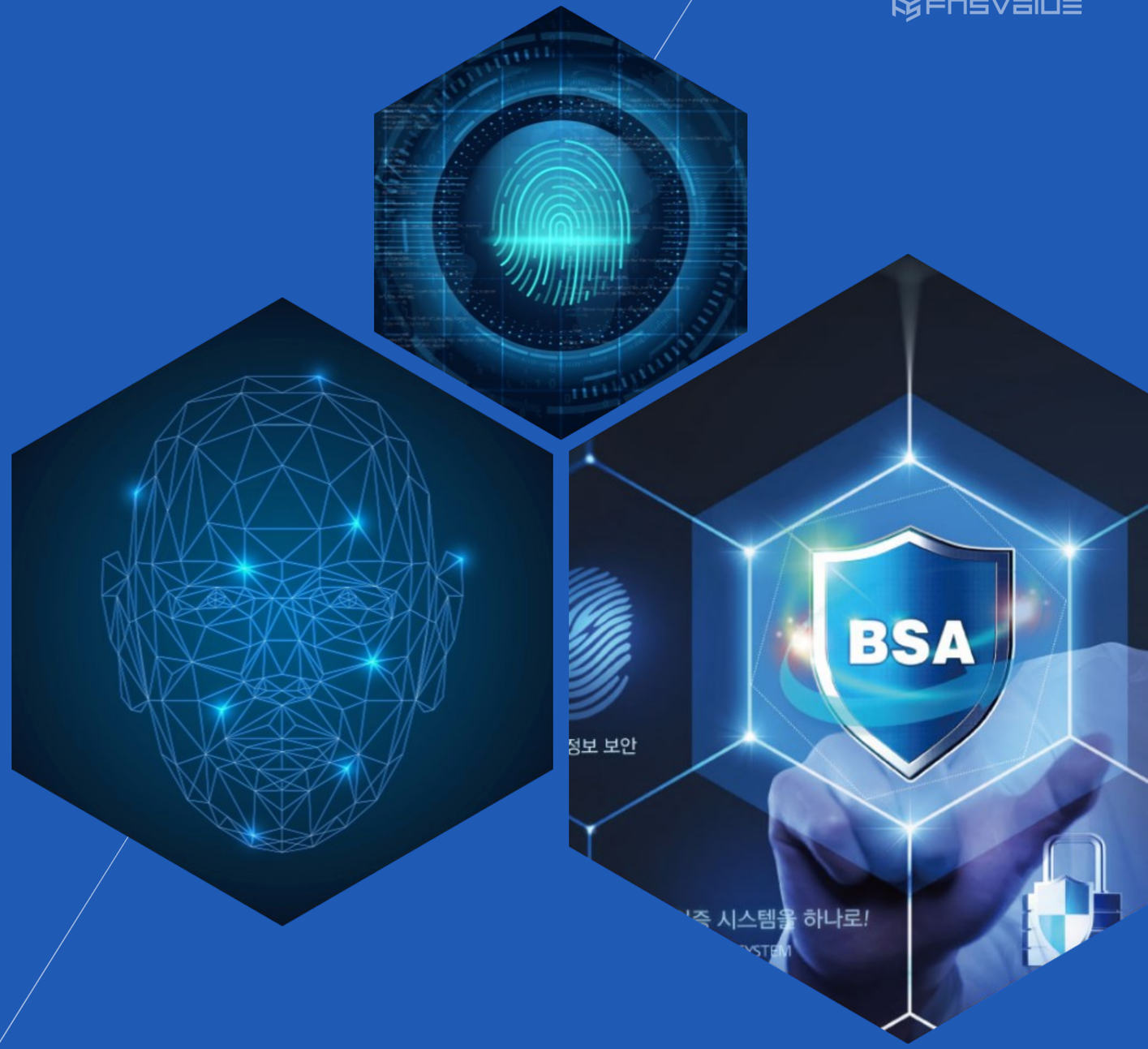
Blockchain
Secure
Authentication

패스워드리스 인증 체계의 새로운 패러다임

BSA



(주) 에프엔에스벨류

International
Telecommunication Union
X.afotak

SAFE • FAST • EASY

CONTENTS

01

인증 트렌드 변화

패스워드 사용의 불편함

복잡한 보안수준 요구에 대한 불만

Passwordless 인증 방식 선호

인증 트렌드 변화

사용자들이 가장 많이 불편해 하는 부분은 패스워드를 기억하기 어려움

패스워드 재설정

30%

패스워드 재설정

패스워드 재설정 절차가 복잡하고
재설정 중에는 일시적으로
서비스에 접속할 수 없어 불편함

보안 위협

20%

보안 위협

피싱 등 해킹에 의해 패스워드가 유출되면
개인정보가 도용될 위험

기억하기 어려움

40%

기억하기 어려움

대문자, 특수문자 등을 포함한
복잡한 패스워드 규칙을 요구해
기억하기 어려움

관리 어려움

8%

관리 어려움

패스워드를 기록하거나
기억하는 방법은 비효율적이며,
잃어버릴 위험 존재

인증 과정 불편

2%

인증 과정 불편

보안을 위한 자동 로그아웃,
이중 인증(2FA) 등이 불편함 초래

※ 출처 : Secureframe Blog - 80+ Password Statistics to Inspire Better Security Practices [2023]

복잡한 보안수준 요구에 대한 불만

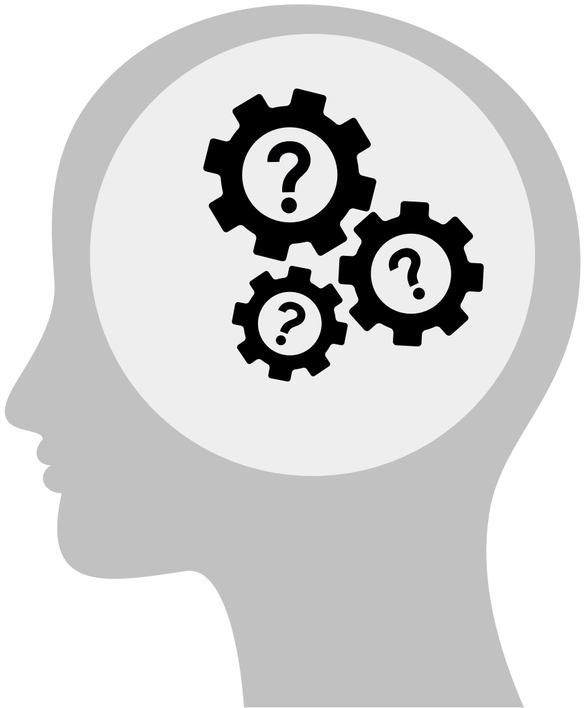
인증 트렌드 변화

다양한 인증 수단이 등장하지만 근본적 문제 해결이 부족한 변화 시도는 보안수준 제고보다는 불편만 야기

OTP 보안카드를 사용하세요.

핀 번호를 등록하셔야 합니다.

다중 인증은 필수입니다.



특수 문자를 써야……

3개월마다 바꿔야……

영대소문자를 꼭 섞어야……

Passwordless 인증 방식 선호

인증 트렌드 변화

True Passwordless 구현으로 사용자 및 관리자 측면의 모든 스트레스 해소

01. PW 재등록 불편함 감소

02. 유출/도용 위험 제거

03. PW 분실 리스크 감소

04. PW 기억 불필요

05. PW 주기적 변경 불필요

06. PW 정책관리 불필요

자리 수 제안 / 만료기한 설정 / 특수문자 입력 / 영대문자 입력 / 입력제한 (생년월일, 전화번호) 등

02

솔루션 소개

초 간편 인증 방식

BSA의 소개

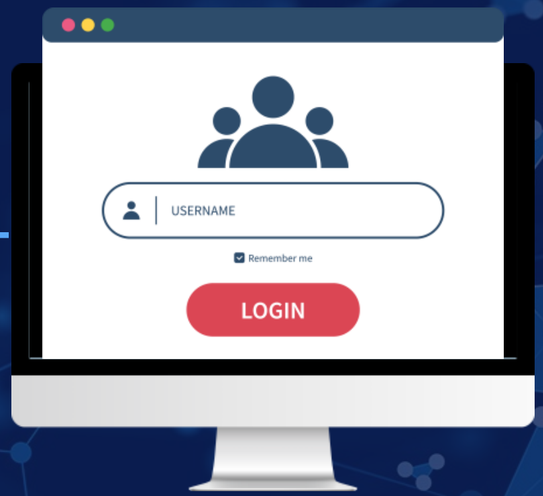
차세대 인증 솔루션

BSA의 핵심 기술

초 간편 인증 방식

솔루션 소개

아이디 입력만으로 간편하고 안전하고 빠르게 로그인을 지원



01 아이디 입력

02 인증

03 인증 완료

솔루션 소개

세계 표준 기술인 BSA는 True Passwordless 방식을 통해 보안성, 편의성을 제공

가장 안전하고,
빠르고, 쉽고,
신뢰할 수 있는
인증 솔루션

ITU[2] 와 파트너십을 체결하는 등 높은 신뢰성을 확보한
세계 표준 기술의 보안 인증 솔루션

계정 접근 및 인증에 탁월한 보안성과 속도, 편의성으로
인증시장의 변화를 선도하는 기술

패스워드를 원천적으로 없앤
"True Passwordless" 보안 인증 솔루션

디지털 인증 서비스에서 최고의
사용자 경험, 보안성, 빠른 인증 처리 속도 및 확장성 제공

☑ 1) BSA : Passwordless Blockchain Secure Authentication
☑ 2) ITU(국제전기통신연합) : International Telecommunication Union

차세대 인증 솔루션

솔루션 소개

BSA는 세계표준기술로서 완벽한 해킹 방지하므로 사용자 자격 증명을 보호함으로써 사이버 공간에서 패스워드를 제거

What?

쉽고 빠르고 안전한 99.99% 해킹차단의
혁신적 보안인증 솔루션

Why?

패스워드를 기억할 필요가 없으므로 해킹
위험이 줄어들어 보안성 제고

How?

개인 기기의 고유 식별정보를 기반으로 일회성
패스워드가 생성되고, 사용 후 완전히 폐기됨

BSA

BSA는 차세대 인증 솔루션입니다

패스워드를
‘완전히’ 없앤
혁신적 인증
솔루션입니다.

세계표준기술

완벽한해킹방지

사용자자격증명보호

관리비용절감

BSA의 핵심 기술

솔루션 소개

BSA는 세계 8개국 특허·세계 표준 기술에 기반한
안전하고 편리한 인증을 제공함

일회성 보안키

- 분산원장 기반의 해킹이 불가능한 인증키로 인증과정의 변조위험을 제거
- 슈퍼앱(원앱)을 서비스하는 금융기업에 적합

다중 사용자 인증요소 임의 조합

- 사용자 기기의 수집한 인증요소들을 임의로 추출하여 조합하는 기술
- 일회성으로 생성되고 삭제되므로 해킹이 불가능

다중 분산 검증

- 보안 수준 극대화를 위한 다중 분산 검증
- 일회성 인증키를 탈취하더라도 검증에 참여할 수 없음

하이브리드 분산원장

- 분산원장기술의 장점을 융합해 신뢰성 · 성능 · 보안성을 최적화

표준 기술

- ITU-T 세계표준화 2건 승인
- 한국을 포함한 전세계 8개국 특허 보유, CCRA 인증(글로벌 레벨 CC인증)
- 국내 과학기술정보통신부/금융위원회 유권 해석 완료

03

주요 기능

BSA 4가지 핵심 기술

1. 다중 사용자 인증요소 임의 조합 | 2. 일회성 인증키 | 3. 다중 분산 검증 | 4. 하이브리드 분장원장 기술

BSA 작동 매커니즘

BSA 인증 프로세스

BSA 4가지 핵심 기술

주요 기능

BSA는 4가지의 핵심 기술을 바탕으로 간편인증과 문서보안, 거래확인(서명), IoT 등 모든 산업에 맞춤형 보안솔루션 제공 가능

Multiple Identifier Random Combination

1. 다중 사용자 인증요소 임의 조합(MIRC)

전체 블록에서 다수의 유일 식별자를
추출하여 해킹이 불가능한 일회성 키 생성

One Time Authentication Key

2. 일회성 인증키(OTAK)

일회성 인증키를 사용해 위·변조위험 제거

Multiple Distributed Validation

3. 다중 분산 검증(MDV)

보안 수준을 극대화하기 위한 다중 분산 검증

Kernel Chain Core

4. 하이브리드 분산원장 기술

Public, Private chain의 장점을 융합해
신뢰성 • 성능 • 보안성 최적화

1. 다중 사용자 인증요소 임의 조합 > BSA 4가지 핵심 기술 > 주요기능

전체 블록에서 다수의 유일 식별자를 추출하여 해킹이 불가능한 키 생성

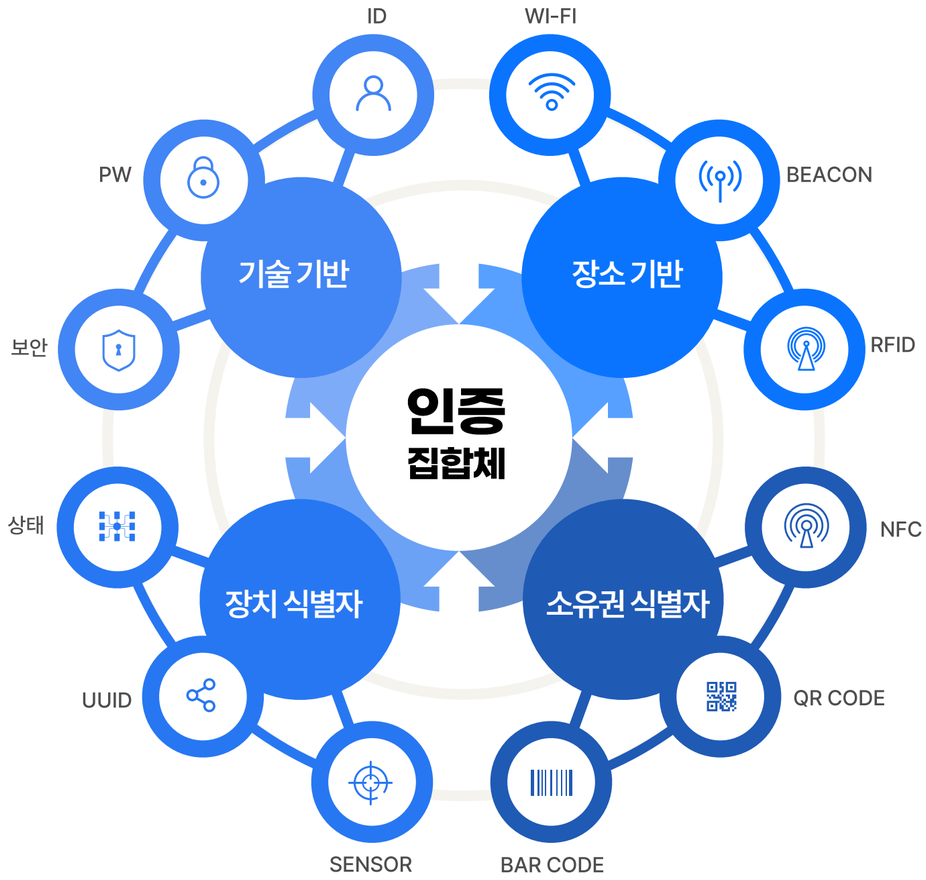
01 사용자 모바일 기기의 고유식별자를 BSA 서버에 전달

02 서버에서 사용자 기기의 고유식별자를 임의로 추출

03 위치, 소유권, 장치 식별자 및 지식 기반 정보의 결합

04 패스워드 없이 안전하게 인증이 가능하도록 일회성 인증키(OTAK) 생성

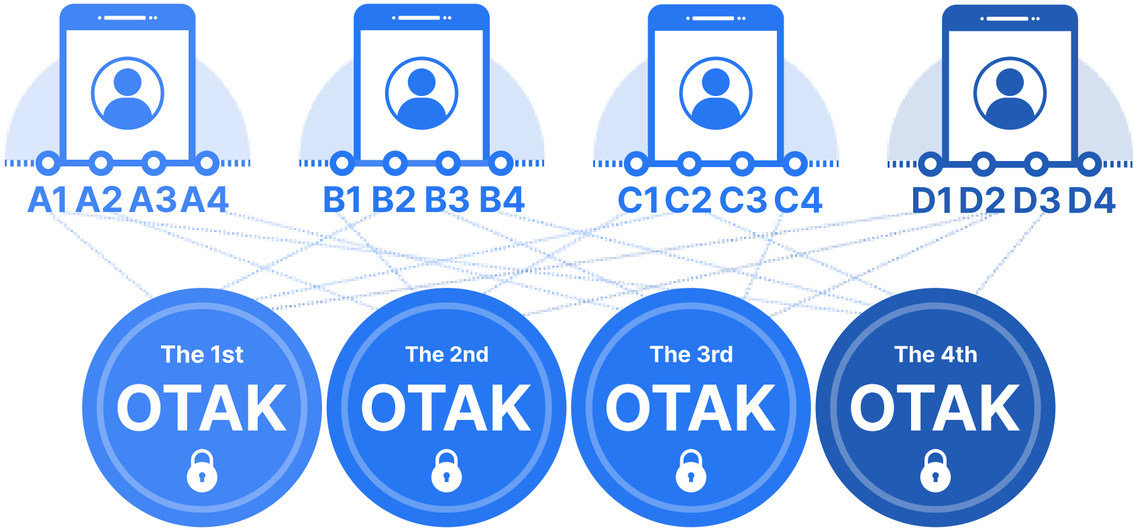
- **전화번호** 01012345678
- **Wi-Fi 정보** FNS iptime
- **주변광 센서** 990
- **기기 고유 번호** 00000000-7849-064-f202-3db11c503a2e
- **Bluetooth 주소** 02:00:00:00:00:00
- **근접센서** 8
- **지자기 센서** 13|52|-39
- **소리 센서** 15|11|0|0|0|0|4



2. 일회성 인증키 > BSA 4가지 핵심 기술 > 주요기능

DLT 기반의 인증으로 해킹이 불가능한 일회성 인증키를 사용해 인증과정에서의 위·변조 위험 제거

OTAK (One-Time Authentication Key) 생성 방법



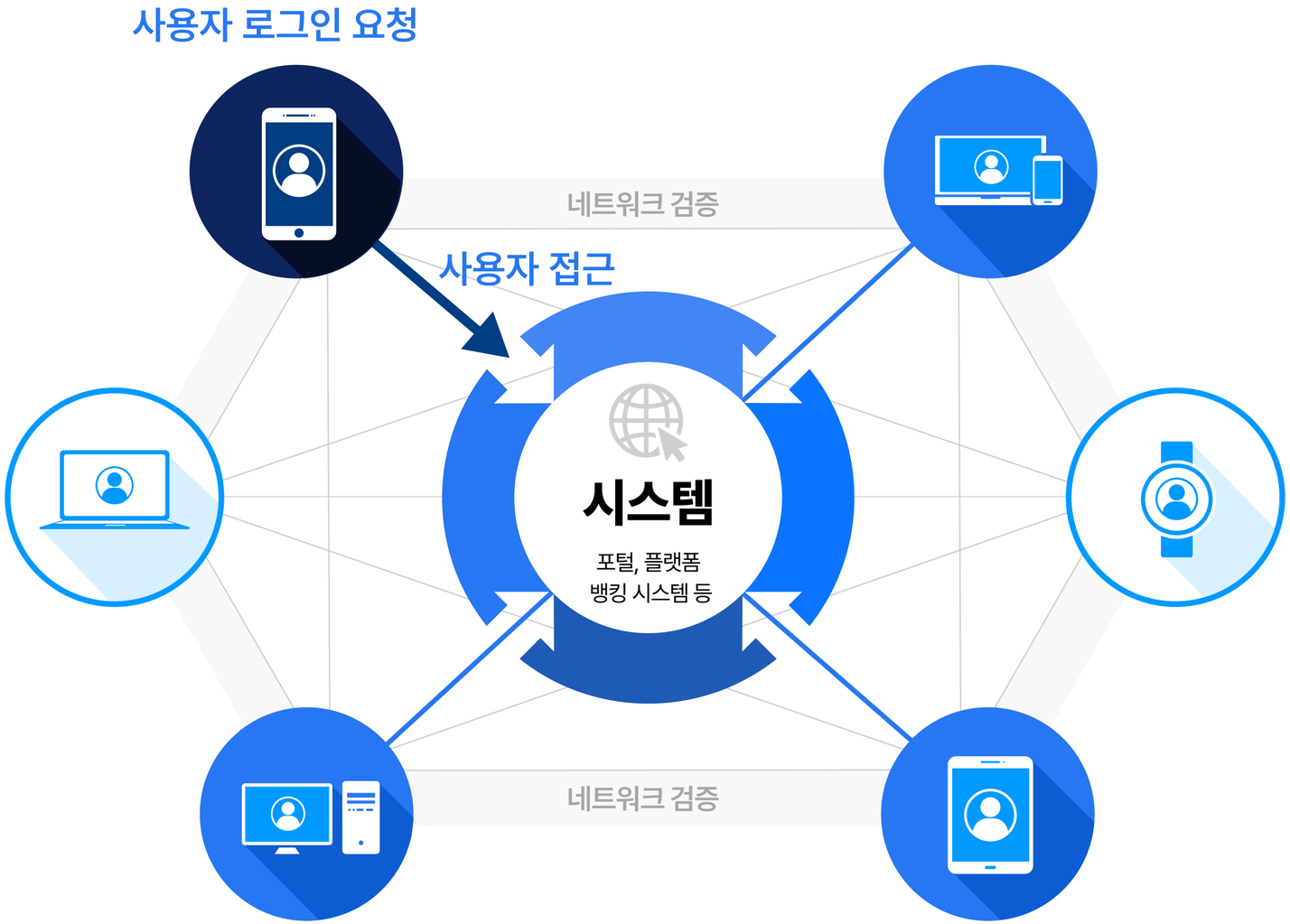
일회성 인증키 (OTAK)	OTAK를 구성하는 랜덤 디바이스 인증 자격 증명
The 1st OTAK	A(1), B(2), C(2), D(2)...
The 2nd OTAK	A(2), B(1), C(1), D(3)...
The 3rd OTAK	A(4), B(3), C(4), D(1)...
The 4th OTAK	A(1), B(4), C(2), D(4)...

[디바이스의 인증 자격을 랜덤으로 선택하여 구성된 OTAK]

인증 절차

- 인증서버는 서비스 제공자의 인증 요청을 수신 후 인증 서버에 저장된 랜덤화된 디바이스 인증 크리덴셜로부터 선택된 데이터를 암호화, 축약, 병합, 재암호화 절차를 거쳐 OTAK 생성
- 생성된 OTAK는 서비스 제공자, 사용자 및 디바이스 검증에 사용되는 노드 중 선택된 노드로 전송하며, OTAK 전달 과정에서 탈취되거나 변경될 가능성을 고려해 재검증하기 위해 사용자는 다시 OTAK를 인증서버에 전송
- 인증 절차가 완료되면 인증 서버는 검증에 사용된 OTAK를 폐기

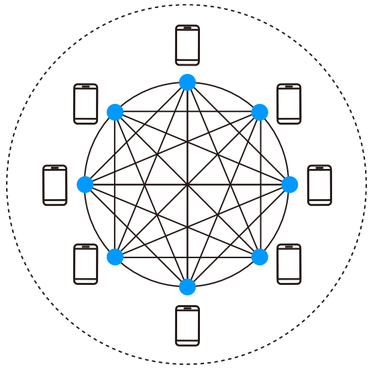
3. 다중 분산 검증 > BSA 4가지 핵심 기술 > 주요기능



4. 하이브리드 분장원장 기술 > BSA 4가지 핵심 기술 > 주요기능

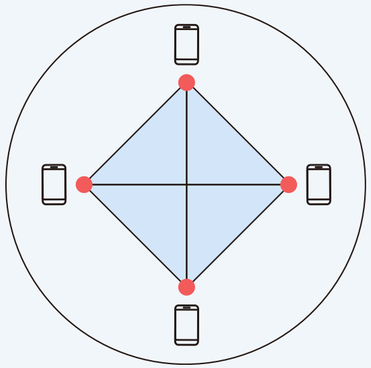
DLT(분산원장기술) 장점을 융합해 신뢰성·성능·보안성 최적화

Public Blockchain



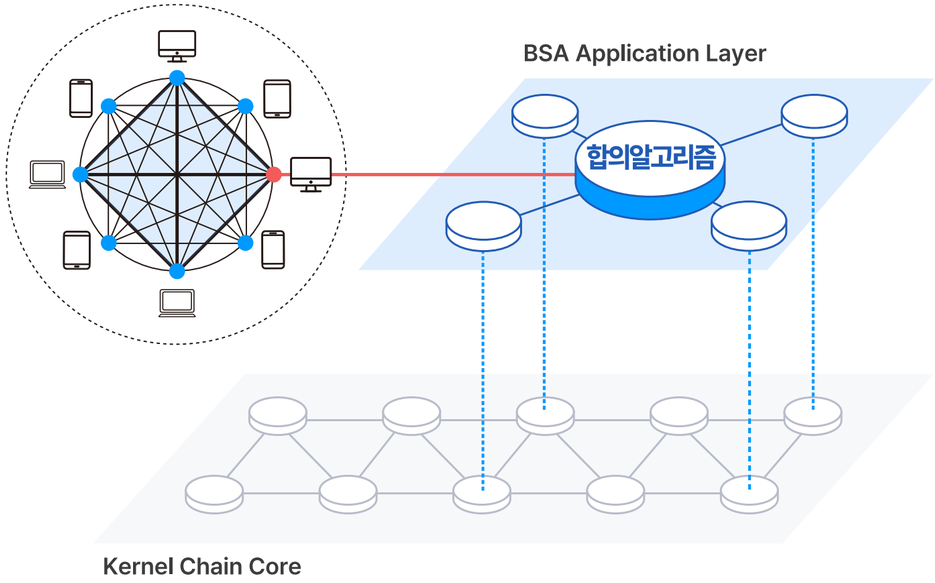
- 일반 대중의 자유롭게 참여할 수 있는 형태의 네트워크 구성
- 개발형 블록체인, 공공 블록체인이라는 명칭을 사용
- 네트워크에 참여하는 개별 컴퓨터, 휴대폰 등의 디바이스를 노드(Node)라 칭함
- 사용자 영역에서는 모든 대중이 자유롭게 참여하고, 개방기술을 제공

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
- Private Blockchain 구성하여 인증처리 영역에 대한 보안성을 강화

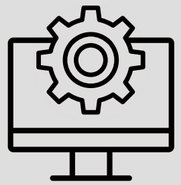
Hybrid Blockchain



- 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

주요 기능

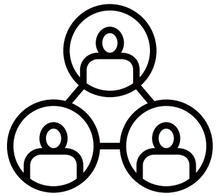
사용자의 간단한 조작으로 안전하고 편리한 인증 서비스 제공



DEVICE

타인이
인증절차
진행 불가

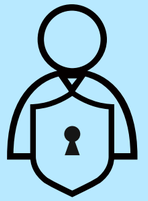
다중 사용자 인증요소 임의 조합
Multiple Identifier Random Combination
MIRC + OTAK
One Time
Authentication Key



COMMUNITY

다중분산검증 기술로
일회성 인증키를
탈취해도 검증 절차에
참여 할 수 없는
극대화된 보안성

MDV 다중 분산 검증
Multiple Distributed Validation



USER

BSA 인증 후
FACE ID,
지문 인식 등으로
보안성 강화

Biometrics

BSA 인증 프로세스

주요 기능

블록체인 기술 기반의 패스워드리스 솔루션으로서 피싱 및 무차별 공격을 원천 차단하며, 사용자들의 간편한 인증을 위한 사용자 인터페이스 제공

STEP 01. 사용자 등록 / 사용자 단말기 정보 수집

STEP 02. 서비스 접속 요청

STEP 03. 인증요청

STEP 04. 채널 및 블록 키 생성

STEP 04. 일회성 인증키 조합

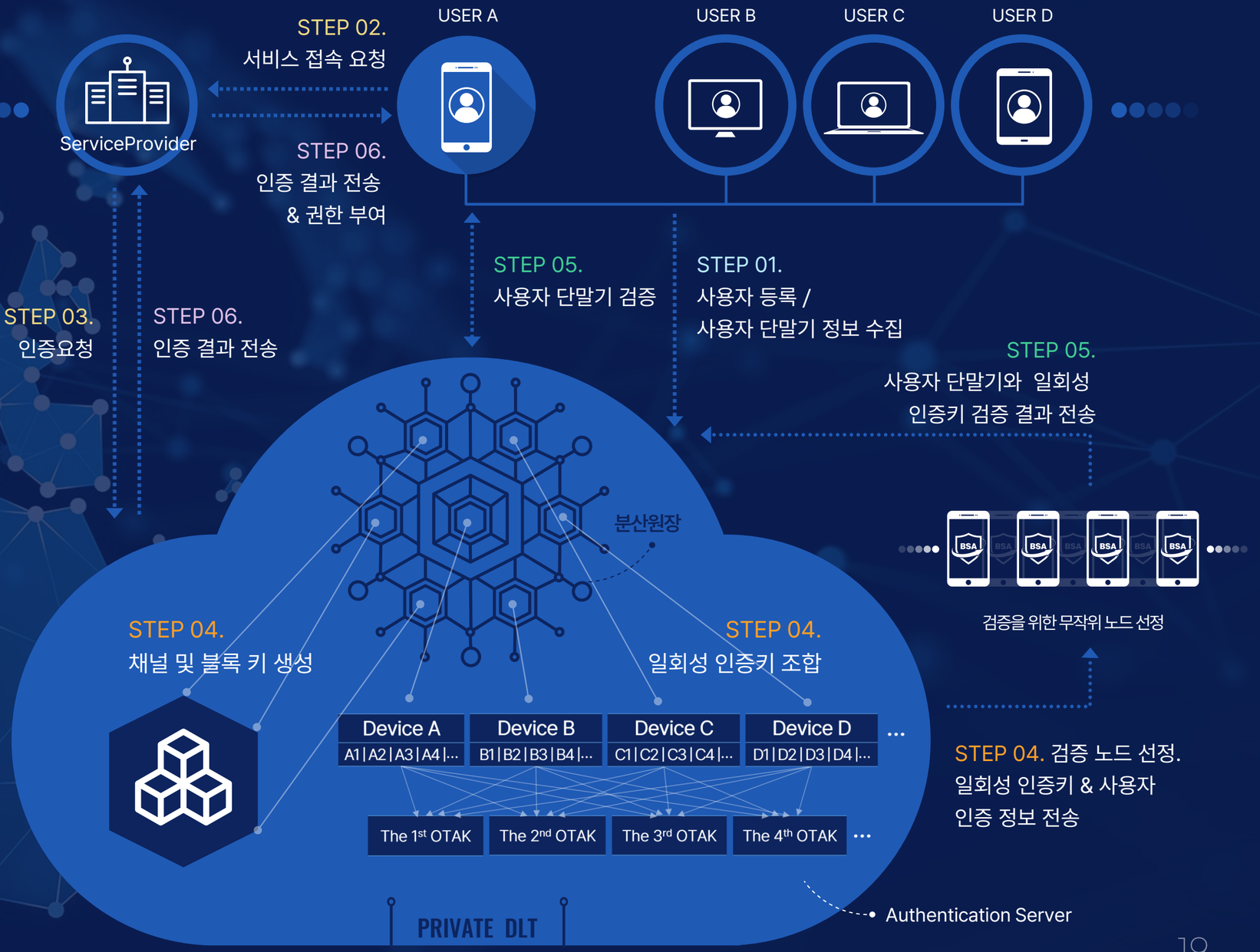
STEP 04. 검증 노드 선정 | 일회성 인증키 & 사용자 인증 정보 전송

STEP 05. 사용자 단말기와 일회성 인증키 검증 결과 전송

STEP 05. 사용자 단말기 검증

STEP 06. 인증 결과 전송

STEP 06. 인증 결과 전송 & 권한 부여



04

솔루션 특징

BSA의 혁신성과 확장성

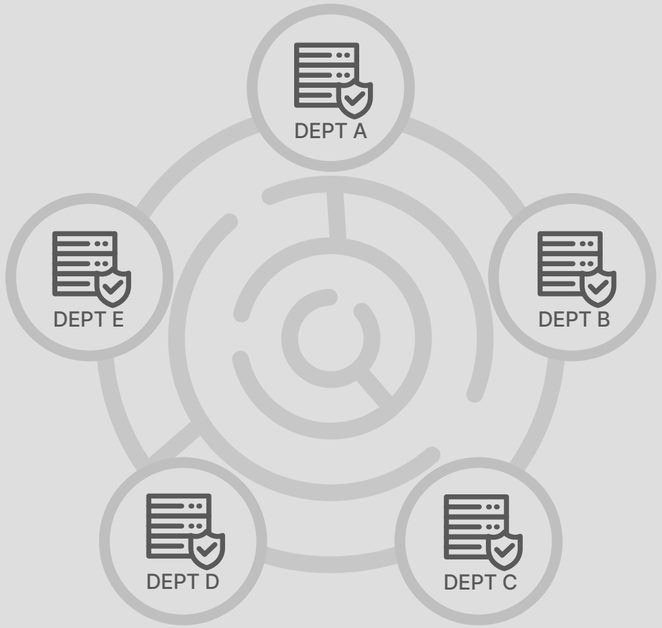
BSA의 경쟁력 및 가치

BSA의 혁신성과 확장성

솔루션 특징

서로 다른 서비스 제공업체의 인증요소를 공유하고 액세스할 수 있도록 확장이 가능하며, 여러 유형의 기업이 협력하여 공동 운영이 가능함

As-Is



사용자가 증가할 시 패스워드
변경과 관리가 복잡하고 시간적,
금전적 부담이 점점 늘어남

Challenges

Objective

다양한 서비스 제공자의 인증 요소를 공유하고 액세스할 수
있도록 확장이 가능하므로 여러 기업이 협력해서 공동 운영 가능

Value

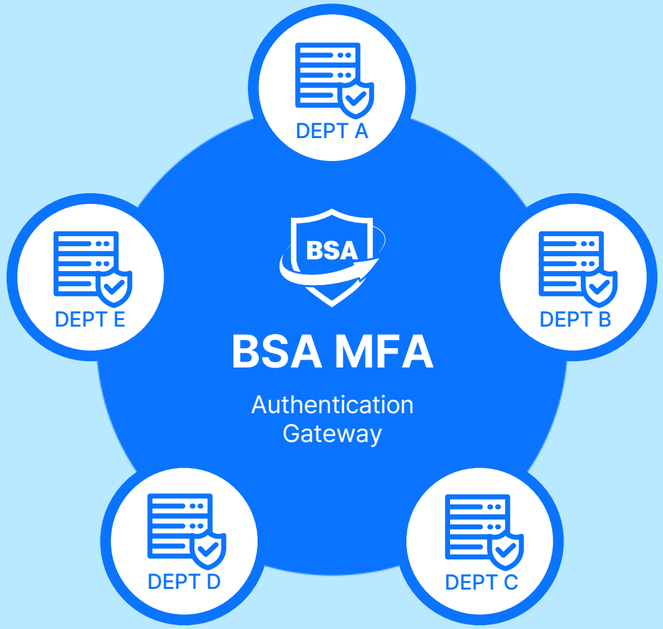
- User Value -

신뢰할 수 있고 일관된 인증 방법을 제공하고 데이터를 보호할
수 있도록 지원

- Organization Value -

신속하고 간편한 인증을 통해
패스워드 관리 비용 절감

To-Be



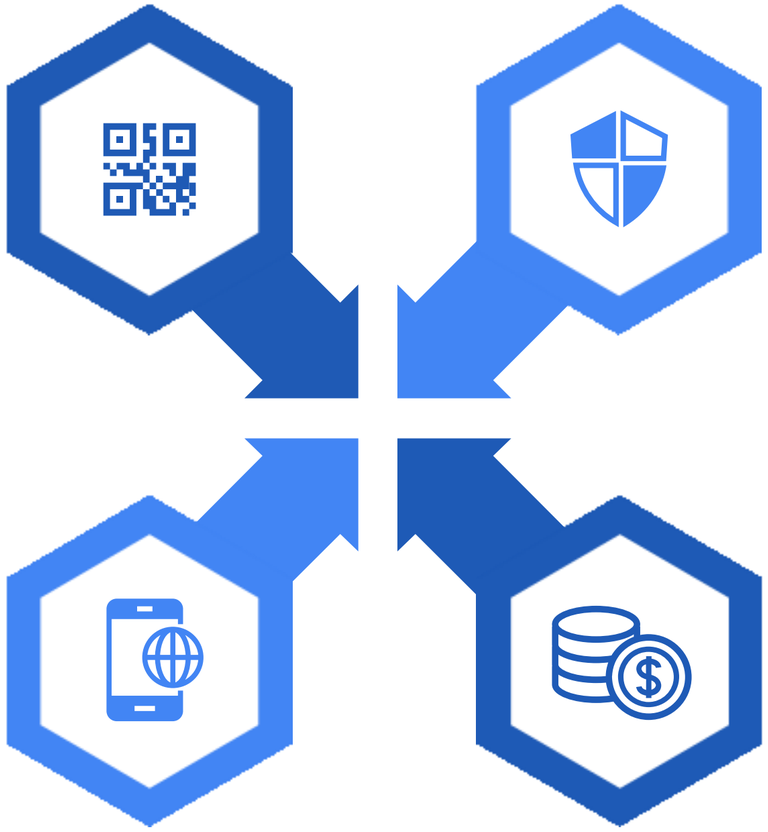
BSA는 사용자 및 장치 접근에 대한
사용자 인증 보안 정책을 표준화,
단순화하여 서비스 통합 운영

솔루션 특징

BSA는 세계 표준 기술로 국내 관련 당국의 유권해석으로 신뢰할 수 있으며, 안전하고, 편리하며, 관리비용을 절감할 수 있음

편의성

- 패스워드리스 방식의 원스톱 인증
- 0.5초 내의 고속 인증
- 사용자 친화적의 편의성 제공



안전성

- 일회성 인증키 사용으로 해킹 불가능
- KOIST, TTA 시스템 성능 검사 완료

신뢰성

- 세계표준기술
- 과기정통부 / 금융위원 유권해석 획득
- CCRA (글로벌 레벨 EAL2 획득)

비용 절감

- 패스워드 관리를 위한 물적비용 절감
- 관리 인적비용 절감

05

평판 & 수상 이력

UN 산하 ITU가 선택한 Passwordless 블록체인 보안인증 파트너

세계적으로 인정받은 기술력

과학기술정보통신부 · 금융위원회 유권해석

평판 & 수상 이력

ITU를 통한 세계표준기술 추진 및 전세계 유일의 ITU 공식 파트너

2023 9월
표준화 연구 아이템 승인

2024년 9월
제네바 국제회의에서 X.afotak 사전 채택

2025년 3월
Recommendation(권고안) 승인

세계적으로 인정받은 기술력

평판 & 수상 이력

글로벌 레벨의 CC인증인 CCRA 인증 획득, OIC-CERT GLOBAL CYBERSECURITY AWARD 대상 수상 및 전 세계 8개국에 혁신성을 인정 받은 기술특허 보유

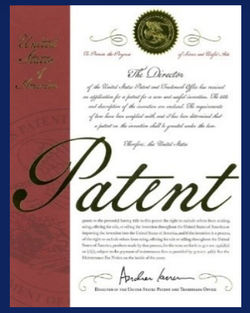
Cybersecurity Certification ISO/IEC15408
(CC인증/글로벌 레벨)

2021 OIC-CERT 글로벌 어워드 Cybersecurity 대상 수상

한국

대만

말레이시아



미국

중국

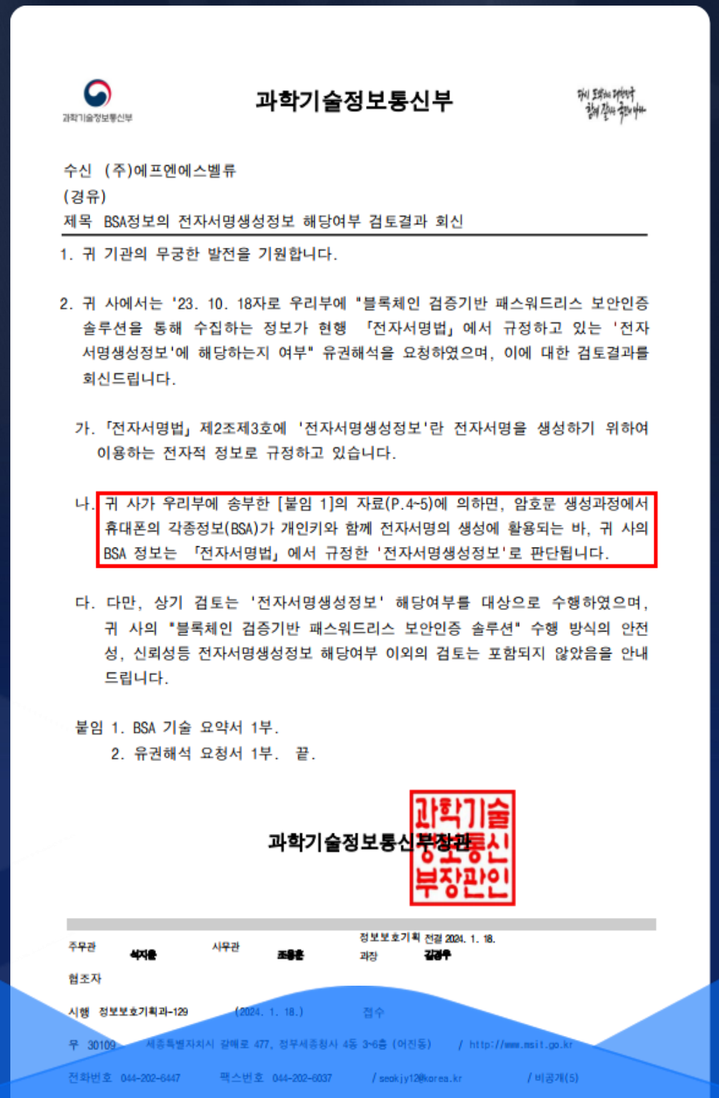
일본

싱가포르

영국

평판 & 수상 이력

과학기술정보통신부와 금융위원회로부터 국내 최초로 BSA의 기술이 유권해석을 완료함으로써 국내 보안인증 솔루션 시장 본격 진출



과학기술정보통신부

과학기술정보통신부

수신 (주)에프엔에스벨류
(경유)
제목 BSA정보의 전자서명생성정보 해당여부 검토결과 회신

1. 귀 기관의 무궁한 발전을 기원합니다.

2. 귀 사에서는 '23. 10. 18자로 우리부에 "블록체인 검증기반 패스워드리스 보안인증 솔루션을 통해 수집하는 정보가 현행 「전자서명법」에서 규정하고 있는 '전자서명생성정보'에 해당하는지 여부" 유권해석을 요청하였으며, 이에 대한 검토결과를 회신드립니다.

가. 「전자서명법」 제2조제3호에 '전자서명생성정보'란 전자서명을 생성하기 위하여 이용하는 전자적 정보로 규정하고 있습니다.

나. 귀 사가 우리부에 송부한 [붙임 1]의 자료(P.4-5)에 의하면, 암호문 생성과정에서 휴대폰의 각종정보(BSA)가 개인키와 함께 전자서명의 생성에 활용되는 바, 귀 사의 BSA 정보는 「전자서명법」에서 규정한 '전자서명생성정보'로 판단됩니다.

다. 다만, 상기 검토는 '전자서명생성정보' 해당여부를 대상으로 수행하였으며, 귀 사의 "블록체인 검증기반 패스워드리스 보안인증 솔루션" 수행 방식의 안전성, 신뢰성등 전자서명생성정보 해당여부 이외의 검토는 포함되지 않았음을 안내드립니다.

붙임 1. BSA 기술 요약서 1부.
2. 유권해석 요청서 1부. 끝.

과학기술정보통신부장관

과학기술정보통신부 장관인

정보보호기획 전결 2024. 1. 18.

주무관 박지윤 시무관 조종훈 과장 김경주

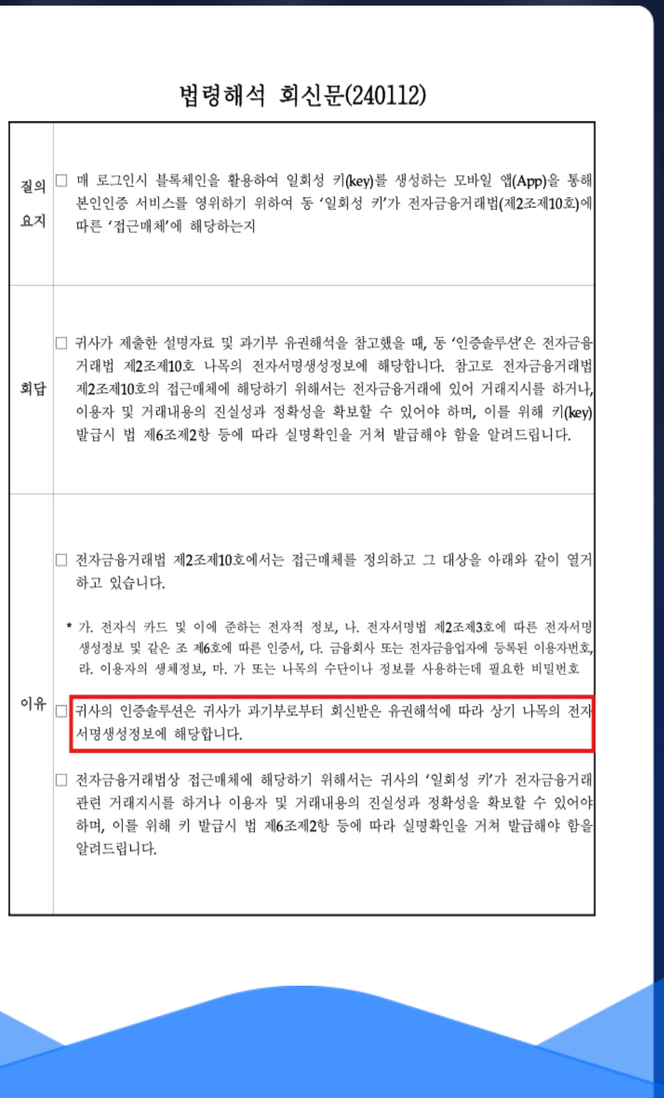
협조자

시행 정보보호기획과-129 (2024. 1. 18.) 접수

우 30109 세종특별자치시 갈매로 477, 정부세종청사 4동 3~6층 (어진동) / http://www.msit.go.kr

전화번호 044-202-6447 팩스번호 044-202-6037 / seokjy12@korea.kr / 비공개(5)

과학기술정보통신부 유권해석



법령해석 회신문(240112)

질의 요지	□ 매 로그인시 블록체인을 활용하여 일회성 키(key)를 생성하는 모바일 앱(App)을 통해 본인인증 서비스를 영위하기 위하여 동 '일회성 키'가 전자금융거래법(제2조제10호)에 따른 '접근매체'에 해당하는지
회답	□ 귀사가 제출한 설명자료 및 과기부 유권해석을 참고했을 때, 동 '인증솔루션'은 전자금융거래법 제2조제10호 나목의 전자서명생성정보에 해당합니다. 참고로 전자금융거래법 제2조제10호의 접근매체에 해당하기 위해서는 전자금융거래에 있어 거래지시를 하거나, 이용자 및 거래내용의 진실성과 정확성을 확보할 수 있어야 하며, 이를 위해 키(key) 발급시 법 제6조제2항 등에 따라 실명확인을 거쳐 발급해야 함을 알려드립니다.
이유	□ 전자금융거래법 제2조제10호에서는 접근매체를 정의하고 그 대상을 아래와 같이 열거하고 있습니다. * 가. 전자식 카드 및 이에 준하는 전자적 정보, 나. 전자서명법 제2조제3호에 따른 전자서명생성정보 및 같은 조 제6호에 따른 인증서, 다. 금융회사 또는 전자금융업자에 등록된 이용자번호, 라. 이용자의 생체정보, 마. 가 또는 나목의 수단이나 정보를 사용하는데 필요한 비밀번호 □ 귀사의 인증솔루션은 귀사가 과기부로부터 회신받은 유권해석에 따라 상기 나목의 전자서명생성정보에 해당합니다. □ 전자금융거래법상 접근매체에 해당하기 위해서는 귀사의 '일회성 키'가 전자금융거래 관련 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보할 수 있어야 하며, 이를 위해 키 발급시 법 제6조제2항 등에 따라 실명확인을 거쳐 발급해야 함을 알려드립니다.

금융위원회 유권해석

06

도입 사례

BSA 솔루션 적용 & 진행중인 고객 현황

도입 사례

해외에서 먼저 기술력을 인정 받은 BSA

고객별 BSA 솔루션 적용 사례 및 세부 정보

분야	고객	프로젝트	세부 정보
공공	Sarawak Digital Economy Corporation Berhad (SDEC)	MyVMS	• 회사 인증 시스템에 BSA 적용 • 화이트 라벨 애플리케이션 배포 • 사용자 : 임직원
공공	Inland Revenue Board of Malaysia (LHDN)	MYDATA+	• 회사 인증 시스템에 BSA 적용 • 1) 화이트 라벨 애플리케이션 배포 • 사용자 : 임직원
기업 및 엔터프라이즈	PETRONAS Dagangan Berhad (PDB)	Secured VPN access	• Fortiget Secured VPN access에 BSA 적용 • BSA를 인증자 및 다중 요소 인증(MFA)으로 사용 • 사용자 : 임직원 및 거래처
기업 및 엔터프라이즈	Landasan Network Solutions (LNS)	Secured VPN access	• Fortiget Secured VPN access에 BSA 적용 • BSA를 인증자 및 다중 요소 인증(MFA)으로 사용 • 사용자 : 임직원
기업 및 엔터프라이즈	Big Dataworks (BDW)	MYDATA+	• BDW 솔루션에 BSA 적용 • 화이트 라벨 애플리케이션 배포 • 사용자 : 임직원 및 BDW 고객
기업 및 엔터프라이즈	Rakan Net	Secured VPN access	• 회사 인증 시스템에 BSA 적용 • 화이트 라벨 애플리케이션 배포 • 사용자 : 임직원

☑ 1) 화이트 라벨 : 상품이나 서비스의 원산지나 브랜드를 숨기고 다른 브랜드로 제공하는 형태를 의미. 즉, BSA 상표를 숨기고 대신 고객사의 상표로 애플리케이션을 제작, 배포

도입 사례

해외에서 먼저 기술력을 인정 받은 BSA

고객별 BSA 솔루션 적용 사례 및 세부 정보

분야	파트너	고객	프로젝트	세부 정보
기업 및 엔터프라이즈	Big Dataworks (BDW)	정부 기관 및 일반 사용자	MyDigital ID	• MyDigital ID 플랫폼을 기반으로 프레임워크를 개발 중이며 BSA는 접근 보안을 보완하는 인증 요소 역할
기업 및 엔터프라이즈	Heitech Padu	정부 및 기업 부문	1) POC(Proof Of Concept)	• Heitech Padu 자체 시스템에 BSA 적용
기업 및 엔터프라이즈	Heitech Padu	정부 및 기업 부문	POC(Proof Of Concept)	• Heitech Padu 고객을 위한 보안 서비스로서의 BSA 적용
교육	Koleksi Niaga (KN)	Mulawarman University (UNMUL)	POC(Proof Of Concept)	• SSO 시스템에 BSA 적용 • BSA를 인증자 및 다중 요소 인증(MFA) 으로 사용 • 대상 사용자: 교수, 학생 및 직원

☑ POC(Proof Of Concept) : 아이디어나 기술이 실제로 작동하는지 입증하기 하기 위한 실험적 구현이나 시제품을 제작하는 과정

07

구축 및 유지보수

구축 방법론

유지보수 관리

구축 및 유지보수

체계적인 구축 절차를 통해 BSA 인증 시스템을 성공적으로 구축

에프엔에스벨류 고객사

KICK-OFF

- 계약사항 및 담당자 안내
- 구축 일정 협의 및 구축 시 사전 필요항목 안내

운영 환경 분석

- 시스템 환경 분석 (OS, DB, 이중화, 네트워크, 방화벽 설정 등)

연동 시스템 개발 협의

- 연동 시스템 개발을 위한 협의 및 API 제공

SW 설치

- BSA 인증 시스템 설치 (서버, 모바일 등)

시스템 설정 및 교육

- 사용자 정보 등 연동 및 SMTP, 인증정책 설정
- 운영을 위한 관리자 교육

단위 테스트

- 사용자 정보 등 연동 및 SMTP, 인증정책 적용 테스트
- BSA 연동 테스트

통합 테스트

- 통합 테스트
- 시험 운영

운영

- BSA 인증 시스템 운영

연동 시스템 개발

- 패스워드리스 로그인을 위한 페이지 수정 개발 진행

구축 및 유지보수

유지보수 및 운영 고도화 지원

A/S

(요구사항 접수)

접수
(전화, Email 등)

1차 즉시 해결

2차 운영 고도화

- 유지보수 접수 및 내용 확인
- 유지보수 유형 세부분석
- 접수 조치 및 결과보고
- 유지보수 이력 관리

1. 유지보수 접수 및 내용 확인

- 접수 : 고객사 > 유지보수지원팀
- 유형 구분 – 장애, 기능 문의 및 개선, 추가개발 등
- 요구사항 발생 시 고객사 담당자에게 우선 보고

2. 유지보수 1차 조치

- 바로 해결이 가능한 요구사항 즉시 조치

3. 유지보수 유형 세부분석

- 유지보수지원팀 자체적으로 해결이 어려운 부분은 개발팀으로 통보하여 공동 대응
- 조치사항 관리와 유형 분석을 통한 유사상황 대응

4. 유지보수 2차 조치

- 상황에 따른 개발팀 공동 대응 및 조치 진행
- 방문 조치가 필요한 상황 시 고객사 방문 대응
- 조치사항 기록 및 유형 분석

5. 접수 조치 결과보고

6. 유지보수 이력 관리

08

Annex

Frequently Asked Questions on BSA

Frequently Asked Questions on BSA

사용자 등록을 위해 필요한 정보는 무엇인가요?

아이디, 사용자명, 이메일, 휴대폰 번호 총 4가지 정보를 수집하며, 이 외에 다른 개인 정보나 사용자 데이터를 수집하지 않습니다.

두 개 이상의 기기에 BSA를 설치하려면 어떻게 해야 하나요?

BSA는 사용자 계정당 한 대의 기기만 허용합니다. 기기가 분실되거나 도난 당하거나 업그레이드가 필요한 경우, 새 기기를 등록 할 수 있으며, 이전 기기는 사용할 수 없습니다.

BSA 계정을 삭제할 수 있나요?

네, 앱의 My Page에서 “회원 탈퇴"를 선택해 계정을 삭제할 수 있습니다.

시장의 다른 패스워드리스 인증과 차별화되는 점은 무엇인가요?

비밀번호를 저장하지 않고 인증시에 일회성 인증키를 생성하므로 중간 공격자가 일회성 인증키를 탈취하더라도 인증에 참여할 수 없어 보안성이 매우 높습니다.

Thank you

(주) 에프엔에스벨류

02-303-3885 02-304-3885

서울특별시 마포구 월드컵북로 396,7층 (상암동, 누리꿈스퀘어 연구개발타워)

hannah@fnsvalue.co.kr (대외협력부 장헌주 상무)

www.fnsvalue.co.kr