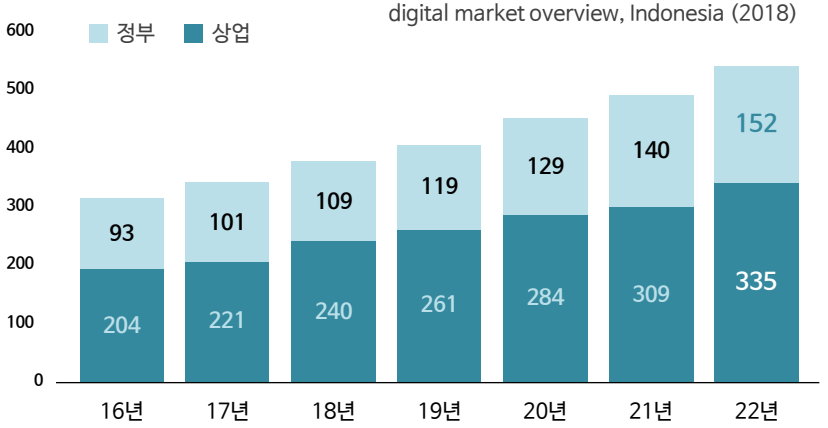
〈자료 : Statista (2019)〉



인도네시아 사이버 보안 시장 규모

(단위: 백만$)

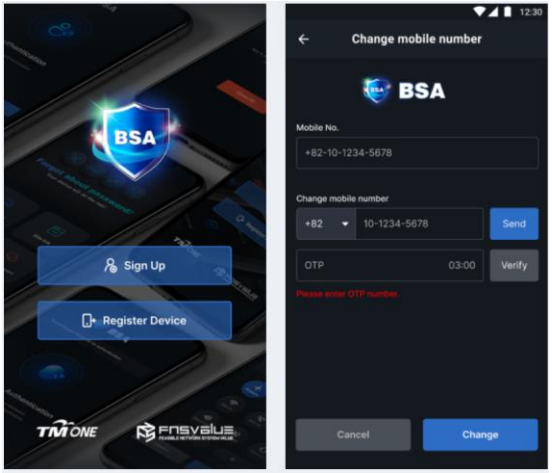
자료: Frost&sulivan,
digital market overview, Indonesia (2018)



Business Case

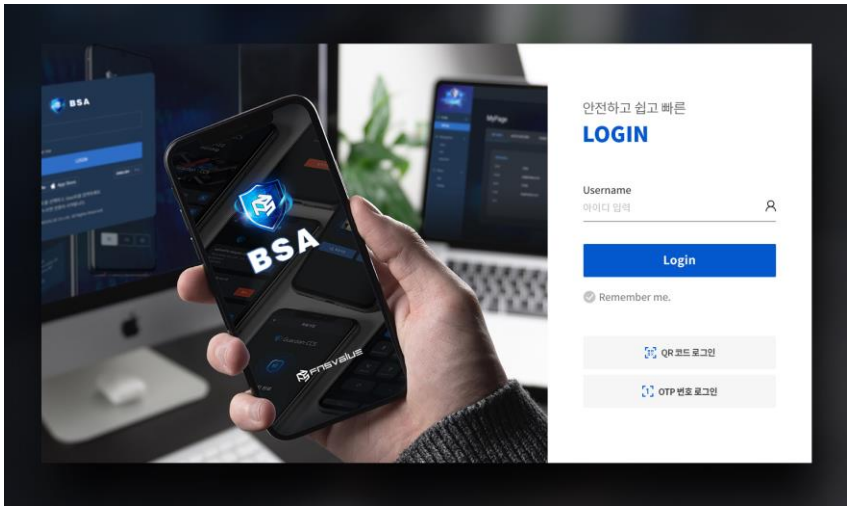
2020년 **말레이시아의 최대 국영통신기업 Telekom Malaysia(이하 TM)와 라이선스 계약 체결 후 현재까지 솔루션 공급** 중이며, 같은 해 **말레이시아 국영 에너지기업 PETRONAS** 납품했고 2021년 **인도네시아 통신장비업체인 PT VADS** 계약을 성사시켰습니다. 국내에서는 2021년 기업용 올인원 협업툴 **티그리스와 서비스 제휴**를 기반으로 BSA의 솔루션의 성능 및 보안성을 인증 받아 강력한 보안 기술 및 서비스를 제공하고 있으며, 2022년 11월 **의료용품 및 분자진단 소프트웨어 기업인 씨젠의 관계기관인 씨젠의료재단에 BSA기반 사내 통합계정 솔루션 서비스** 제공 계약을 체결했습니다.

국외 적용 사례



- 텔레콤 말레이시아 전사적 관리시스템 공급(Secure Authentication, BSA)
- 인도네시아 PT VADS의 보안인증 솔루션 공급
- 말레이시아 PETONA 보안인증 솔루션 공급

국내 적용 사례



인사관리 | 이메일 | 전자결재 | 캘린더 | 메신저 | 저장소

스타트업부터 공공기관까지 사용기업 300+ 누적 사용자 12만+

Cyber security attack

증권사 39만명 개인정보 털렸다… 흥신소·통신사 직원 일당 검거

서울경제 | 2022.04.14 18:49

증권정보 사이트를 해킹해 수십 만 명의 개인정보를 빼돌려 팔아 넘긴 흥신소 일당이 경찰에 붙잡혔다.

서울경찰청 사이버수사과는 흥신소 업자 9명을 개인정보 보호법, 정보통신망법, 성폭력처벌법(카메라 등 이용 촬영) 위반 등 혐의로 검거했다고 19일 밝혔다. 이들 중 4명은 불구속 상태로, 5명은 구속 상태로 검찰에 넘겨졌다.

이들은 2019년 12월부터 지난해 9월까지 증권정보 포털 등 기업 사이트를 해킹해 빼돌린 회원정보와 통신사·보험사·택배사 직원에게 매수한 고객 정보를 팔아 넘긴 혐의를 받는다. 이들은 불법 취득한 개인정보 1207건을 의뢰인들에게 팔아 넘겨 3800만원 상당의 부당이득을 취한 것으로 전해졌다.

S사 금융 통합 앱 출시 4일 만에 개인정보 유출

글로벌E | 2022.04.22 16:36

S사들이 선보인 통합 앱 'OOO'가 출시된 지 나흘 만에 개인정보 유출 사고가 발생했다. OOO 는 생명·화재·카드·증권 등 S사 금융 네트웍스가 통합 서비스하는 앱이다.

금융권에 따르면 ' OOO '는 18일 오후부터 19일 오전 사이 S사 증권 고객 344명의 투자 정보를 타인에게 노출했다. S사 증권이 제공하는 개인 고객정보 화면에 타인의 정보가 그대로 보였다.

S사 증권 고객의 보유 종목과 수익률, 입출금 거래 내역, 현재 잔고 등이 타인에게 모두 노출됐다.이번 오류는 OOO 를 통해 4개 회사의 개인 자산 정보를 볼 수 있는 화면에서 S사 증권의 페이지로 넘어가는 과정에서 발생했다. 다행히 매매는 할 수 없었다.

"재택근무 일상화되면서 해킹 피해액도 사상 최대"

한국일보 | 2021.08.02 13:39

신종 코로나바이러스 감염증(코로나19) 확산과 함께 재택근무가 일상화되면서 사이버 보안 위협도 급증하고 있는 것으로 나타났다. 특히 기업들의 데이터 유출 피해 금액은 사상 최고치에 달한 것으로 조사되면서 주의가 요구된다.

2일 IBM 시큐리티가 지난해 5월부터 올 3월까지 전 세계 500개 이상의 기업 및 조직에서 발생한 데이터 유출사고를 분석한 결과, 조사 대상 기업들은 데이터 유출로 인해 사고당 평균 424만 달러(약 48억8,200만 원)의 손실을 입었다. 이는 전년 대비 10% 증가한 규모로, 지난 17년 동안 손실 규모를 집계한 이후 최고치다. 데이터 유출 사고에 따른 국내 기업의 평균 손실 규모는 41억1,000만 원으로 조사됐다.

Cyber security necessity

코로나19 팬데믹 이후 우리의 일상이 크게 달라지며, 대면활동이 급격히 감소, 비대면 활동이 모든 사회, 경제 활동의 핵심으로 자리 잡았습니다.
특히 비대면 서비스에 다양한 디지털 기술의 결합되면서 4차 산업혁명으로 불리는 패러다임 변화가 가속화되고 있습니다.

- 디지털금융 거래로 계정 탈취, 조작 등 사이버 범죄 증가
- 근무 형태 유연화에 따른(재택근무) 사이버 보안 문제 가시화
- 가상자산 등 디지털자산에 대한 우려 증대
- 국내외 기업 및 기관의 대규모 개인정보 유출 피해 증가
- IoT 계정 탈취 등 다양한 형태로 끊임없이 진화하는 랜섬웨어 공격

2022년 발생 사이버 위협 동향 – 비대면 서비스의 확산에 따라 기업 및 개인정보, 자산 보호를 위한 사이버 보안 문제가 사회적 이슈로 제기됨

국가 핵심 인프라를 위협하는 대규모 랜섬웨어 공격 증가

디지털 워크 플레이스 확대에 따른 위협 시도

코로나19 팬데믹 등 사회적 분위기를 편승한 사이버 공격 기승

국내외 기업 및 기관의 개인정보 유출로 인한 피해 급증

We are & Our Authenication

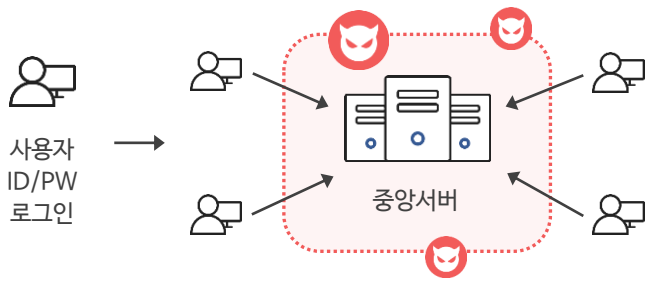
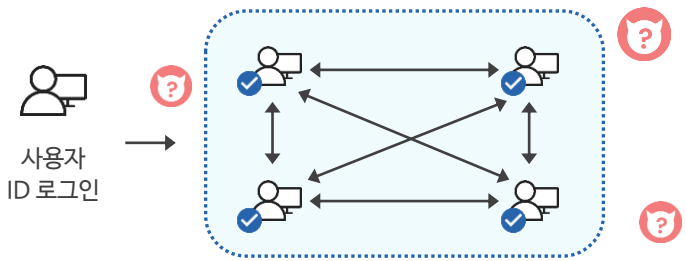
- FNSValue는 10년 이상의 정부 부처 대상의 SI 비즈니스 를 기반으로 소프트웨어 솔루션 회사로 새롭게 도약하고 있습니다.
- 사용자의 스마트 폰을 이용하여 세계 최초 유일무이의 암호 없는(Passwordless) 블록체인 검증 기반의 로그인 인증 기술을 구현합니다.

인증방식 종류와 발전단계

지식기반 인증	계정과 비밀번호/ 질문과 답변/ 코드북/ 패턴/ 이미지 등
	· 보통 비밀번호는 사용자 개인정보를 이용해서 비밀번호를 생성하기 때문에 사용자가 비밀번호를 기억하지 못할 수 있어 공격자가 이러한 맹점을 이용하면 쉽게 추측이 가능
소유기반 인증	신분증의 날짜 인증/ 신용카드의 CVC 번호 인증/보안카드/OTP /USB 공인인증서 등
	· 부정한 사용자가 복제 등의 방법을 통해서 부정하게 소유물을 구할 수 있는 위험이 있음 · 손실이나 도난 시에 대체해야 하는 관리 기능 비용이 추가로 요구
생체기반 인증	지문/ 음성/ 홍채/ 안면/ 심박수 등 개인의 신체 특징을 활용
	· 사용자의 생체정보를 저장 및 보관해야 하는 관리상의 어려움이 존재. 특히 몸의 특징은 한정돼 있기 때문에 유출되면 이를 대체해 인증할 수단이 존재하지 않음.
블록체인 기반 인증	위변조가 불가능하며 사용자의 디바이스나 중앙 서버에 저장하는 **보안키가 존재하지 않아 계정탈취 및 침해의 위험이 현저하게 감소.**

Blockchain Login

일반적인 ID & PW 방식은 사용자 로그인 Session 및 Cookie에 정보를 담는 방식으로 사용자의 정보가 노출되는 단점이 존재합니다. 블록체인 검증 기반 기술은 그 해결책으로 사용자의 로그인을 허가하는 방식으로 로그인이 필요한 시스템 외에도 보안 및 인증이 필요한 모든 시스템에 적용할 수 있습니다.

일반적인 ID&PW 로그인 방식	비교 방식	블록체인 검증 기반 로그인 방식
	기본구조	
Session 및 Cookie에 사용자 정보를 담아 서버 장애로 인한 **데이터 손실 우려**와 해당 부분의 정보를 탈취하기 쉽고 **해킹 공격으로부터 취약함**	안전성	블록체인 검증 기반 불특정 다수의 사용자가 로그인 허가하며, OTSK, MDV, MIRC 다수의 보안 및 암호화 기술을 사용함. **로그인시 발생되는 정보는 별도 저장 및 관리하지 않으므로 내외부 공격으로부터 안전하게 보호**
서비스마다 **복잡한 암호**를 설정해야 하며, 설정된 암호를 **주기적으로 변경해야** 되는 **암호 관리의 어려움 존재**	편의성	**패스워드 없이(Passwordless) ID, QR, OTP로 간편 인증**
저장되는 정보의 양이 많아 **서버 유지관리 비용 증가**	유지관리	보호할 정보 감소로 시스템 유지에 대한 불필요한 **관리 노력 및 비용 감소**

Password 사용의 심각한 문제점

1. 웹 사이트나 서비스마다 서로 다른 암호를 설정하고 이를 기억하는 것이 쉽지 않습니다.
2. 하나의 암호를 여러 사이트나 서비스에서 중복 사용함으로써 공격 위험성이 높습니다.
3. 어렵고 복잡한 암호는 기억하기 쉽지 않아 너무 쉽고 간단한 암호를 반복적으로 사용함으로써 보안성에서 취약합니다.

암호 사용 로그인 문제로 발생하는 침해 사고

1. 동일한 비밀번호, 너무 단순한 비밀번호 등 사용자들의 습관이나 관행이 계정 탈취 및 도용, 개인 정보 및 데이터 유출 등 다양한 보안 사고의 주요 요인이 되고 있음

2. 미국 통신기업 Verizon의 데이터 침해 조사 보고서에 따르면, 침해 사고의 80%가 탈취되거나 무차별 대입 공격을 받은 자격 증명과 연관된 "해킹"으로 자격 증명 탈취는 가장 빈번한 해킹 전술임.
자격 증명 스터핑이나 피싱과 같은 비밀번호 기반 공격이 증가하는 추세임.

3. 2022년 9월 IBM (시큐리티) 발표 '2022 데이터 유출비용 연구 보고서' 자료에 따르면, 데이터 유출사고 건당 피해 금액이 가장 큰 산업은 금융, 서비스, IT순이며 데이터 유출사고의 최다 공격방법은 '사용자 인증 정보 도용'이 약 20%로 가장 많은 것으로 드러남 .

4. 다단계 인증이나 암호 관리자 등 대안을 적용하는 기업들이 늘어나고 있어 Passwordless 로그인은 이러한 암호 기반의 사용자 인증의 문제점을 해결할 수 있는 대안으로 주목받고 있음.

“내년부터 비번없이 로그인“.. 애플·구글 ·MS ‘패스워드리스’ 합심

머니투데이 | 홍효진 기자 | 2022.05.09 08:21

애플과 구글, 마이크로소프트(MS)가 합심해 암호 없는 로그인 지원을 확대한다.

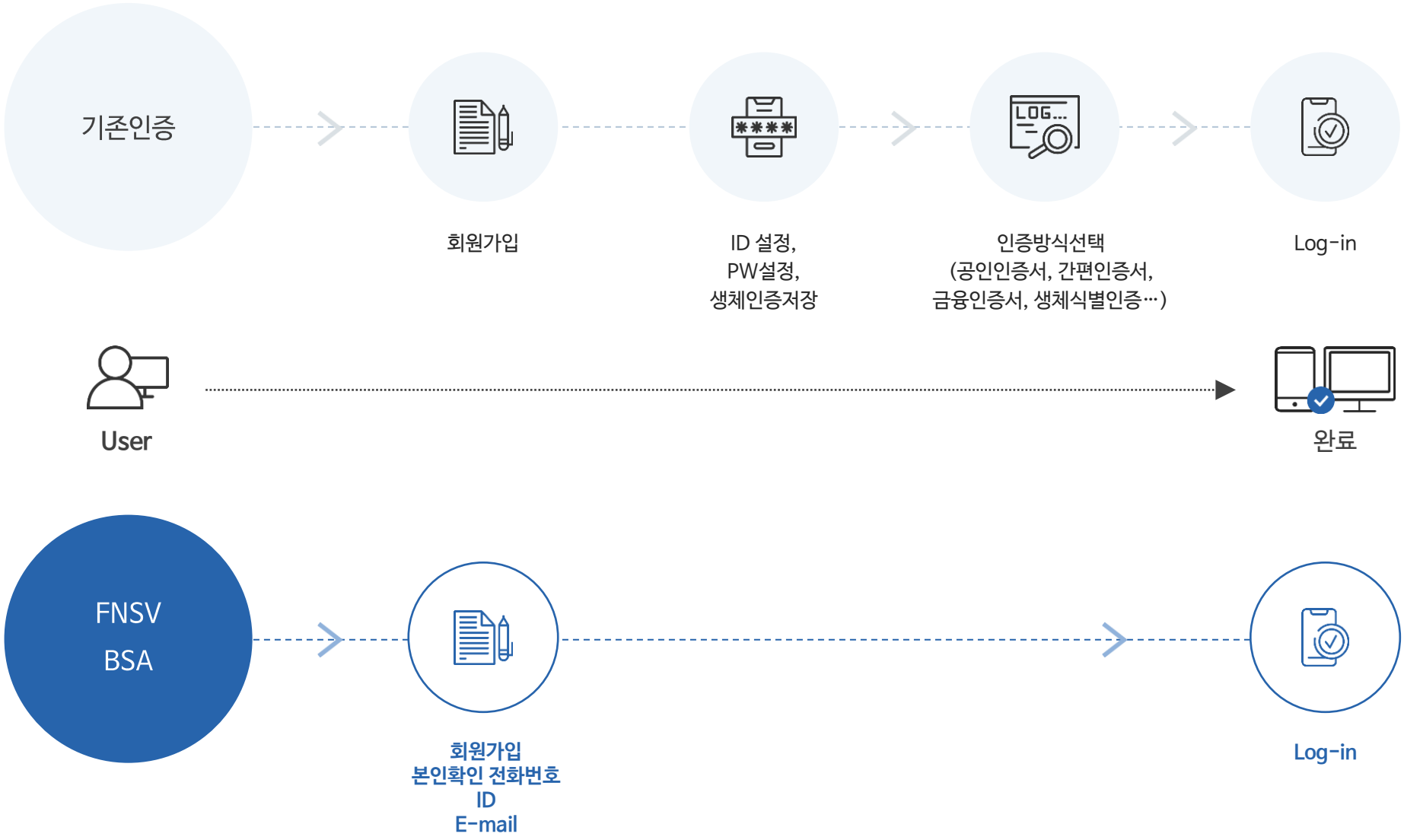
5일(현지시간) 엔가젯·테크크런치 등 IT매체에 따르면 해당 빅테크 3사는 이날 "비밀번호 없는 로그인 표준을 위해 'FIDO(Fast Identity Online) 얼라이언스' 기술 지원을 확대하겠다"고 밝혔다.

FIDO는 지문, 안면인식, 개인식별번호(PIN) 등의 인증방식을 웹사이트나 애플리케이션(앱)에서도 로그인할 수 있도록 한 기술이다. 현재 FIDO 얼라이언스와 월드와이드웹(W3C) 컨소시엄에서 표준화 작업 중이다. 기존 비밀번호 인증은 여러 암호를 관리해야 해 번거로울 뿐만 아니라 같은 암호 재사용으로 보안 문제가 발생할 수 있다.

3사는 이미 FIDO 얼라이언스 표준을 지원해왔지만 사용자가 기기별로 웹사이트나 앱에 각각 로그인해야 했다. 이번 지원 확대로 기기와 웹브라우저 제한 없이 간편한 인증방식이 적용돼 사용자 편의성이 높아질 것으로 보인다. 계정별 등록 없이 여러 기기에서 FIDO 로그인 패스키에 자동 접근이 가능하기 때문이다. 운영체제(OS)나 웹브라우저 관계 없이 모바일 기기 FIDO 인증을 통해 주변 기기 앱·웹사이트 등에 로그인할 수 있다. 해당 신규 기능은 내년쯤 3사 플랫폼에 도입될 전망이다.

커트 나이트 애플 플랫폼 제품 마케팅 수석 이사는 "타 기업들과 협력해 향상된 보안 환경을 제공하고 암호 취약성을 제거하는 안전한 로그인 방식 마련은 사용자 개인 정보 보호를 위한 노력의 일환"이라고 말했다.

BSA User Process

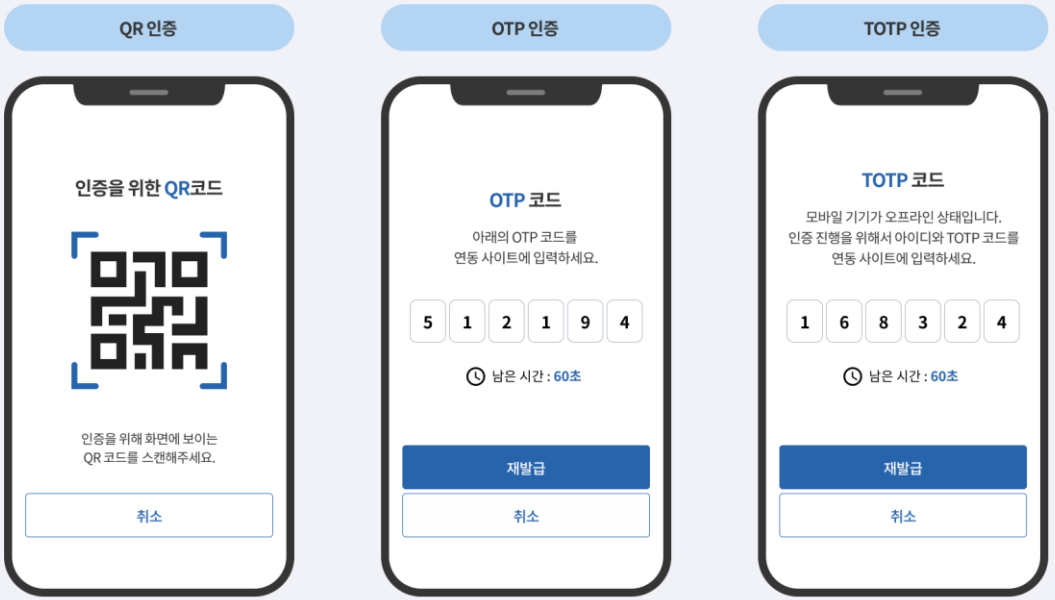


Authentication Process

BSA의 인증 프로세스는 **패스워드 입력 없이(Passwordless) 클릭 한번으로 인증절차를 완료합니다.**

비밀번호 및 Legacy MFA

- 비밀번호에 의존해 비밀보안 위협요소 해소
- 신용정보 재사용 및 2FA 피싱 요소 해소

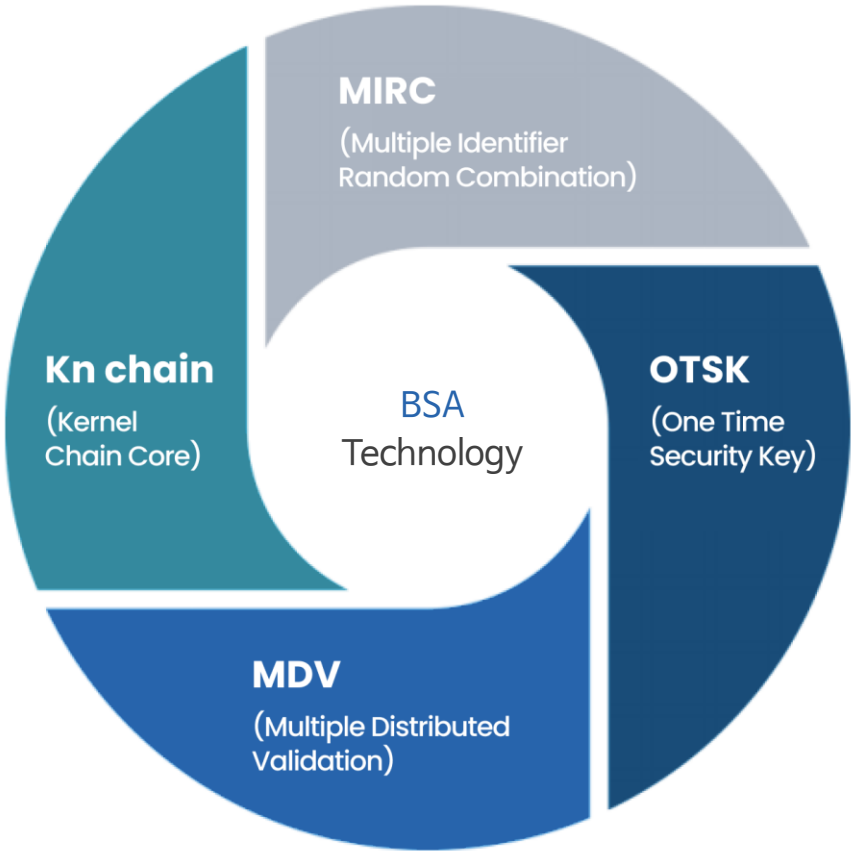


정확한 Passwordless MFA

- 초고속의 사용자 편의성 경험 제공
- 비밀번호를 공공키 암호체계로 대체
- 사용자와 데스크탑 MFA의 간극 해결

Patented Technology

BSA는 국내 뿐만 아니라, 미국, 일본, 중국, 싱가폴, 말레이시아 등의 해외에서 **특허 받은 MIRC(다중 식별자 랜덤 조합), OTSK, MDV, Kernel Chain의 주요 4가지 기술로 안정적인 기술 서비스를 제공**합니다.



BSA 기술의 특장점

Passwordless로 간편하게 인증

- 패스워드 입력이 필요하지 않은 자체검증 인증프로세스의 편리함

+

해킹으로부터 안전하게 보호

- 사용자 인증은 2초 이내 처리되므로 해킹의 물리적 시간 존재하지 않음
- 탈중앙화, 블록체인 기반 기술로 모바일 기기 내 탈취 가능한 정보를 보유하고 있지 않음

+

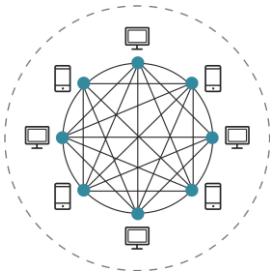
자체 블록체인 검증엔진(Kn chain) 보유

- 사용자 애플리케이션 부분은 Public Blockchain, 주요 인증처리 Core 영역은 Private Blockchain 형태의 Hybrid Blockchain 방식 기술 적용
- Hybrid Blockchain 방식 기술 적용으로 보다 빠르고 안정적이며, 높은 보안성을 제공

Hybrid Blockchain - Kernel Chain

BSA는 자체 개발한 블록체인 기술인 'Kernel Chain'을 기반으로 고유의 보안인증 알고리즘을 사용하여 개발한
커널 체인은 인증의 3가지 핵심 목표인 신뢰, 성능 및 보안성을 동시에 달성하기 위한 하이브리드 블록체인 네트워크 사상으로 구현합니다.

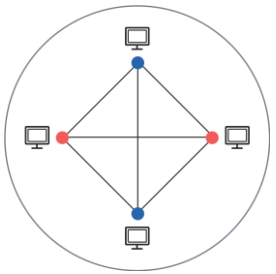
Public Blockchain



- 일반 대중의 자유롭게 참여할 수 있는 형태의 네트워크 구성
- 개발형 블록체인, 공공 블록체인이라는 명칭을 사용
- 네트워크에 참여하는 개별 컴퓨터, 휴대폰 등의 디바이스를 노드(Node)라 칭함
- 사용자 영역에서는 모든 대중의 자유롭게 참여하고, 개방기술을 제공.

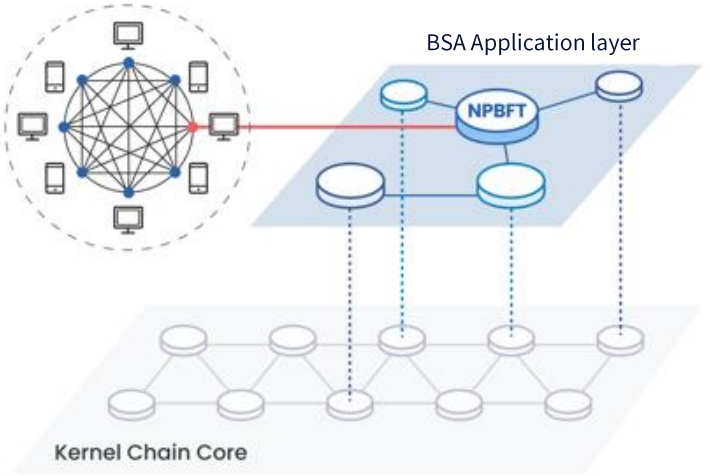
+

Private Blockchain



- 소수의 허락된 사람만이 참여할 수 있는 폐쇄적인 형태의 네트워크 구성
- 은행, 공공기관에서 주로 사용
- 허가 받은 사용자만 노드로 참여할 수 있는 형태로 퍼블릭 블록체인에 비해 상대적으로 적은 노드로 운영
- Public Blockchain 주요 인증처리 Core영역 Private Blockchain 구성하여 인증처리 영역에 대한 보안성을 강화

Hybrid Blockchain



- 퍼블릭과 프라이빗의 장점을 최대한 구성한 네트워크
- 보안성, 불변성, 투명성, 탈중앙화 등의 주요 기능을 제공
- 사용자의 익명성은 제한되나 공개 익명성은 유지되어 네트워크 외부의 누구도 블록체인 사용자를 알 수 없음

Applicable Services

BSA는 사용자 인증, 개인키, 보안키 등으로 사용자 정보에 대한 인증 및 검증 서비스가 필요한 모든 산업군의 서비스에 적용 가능하며, 기존의 서비스 대비 고객정보 보호 및 기업의 지적재산 침탈을 방지하는 강력한 보안 기술 및 서비스를 제공합니다.

사용자 계정 인증이 필요한 서비스

- 기업, 금융, 유통 등의 계정 서비스 인증
- 웹/모바일 애플리케이션 사용자 인증
- 고객, 사용자 신원확인 서비스

DeFi / 가상자산의 보관 / Wallet

- 가상자산의 보관에 대한 인증
- Wallet Server(토큰 교환 및 암호화폐 거래소)
- 탈중앙거래소(DEX, DEXes) 서비스

개인정보 도용 위험 없는 앱카드

- 앱카드를 설치/등록하는 안전한 인증방식
- 개인정보 탈취 방지 및 신원정보 유효성 검증

커넥티드 카 Connected Car

- 사용자 접근, 권한에 대한 인증
- 펌웨어 접근에 대한 인증 및 검증
- 차량 애플리케이션, 기기 접근 인증

BSA's Status quo

국제전기통신협회(ITU-T)의 보안 인증 세계 표준화 추진

2년 내 완료 목표. 현재 한국, 말레이시아, 스위스 3국이 BSA를 글로벌 보안인증 표준으로 선정하기 위한 프로세스 진행 중입니다.

금융규제 샌드박스 선정 추진

금융위 산하 한국핀테크지원센터에 요청 및 추진 중인 전자금융거래법(제초 제10호/ 제6조 제2항) 및 전자금융감독규정 특례완료로 금융거래시 당사의 인증 솔루션 도입을 위한 기반 마련 중입니다.

이슬람문화권 국가 진출을 위한 교두보 마련

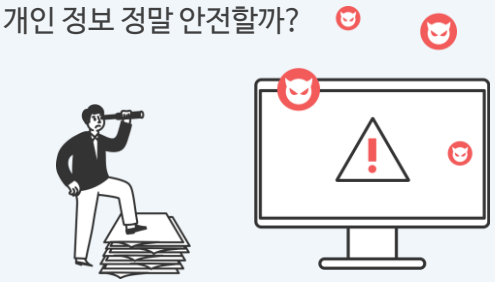
BSA는 OIC-CERT Global Cyber security Award 2021을 2021. 11월에 수상, OIC회원국 내 기술력을 인정받음. 이런 장점을 활용해 이슬람문화 권역 내 57개 국 시장 진출을 추진 중입니다.
OIC:Organization of Islamic Cooperation

미국 및 중국시장 진출 추진

동남아 이외 기술 선진국(미국, 중국 등) 진출을 통한 사업 권역 확장을 위해 현재 미국 기업들과 initial meeting 진행 중입니다.

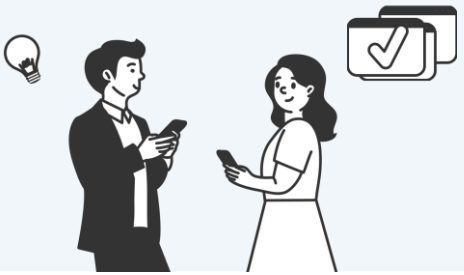
Groupware Services

불편한 그룹웨어는 이제 그만, 클릭한번으로 편리하게 사용하는 BSA를 통해 간편하게 로그인하여 번거로운 비밀번호 관리 및 불필요한 시간을 줄이고 생산성은 증가합니다.



불필요한 비밀번호 없이 간편한 출퇴근 관리가 가능합니다.

모든 업무가 스마트폰 하나로 해결됩니다



BSA 보안시스템으로 안심할 수 있습니다.

Financial Services – DeFi

FNS Value의 블록체인기술을 활용한 탈중앙화 금융 서비스(DeFi), NFT 기술 서비스 제공하며, 가상화폐를 보관하는 전자지갑의 보안 가상화폐 저장금고에 대한 최적의 보안 서비스를 제공하여 향상된 보안 서비스를 사용자에게 제공합니다.

탈중앙화된 금융 서비스 제공

디파이를 통해 각종 중앙기관을 거치지 않고 블록체인 기술을 이용하여 APP을 통해 다양한 금융 서비스가 이용 가능합니다.

보다 안전하고 투명한 금융거래 제공

중개인이 없이 많은 기능을 자동화해 비용을 낮추고, 보안 위험성을 줄이면서 개인정보 보호 수준을 높이고 누구나 금융 서비스에 참여할 수 있습니다.

금융서비스 이용 시간 단축

언제 어디서나 어떤 환경에서도 모든 금융서비스를 제약없이 이용 가능하여 시간이 단축되고 효율성이 높아집니다.

Mobility Services

BSA Mobility 보안 적용 가능 기술

Passwordless

Passwordless 인증을 통한
ID & 비밀번호 탈취 방지

Hybrid Blockchain

자체 개발 Hybrid Blockchain
인증 방식으로 해킹 위협 완전 차단

Quantum cryptography

양자암호화 + BSA로
자율주행 Mega Data 암호화

2023~2025 Estimated Revenue Strategy

기술, 해외 시장 개척

에프엔에스밸류 해외 시장 개척은
꾸준히 진행 중입니다.

기술 중심 해외 시장 개척 전략 + TM 과의 전략적 사업 제휴 전략 + 동남아시아 인증, 보안 분야 시장 개척 (홍콩뱅크, 메이뱅크, Shopee)

(단위: USD)

구분	2023년	2024년	2025년
매출 목표액	6,000,000	30,000,000	60,000,000
목표 유저수	10,000,000	50,000,000	100,000,000

사업전략	TM 주요 사업군	세부사업	사업 추진 영역
TM과 거버넌스 구축과 각 사업별 커스터 마이징 기술제휴를 통한 말레이시아, 인도네시아 시장 공략 (주력 사업)	BFSI (금융 주요 산업) Banking, Financial Services, and Insurance	데이터분석, RPA, AI, 블록체인, 챗봇, 데이터분석	각 사업별 인증 역할 User 당 2$ 로열티 수익
	교육	스마트학습, 학교 및 학습관리, 통계, 연결, 보안	출석관리, 학습 ID, 보안 문서보안 등 솔루션 개발
	공공, 정부	ICT, 디지털의료, 교육, IOT, 보안, 데이터분석	말레이시아, 인도네시아 공공 사업 공동 프로젝트
	헬스케어, 의료	빅데이터분석, 인공지능, IOT, 보안, 블록체인	환자인증, 예약, 개인정보, 의료 기록 보호 등
	OIL & GAS	고속네트워크, 5G, IOT, 하이브리드 클라우드, 보안	해양석유, 가스라인 IOT 인증, 보안

(한국능률협회컨설팅(KAMC) 컨설팅 발췌자료)

Key personnel

전승주 대표이사

- LG CNS Architecture
- SCJP 자격보유
- OCP DBA 자격보유
- 한국외국어대학교 컴퓨터학 공학사
- ㈜에프엔에스밸류 대표이사
- FNS(M) SDN. BHD 대표이사
- 정보관리기술사 자격보유
- 삼육보건대학교 외래교수

류성춘 글로벌사업부 전무

- ㈜에프엔에스밸류
해외사업총괄 대표이사
- 미래에셋증권 부사장
- University of Michigan, USA - MBA
- 연세대학교 경제학과 경제학사

장헌주 대외협력부 상무

- Deloitte Korea 커뮤니케이션 전략실장
Deloitte AP WorldImpact Council member
- 중앙일보·한국경제 기자
- University of California, Los Angeles
- 부산대학교 신문방송학과 학사

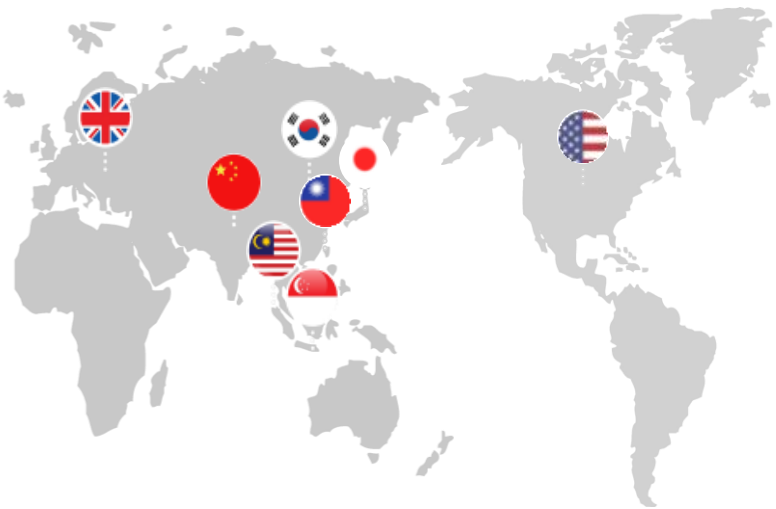
Thaib Mustafa 이사

- FNS(M) SDN. BHD. CEO
- IT분야 근무경력 32년 이상
- 글로벌 ACE인증 거버너스 위원회 위원
- 정보보안표준개발위원회(TC5) 회장
- 소프트웨어 아키텍트 국제협회 부회장

Radhilufti Madehi 마케팅 매니저

- FNS (M) SDN. BHD. 마케팅 시니어 매니저
- IT분야 근무경력 20년 이상
- 말레이시아 TM Berhad 사이버보안부분 총괄
- 프라이스워터하우스쿠퍼스(PwC)

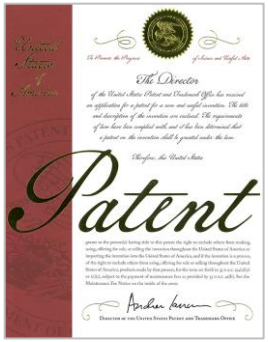
Patents and Certifications



대한민국 특허

대만 특허

말레이시아 특허



미국 특허

중국특허

일본 특허

싱가폴 특허

영국 특허

Patents and Certifications

품질관리 인증

저작권 등록증

우수기술대상

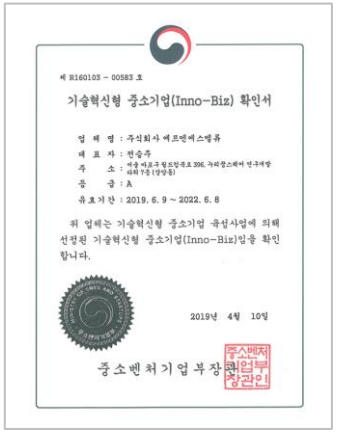
소프트웨어 품질 인증서

CCRA

KOIST 인증서

OIC-CER GLOBAL CYBERSECURITY AWORD

Main-Biz 인증서



Inno-Biz인증서

벤처기업확인서

BSA's Status quo

"OIC-CERT GLOBAL CYBERSECURITY AWARD 대상 수상"

- OIC-CERT GLOBAL CYBERSECURITY AWARD는 각 57개 국가에서 정부, 기업, 기관 등에서 혁신적인 사이버 보안 프로젝트를 인정 받기위해 지원함. 2021년 당사는 중국 화웨이와 함께 공동으로 대상 수상
- OIC와의 관계 build up을 필두로 아부다비투자진흥청과 UAE 내 VC 설립 논의 중
- 스위스 양자암호 기술기업 itkSwiss와 전략적 파트너십 체결

2021 OIC-CERT GLOBAL CYBERSECURITY AWARD

"스위스 양자암호 기술기업 itkSwiss와 전략적 파트너십 체결. 유럽 등 지역 시장 공동 개척"

스위스 제네바 현지 signing ceremony

BSA's Status quo

스위스 제네바
ITU(국제전기통신협회) ▼

"2023년 2월 스위스 제네바 국제회의서 솔루션 기술 세계 표준화 착수"

ITU 세계표준화 정보보호연구반 리더 미팅

ITU 세계표준화 사무국(TSB) 미팅

"ITU DFS 랩과 보안인증 샌드박스 추진 결정
FIDO에 이어 전세계 기업 중 두 번째"

Thank you.

서울특별시 마포구 월드컵북로 396,7층(상암동, 누리꿈스퀘어 연구개발타워)
TEL : 02-303-3885 | FAX : 02-304-3885 | www.fnsvalue.co.kr

FNSVALUE