Secure Authentication Solution

# Guardian-CCS


FNSVALUE
FEASIBLE NETWORK SYSTEM VALUE

# About **Company**

(주)에프엔에스벨류는 창업 이래 끊임없는 기술 개발을 통해 고객사의 시스템 구축 및 운영관리를 기업환경에 맞춤형으로 지원하고 독자적인 기술인 'Guardian-CCS' 간편 보안 인증 솔루션을 개발하여 차세대 보안 인증 시장을 선두하고 있습니다.

**대표** 전승주 **주소** 서울 마포구 월드컵북로 396(상암동, 누리꿈스퀘어) 연구개발타워 7층

**설립일** 2012년 4월 3일 **업종** SI/SM, 보안컨설팅, 통합시스템, 사이버 보안 솔루션

**증명서** Main-BIZ, Inno-Biz, Good Software Level 1, ISO9001, ISO27001, Public Procurement Service

# FNSVALUE History

## 2021

미래에셋증권 IPO 주관사 선정 및 코스닥 상장 추진
인도네시아 PT VADS 솔루션 및 라이선스 공급 계약 체결
제7회 대한민국 우수기업대상, 보안인증솔루션 우수기술대상 수상
과학기술정보통신부 '소프트웨어 고성장클럽' 사업 고성장 기업 선정
2021년 한국핀테크지원센터 해외진출 컨설팅 사업 선정
2021년 중소벤처기업부 수출바우처 기업 선정
OIC-CERT 글로벌 사이버 보안 대상 수상
Guardian-CCS v1.0 우수제품지정 - 조달청
2021 대한민국 우수기업대상 우수기술대상
정보보호경영시스템 ISO 27001 인증 취득

## 2020

말레이시아 Telekom Malaysia 솔루션 및 라이선스 공급 계약 체결
FNS[M] 말레이시아 현지 법인 설립
한국지식재산보호원 사업 선정
한국핀테크지원센터 해외진출 컨설팅 사업 선정
중소벤처기업부 수출바우처 기업 선정

## 2019

말레이시아 Telekom Malaysia MOC 체결
글로벌 엑셀러레이팅(싱가포르) 프로그램 이수 [창업진흥원]
품질경영 ISO 9001 인증 취득
간편보안인증솔루션 [Guardian-CCS v1.0] GS 인증 취득
경영혁신형 중소기업 [Main-Biz] 취득
말레이시아 Hong Leong Bank Vendor 등록
핀테크 보안컨설팅 완료[금융보안원]

## ~2018

여성가족부 가족친화기업 인증
말레이시아 국방 POC 수주 및 완료
기술혁신형 중소기업[Inno-Biz] 취득

## 2012

에프엔에스벨류 법인 설립

차세대 보안 인증 솔루션

# PASSWORDLESS
# Guardian-CCS


**FAST** **EASY** **SAFE**

# 디지털 시대에 발맞춰 **보안성, 속도, 편리성, 신뢰성을 갖춘 솔루션**

**01.** G-CCS 는 세계 최고 수준의 보안 인증 솔루션이며 높은 신용도를 자부합니다.

**02.** G-CCS 는 Passwordless 블록체인 보안 인증을 통해 세상을 더 안전하게 변화시킵니다.

**03.** G-CCS 만의 우수한 보안성과 속도, 편리성은 계정 접근과 인증에 있어 디지털 전환 시대를 선도하는 기술로 급부상하고 있습니다.

**04.** G-CCS 는 고객경험과 프라이버시 보호, 보안, 유지성, 확장성 측면에서 월등한 디지털 인증 서비스를 제공합니다.

**05.** G-CCS 는 Zero Trust를 토대로 보안성, 프라이버시, 신뢰성에 초점을 맞추었습니다.

**06.** G-CCS 는 범국가적 사이버 문제로 대두되고 있는 신분 도용, 피싱, 랜섬웨어, 무차별 대입 공격, 비밀번호 도용 등에 대한 해결책입니다.

Increase cybersecurity responsiveness

# Guardian-CCS를 통한 **사이버 보안 대응력 제고**

## 보안
Secure

- Zero Trust 프레임워크 (ZTF)
- 능동적 사이버 방어 (ACD)
- Defense in Depth (DID)

## 프라이버시 & 규제
Privacy & Regulatory

- 국내외의 프라이버시 기준과 규제
- 데이터 및 국내 소유권

## 사용자 및 고객경험
User and customer experience

- 초고속 & 편리성
- 3초 미만의 빠른 속도

## 운영방식, 비용절감
Operation method, Cost reduction

- IT 운영과 사용자 지원 간소화
- 운영비용 절감
- 사용자 생산성 향상
- 고객 경험과 효용성 강화

Passwordless blockchain security

# 기업과 기업 고객, 공급 사슬에 대한 **Passwordless 블록체인 보안**

## 거버넌스와 위험관리

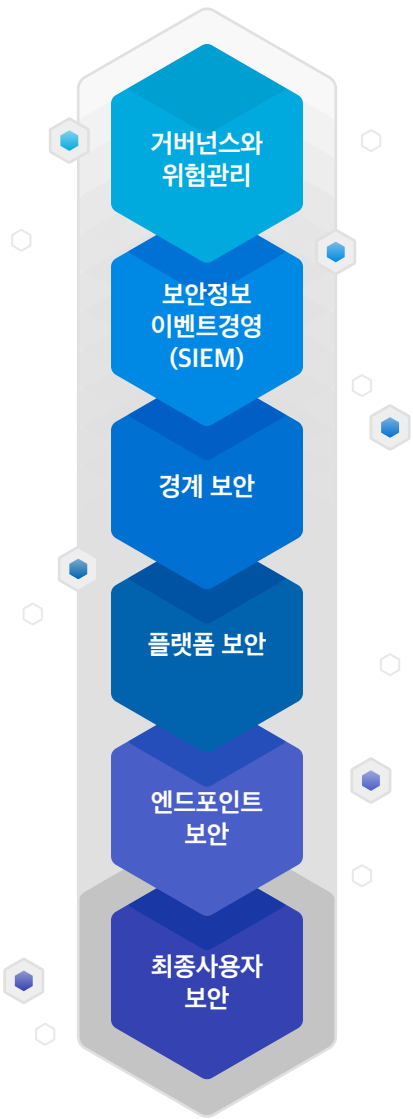
- ISO 27001 준수
- 인터넷보안센터(CIS) 통제권
- 연간 3회의 침투 테스트
- 개인 정보 보호 수료
- GDPR / CCPA 준수
- 기업 위험 등록
- NIST SP 800-53 준수
- SSAE 19 SOC 1 타입 2 수료
- 표준 정보 수집 (SIG)
- 정보 보안 감사 보고서
- 기업 사고 대응

## 플랫폼 보안

- 차사대 방화벽
- 바이러스백신 서버
- Rest에서 AES 256 암호화
- 분리된 Active Directory & VLANS
- 특화된 계정 보관
- 끊임없는 취약점 관리 & 패치 관리
- 보안 데이터 백업과 피해 복구
- 운영 시스템 강화

## 최종사용자 보안

- 사이버 보안 인지 교육
- 다인자 인증
- 역할 기반 접근 통제
- 모의 피싱 캠페인




## 보안정보 이벤트 경영 (SIEM)

- Raw Logs, 엔드포인트 데이터 & 네트워크 트래픽 분석
- 통합된 로그 데이터
- 사용자 행동 분석(UBA)
- 의심 행동 방어 & 알림

## 경계 보안

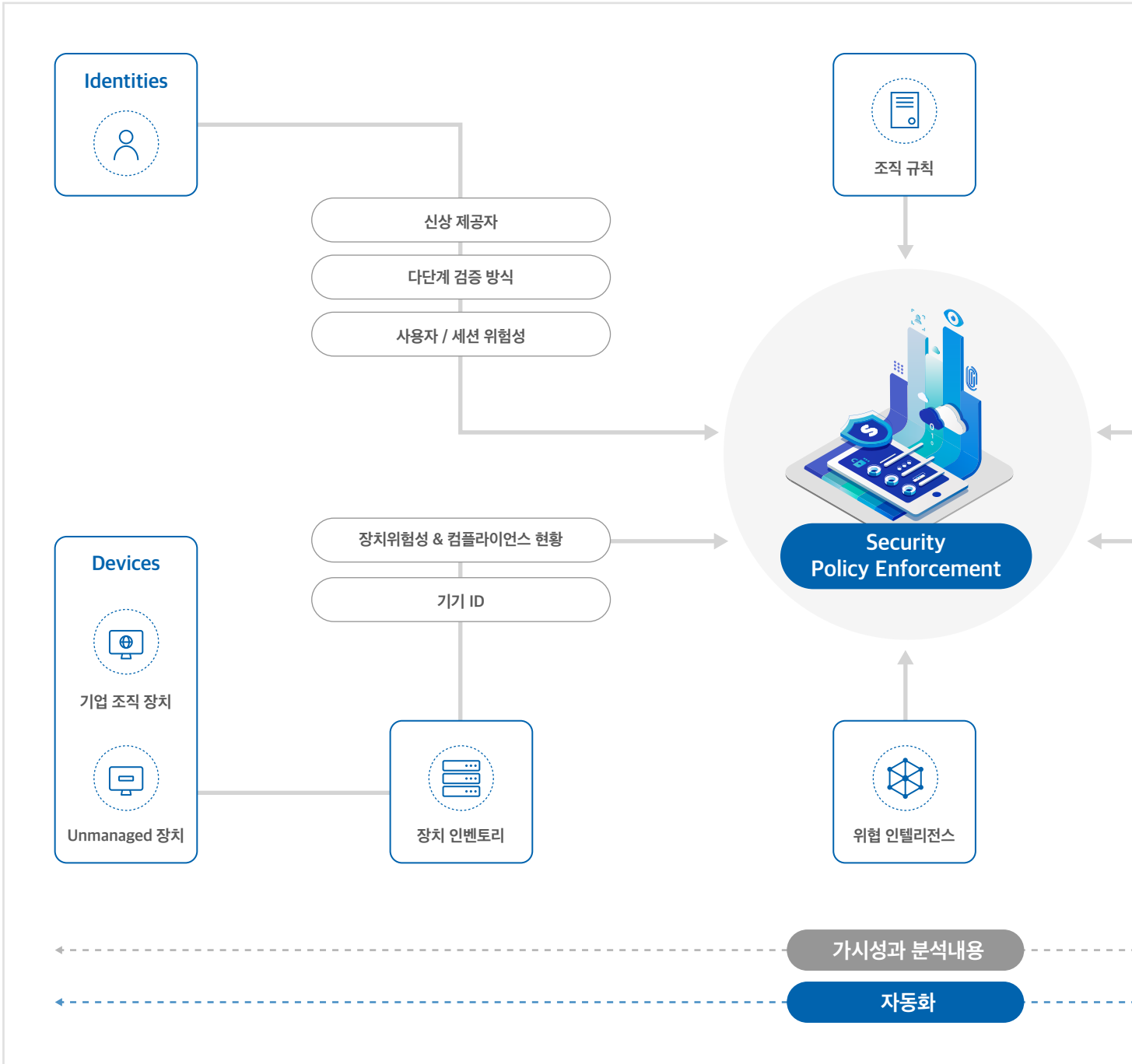
- 외부 방화벽
- 원격 통제
- 스팸 필터링
- 위협 인텔리전스 피드
- 원격 인증 보고
- 무차별 공격과 도스 방어
- 데이터 센터 물리적 보안

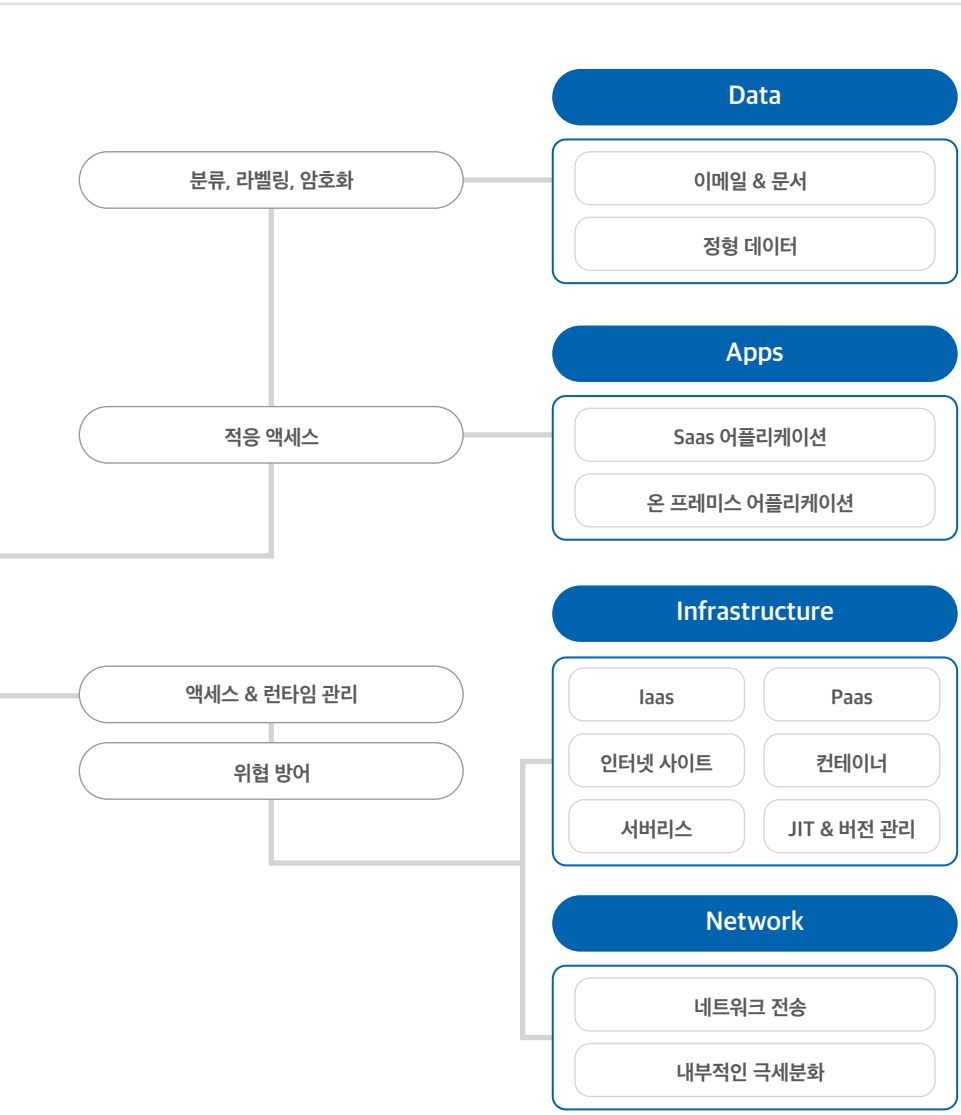
## 엔드포인트 보안

- 자동화된 마이크로소프트 윈도우와 제3자 어플리케이션 패치 관리
- 백신과 엔드포인트 감지 및 대응 (EDR)
- 원격 모니터링 및 관리 시스템
- 로칼 관리자 암호 솔루션
- 전체 디스크 암호화
- 모바일 장치 관리
- 그룹 규칙 강화
- 암호 복장성
- 무차별 공격 방어

Never trust, always verify

# **Zero Trust :** 개인신상, 장치, 어플, 데이터, 인프라, 네트워크에 대한 보안 접근




Data
분류, 라벨링, 암호화
이메일 & 문서
정형 데이터
Apps
적응 액세스
Saas 어플리케이션
온 프레미스 어플리케이션
Infrastructure
액세스 & 런타임 관리
위협 방어
Iaas
Paas
인터넷 사이트
컨테이너
서버리스
JIT & 버전 관리
Network
네트워크 전송
내부적인 극세분화

G-CCS MFA the next generation leader

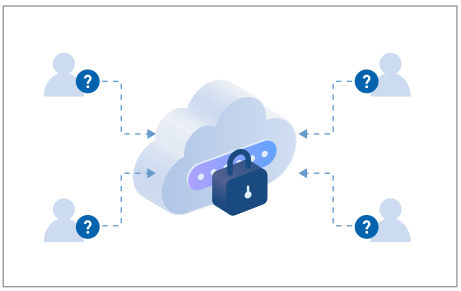
# 차세대 Passwordless **Guardian-CCS MFA**

## 비밀번호 및 Legacy MFA

"비밀번호 관련 보호 위반이 80% 가량에 달한다."

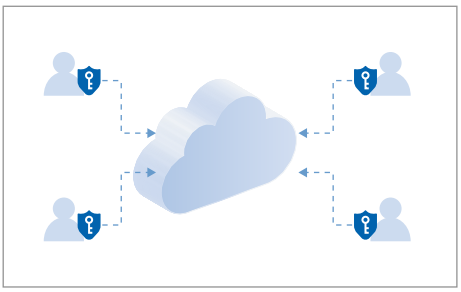
데이터 위반 조사기관 보고서, Verizon - DBIR 참고

- 로그인 충돌 잦음. 사용자가 분열됨
- 비밀번호에 의존해 비밀보안 위험
- 신용정보 재사용 및 2FA 피싱 의심
- 사용자와 데스크탑 MFA 간의 수용 격차



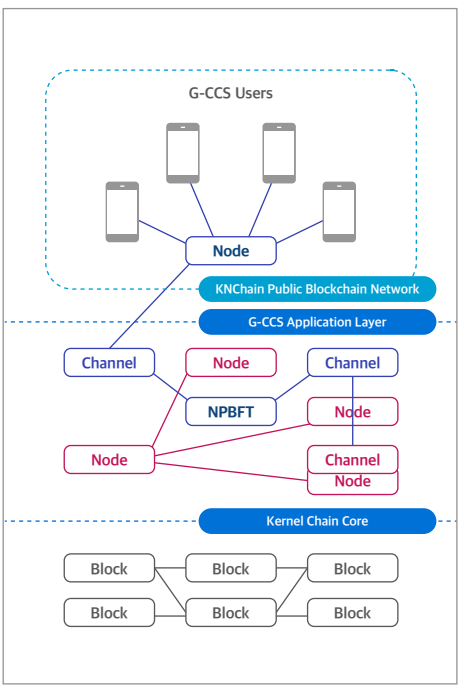
## 정확한 Passwordless MFA

- 초고속의 사용자 경험 제공
- 비밀번호를 공공키 암호로 대체
- 신용정보 스터핑, 사기 및 피싱 방지
- 사용자와 데스크탑 MFA의 간극 해결



## 정확한 Passwordless MFA

- 초고속의 사용자 경험 제공
- 비밀번호를 블록체인 OTSK 로 대체
- 신용정보 스터핑, 사기 및 피싱 방지
- 보안성, 고객, 데스크탑 MFA의 간극 해결




### Design for security, trust, privacy and UX

# Guardian-CCS의 **보안성, 신뢰성, 프라이버시 보호**

### 01 사용자 경험

업계 최초, 고객사와 최종 사용자가 계정에 접근하고, 프라이버시를 보호하는 데에 있어 높은 수준의 보안성과 신뢰성, 편리성을 보장합니다.

### 02 안전성 기반 설계

해킹 침투 위험을 업계 최소 수준으로 낮추어(오차확률 0.02%) 강도 높은 안전성을 보장하며, 인증 처리 절차도 3초안에 완료됩니다. MIRC, OTSK, MDV, KNChain 만의 우수한 특허 기술로 하이브리드 블록체인 검증, 검토, 인증을 실행합니다. 피싱, 랜섬웨어, 계정탈취(ATO), 신용 도용, 사기 및 기업 대상 공격 등의 내외부적 위협을 철저히 제거합니다.

### 03 프라이버시 기반 설계

PDPA 2021, GDPR, RMiT, PCI-DSS, HIPAA 에 의거한 국제·국내 프라이버시와 데이터 보호 규범 및 기준을 준수하여 설계되었습니다.

### 04 신뢰 기반 설계

확인 또는 인증 절차를 위해 사용자와 디바이스 프로필을 통해 기기를 검증합니다. 최소한의 필수적인 데이터만을 저장하며 보안 규제와 기준에 따라 사용할 것을 보장합니다. 최종 사용자와 기기에 사용된 얼굴/지문 등의 생체인식 정보를 포함하는 2FA 데이터는 일체 저장하지 않습니다.

### Digital service through technology

# 보안, 수행능력, 편리성, ROI로 **디지털 서비스 실현**

#### 보안

- 다자간 검증 방식
- 일회성 보안키 보안 (OTSK)
- 보안 블록체인 핵심

#### 수행능력

- 한번의 클릭으로 3초 내 인증
- 10만개 이상의 커넥션 지원 가능
- 수평적인 스케일 아웃

#### 편리성

- 모바일 기기 기반 인증
- Passwordless 인증이 통합된 UX
- 모바일 및 웹 서비스

#### ROI

- 비용 절감
- 데이터 위반으로 인한 손해 감축
- 하드웨어 토큰, OTP 사용 불필요

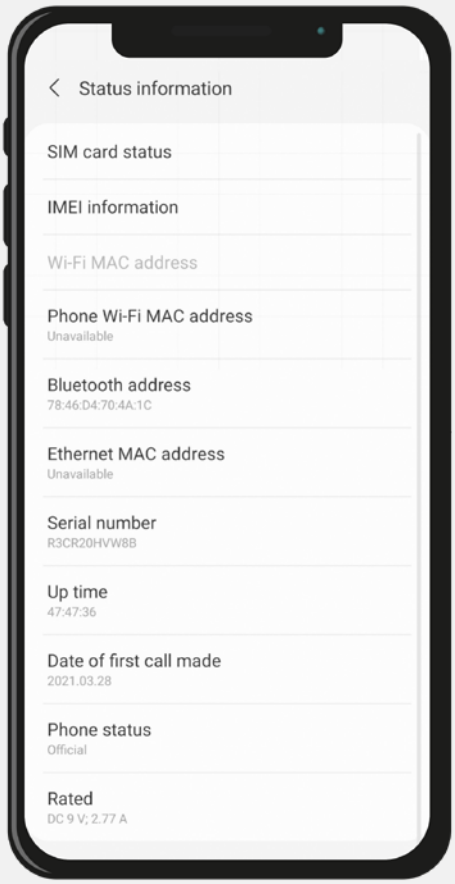
World's first core technology

# Guardian-CCS 특허기술 > MIRC, OTSK, MDV, KNChain

Multiple Identifier Random Combination (MIRC), One-Time Security Key (OTSK),
Multiple Distributed Verification (MDV), Hybrid Blockchain - Kernal Chain Core (KNChain)

## 01 모바일 기기 : 인증장치 주요 소스

## 02 사용자 모바일 기기에서 고유 식별자를 추출




**Mobile number**
010-1234-5678

**Sound sensor**
15 | 11 | 0 | 0 | 0 | 0 | 4

**MAC 주소**
50:77:05:3f:81:49

**블루투스 주소**
20:00:00:00:00:00

**Wi-fi info**
FNS iptime

**Proximity sensor**
8

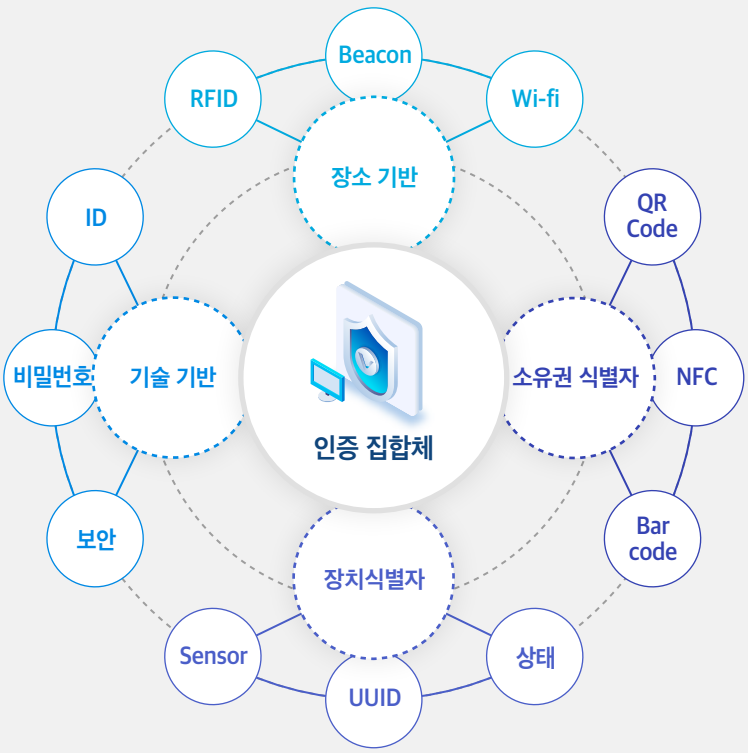
**명도 센서**
990

**지자기 센서**
13|52|-39

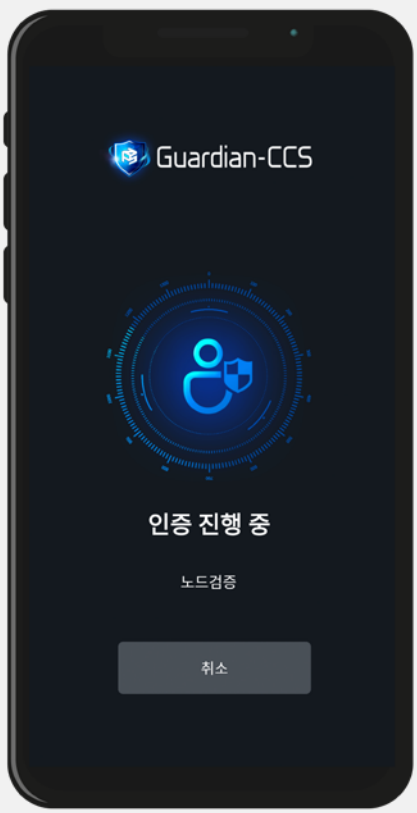
**디바이스 고유번호**
00000000-7849-0649-f202-3db11c503a2e

[ 특허번호 10-1809976 ] 다중 사용자 요소와 그 방식을 결합한 인증키를 발급하는 보안 인증 시스템

## 03 공간 제약없는 식별자 에코 시스템, 소유권 식별자, 장치 식별자, 지식기반 정보의 결합




## 04 해킹 불가능한 Passwordless 인증




특정 사용자 기기로 확인 및 인증

Guardian-CCS

# Product & Service

온클라우드 On-Cloud

온클릭 On-Click

온프리미스 On-Premise

부가가치 서비스 VAS

컨설팅 서비스 Consulting Services

## On-Cloud

온클라우드

- TM ONE 알파 클라우드가 주관하는 Passwordless 블록체인 보안 인증 플랫폼
- 공공고객 및 개인고객을 위한 온클라우드 Saas 제공
- SLA/SLG를 통한 총체적 관리 서비스
- 유저당 라이센스 연간 구독 방식
- 웹/모바일 앱, 클라우드 앱, 화이트 라벨 앱 로그인 서비스
- API와 SDK, 관리자 포털 포함
- 약관 및 조건 적용

## On-Click

온클릭

- TM ONE 알파 클라우드가 주관하는 Passwordless 블록체인 보안 인증 플랫폼
- 공공고객 및 개인고객을 위한 온클라우드 SaaS 제공
- SLA/SLG를 통한 총체적 관리 서비스
- 클릭당 라이센스 기반 연간 구독 방식
- 웹/모바일 앱, 클라우드 앱, 화이트 라벨 앱 로그인 서비스
- API와 SDK, 관리자 포털 포함
- 약관 및 조건 적용

## On-Premise

온프리미스

- 고객 사이트에서 온프리미스를 주관하는 Passwordless 블록체인 보안 인증 플랫폼
- 웹/모바일 앱 사용자를 위한 온프리미스 SaaS 제공
- SLA/SLG를 통한 총체적 관리 서비스
- 사이트 라이센스당 일회성 G-CCS을 부여, 앱 무제한 사용하는 방식
- 클릭/유저당 라이선스 기반 연간 구독 방식
- 웹/모바일 앱, 클라우드 앱, 화이트 라벨 앱 로그인 서비스
- API와 SDK, 관리자 포털 포함
- 약관 및 조건 적용

## Value Added Service

부가가치 서비스(VAS)

- G-CCS 보안 인증 게이트웨이 (SAG)
- G-CCS SSL VPN & SD WAN
- G-CCS eKYC
- G-CCS TM ODS
- G-CCS eKYC & TM ODS
- G-CCS CSP MFA (Google, AWS, Microsoft)
- G-CCS SME
- G-CCS FinTech & BFSI
- G-CCS Wholesale Services (PaaS, SaaS)
- 약관 및 조건 적용

## Consulting Services

컨설팅 서비스

- 프로젝트 관리 서비스
- 시스템 통합 서비스
- 배포 및 서비스 제공
- API 개발 & 고객맞춤형 서비스
- SDK & Plugins 개발 & 고객맞춤형 서비스
- 기획, 개발, 고객맞춤화, 테스팅, 배포 및 RFS
- 교육 & 인증
- 사후 관리, 유지보수 서비스(L1, L2, L3)
- 약관 및 조건 적용

Guardian-CCS

# Case of Use

01 공공 및 개인 고객의 사용자 경험

02 단일 보안인증 서비스

03 2FA 보안 인증 게이트웨이 (SAG)

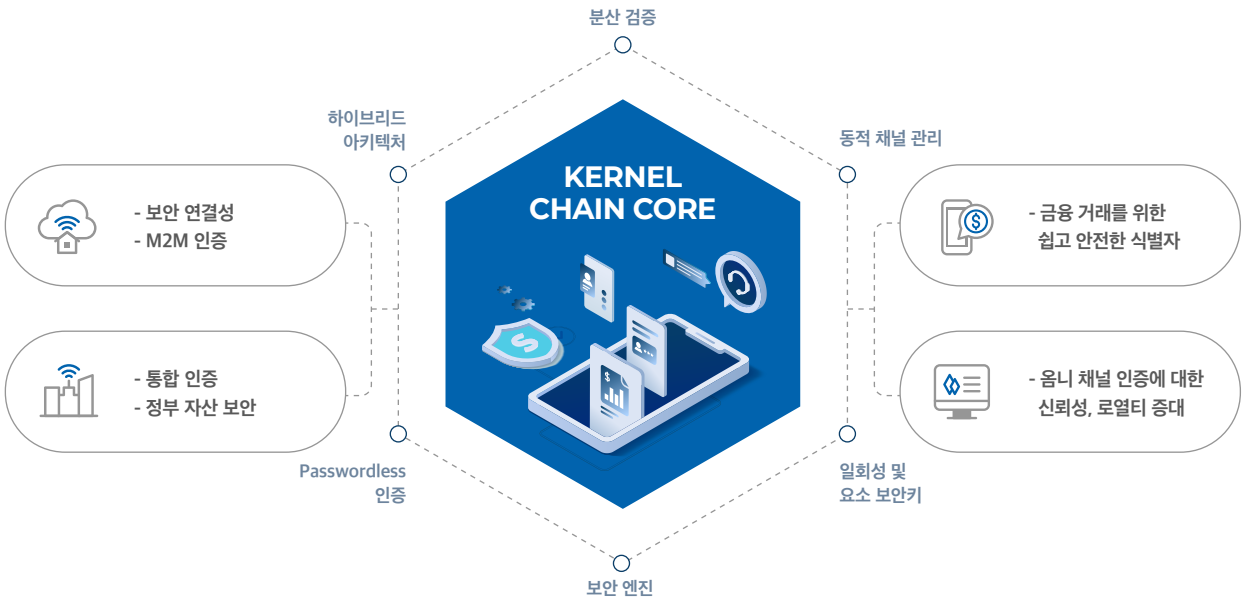
04 금융 서비스

05 SDWAN/SSL VPN 2FA

06 eKYC를 통한 사용자/고객 온보딩 및 인증 원활

### Guardian-CCS Case of Use 1.

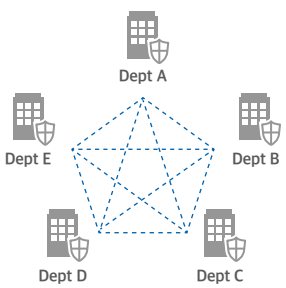
## 공공 및 개인 고객의 **사용자 경험**




### Guardian-CCS Case of Use 2.

## **단일 보안인증** 서비스

**과거 [ID & Password]**




ID/비밀번호 관리가 어렵고 높은 비용이 부과되는 반면, 보안성 · 생산성 · 효율성은 비교적 낮음. 서비스 제공자와 사용자의 수가 증가함에 따라 인증 상호운용성의 복잡성 역시 가중됨.

**Challenges**

**목표**

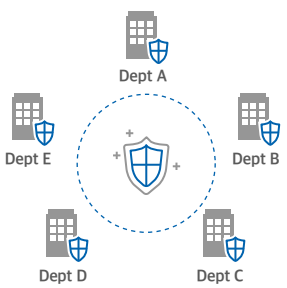
사용자, 장치, 앱 간의 상호 신뢰성 구축.
기업 규모의 인증 솔루션을 통해
공통적인 상호운용을 실현

**가치**

**사용자 가치**
고객사 및 사용자에 신원 인증을 제공.
기밀 보안과 민감한 데이터 보호

**기관 가치**
운영 비용 절감 및 인증 수용성 향상.
기관 내외부에서 사용자의 생산성 증가

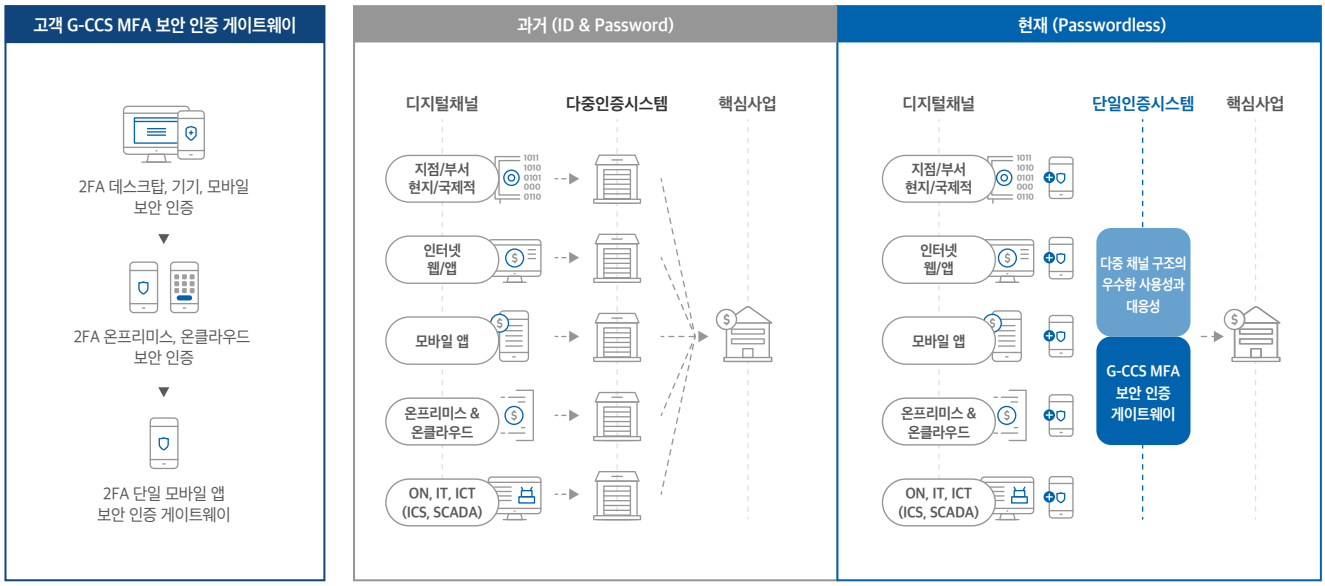
**미래 [Passwordless]**




G-CCS MFA 인증 서비스는 보안 신원 인증 게이트웨이의 역할을 수행하며, 사용자와 기기 접근 권한에 대한 보안 규제의 상호운용성 표준화를 단순화 및 단일화함.

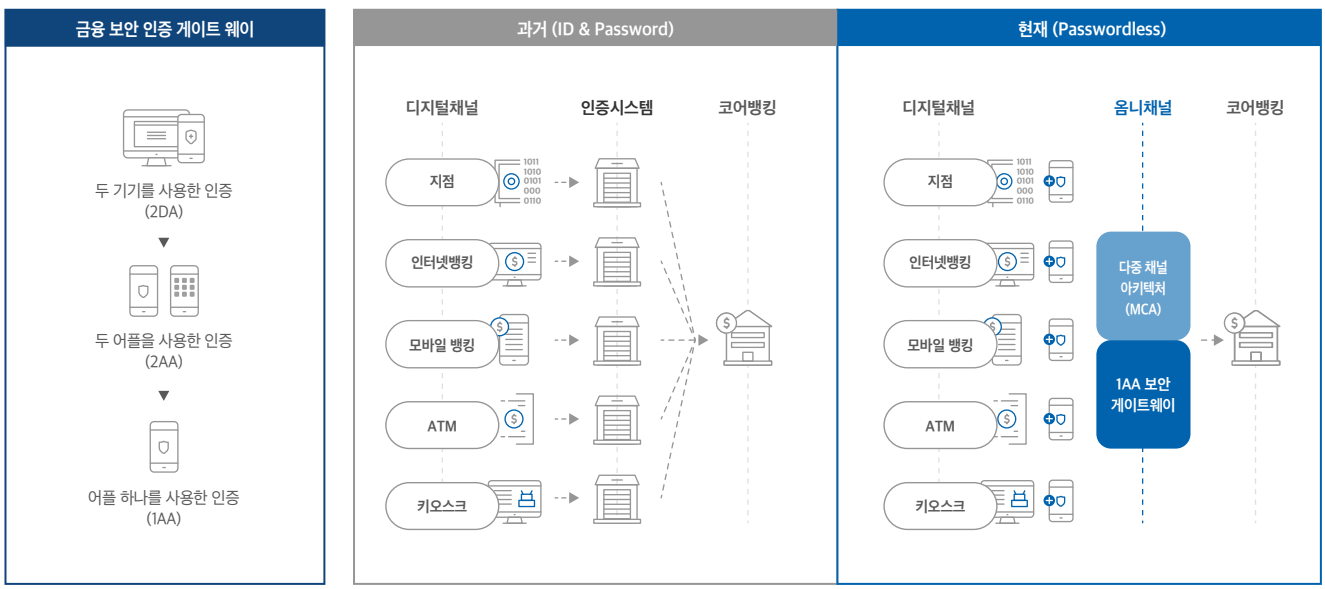
## Guardian-CCS Case of Use 3.

# 2FA 보안 인증 게이트웨이 (SAG)



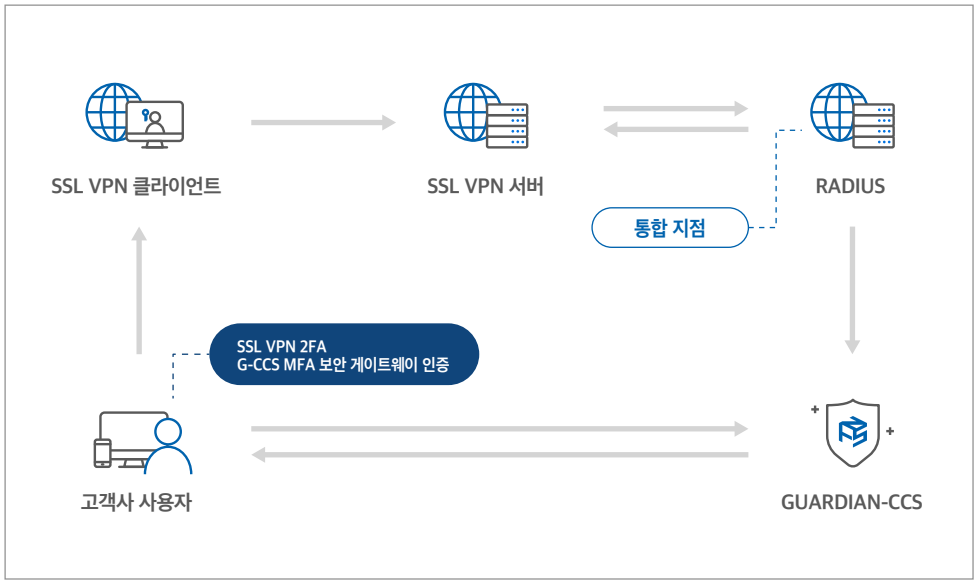

## Guardian-CCS Case of Use 4.

# 금융 서비스



Guardian-CCS Case of Use 5.

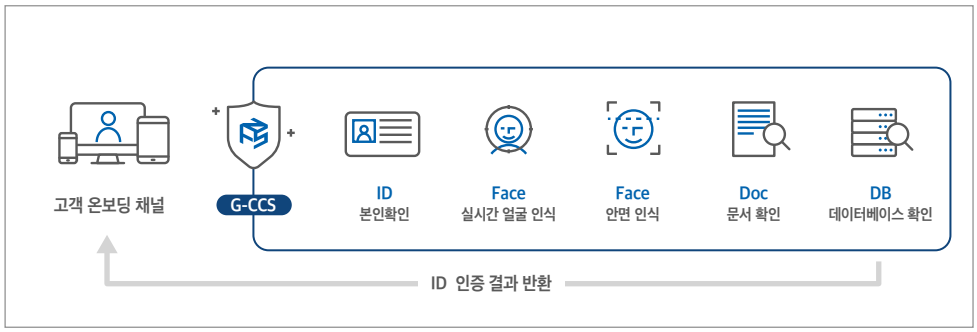
# SDWAN/SSL VPN 2FA




신뢰 할 수 있는 고객사 사용자 인증과 네트워크 보안 강화를 위한 SSL VPN 과의 통합을 제공하며 다양한 GCCS-MFA 인증을 사용하여 엄격한 보안 요구 사항을 충족 시킵니다.

Guardian-CCS Case of Use 6.

# eKYC를 통한 **사용자/고객 온보딩 및 인증 원활**




사용자의 사용 경험인 G-CCS MFA 및 eKYC는 신분증 캡쳐와 얼굴 인증, 다단계 인증(MFA), 거래 후 신원 문서 확인 등과 같은 엄격한 신분 확인 요구사항을 충족합니다.

**1. G-CCS MFA** 최초 사용자 온보딩 및 로그인을 위한 MFA를 통해 Passwordless 블록체인 사용자 인증.

**2. OkayID** OCR을 사용하여 자동적으로 신상 정보, 얼굴 사진, 이미지를 신분증에서 추출

**3. OkayFace** 얼굴 스푸핑을 방지하는 API를 통해 원격 또는 비대면 거래에서 실제 얼굴이 존재하는지 확인. 1:1 얼굴 인증을 통해 신분증 사진으로 실제 얼굴 확인

**4. OkayDoc** 시각적 컴플라이언스와 보안 기능 및 콘텐츠 템퍼링 감지법을 통하여 AI 기반 신원 문서 이미지 확인 및 인증

**5. OkayDB** 원격상에서 존재하는 신분증의 식별 및 확인을 강화하는데 도움이 되는 국가별 데이터

Customer value : Next genaration

# Guardian-CCS의 고객가치 **차세대 Passwordless MFA**

**01**

말레이시아 정부에서 검증된 클라우드 서비스 제공 업체인 TM ONE Cloud에 의해 주관되고 있습니다. 또한, 현지 고객들의 요구를 반영하기 위하여 온프리미스 고객맞춤형 솔루션을 제공합니다.

**02**

거래는 SLA/SLG를 통해 3초 이내에 완료되며, 인증에 침투하기란 거의 불가능합니다.

**03**

온클라우드와 온프리미스 솔루션은 PDPA, RMiT 등의 정부 규제사항에 전제하여 전체 데이터의 저장소와 통제 권한을 보증합니다.

**04**

Guardian-CCS는 "Passwordless" 블록체인 보안 인증을 통하여 개인 및 단체를 사이버 범죄로부터 보호하고, 세계를 더 안전한 곳을 변화시키는 데에 기여합니다.

**05**

Google, Microsoft, Alibaba, AWS, FIDO2, HPR, DUO 등과 같은 클라우드 기반 인증 공급자 및 IAM, eKYC, SSL VPN, EDR 등과 같은 기타 솔루션 공급자와 협력합니다.

**06**

현재, Guardian-CCS의 기술은 유일무이하며 'Passwordless 인증 솔루션' 블루오션에서 독보적인 행보를 이어가고 있습니다. Google Authenticators, DUO, HPR, FIDO2, Samsung, Microsoft 등의 인증 업체가 있기는 하지만 다른 기술과 서비스 플랫폼을 제공한다는 측면에서 대체재로 보기는 어렵습니다.

Realizing security, reliability and privacy

# 보안성, 신뢰성, 프라이버시를 실현하는 **Passwordless Guardian-CCS**


Sale value proposition

# Guardian-CCS의 **판매 가치 제안**

**편리성**

- Passwordless 원스톱 인증 경험
- 사용자/고객을 위한 편리한 설치 및 경험
- 3초 내의 완료되는 초고속 인증(SLA/SLG)
- 사용자 친화적 & 신뢰적 서비스
- 감사 기록을 위해 사용자 및 관리자의 사용내용 기록
- 빠른 사용자 온보딩과 사용 종료 관리 용이

**보안**

- 해커의 침투나 내부적 위협 없음
- 분산 블록체인 다단계 검증 알고리즘
- 블록체인 채널, 차단 및 노드 개체로 일회성 보안 키 생성(OTSK)
- OTSK는 일회성, 실시간 사용으로 해킹방지를 100% 보장
- CCRA Certification EAL2 (2022)
- 취약점 없음

**신뢰증명**

- Zero trust 하이브리드 아키텍처 바탕의 안전성 높은 설계
- 최소한의 비민감성 데이터만 저장하여 프라이버시가 보호 되도록 설계
- 블록체인의 탈중앙화, 분산적 인증과 합의 인증
- BNM RMiT, MCMC INS, PDPA, GPDR 컴플라이언스 표준 충족

**비용절감**

- 온클라우드 및 온클릭 관리 서비스는 선결제 수수료 없음
- 사용자 라이선스 및 사용 기반 요금 부과, 대량 할인
- 검증된 ROI & VOI를 활용해 최대 70%까지 운영비용 절감 가능
- 서비스 이용을 위한 추가적인 장치 불필요
- 통합 및 SDK를 위한 표준 REST API 제공
- MFA 추가 비용 없음

## Value matrix

# Guardian-CCS : 양·질적 가치 매트릭스

### Guardian-CCS MFA 특징

- 안드로이드와 iOS에 간단하고 직관적인 설치
- Passwordless 원스톱 인증 경험
- 추가 기기 불필요(BYOD)
- 생체인식, 패턴, PIN, OTP 등의 추가 인증 장치
- 모바일 앱 및 서버 해킹시도로 부터 자유로움
- 취약점 일체 없음
- REST API로 다른 인증매체와 통합
- 모바일앱, 서버, 관리자 종단간 서비스
- 온프리미스 선결제 금액 최소화. 사용자와 사용량 기반 요금 부과 모델
- 검증된 ROI와 VOI
- 레거시 시스템과 클라우드 서비스로 통합하는 표준 REST API 제공
- 최소한의 서버 스펙을 사용하여 추가 장치 불필요
- 블록체인 노드에 최소한의 사용자 데이터만 저장
- IdP, eKYC, 3rd Party MFA 등으로 동의 관리 시스템 통합
- 민감한 프라이버시 데이터를 저장하지 않도록 기획
- 사용자 정보 공유를 위한 대안 옵션 제공
- 즉석에서 스케일아웃 기능 제공
- 만 개의 연결망을 3초 내에 처리
- 오차확률 0.1% 미만
- HA 및 DR 전략 제공

### 양적 가치

- 고용 생산성 : 연평균 약 520만 USD 향상
- 고객유지율(CRR): 최대 25% 증가
- 콜센터 운영비: 최대 60% 절감
- 데이터 위반 손실: 1120만 USD 감소
- 사용자 생산성: 연간 319.5 USD
- 추가 장치 비용: 연간 45USD 절감

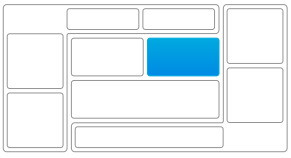
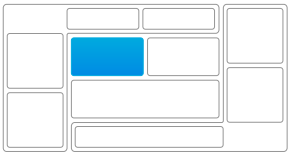
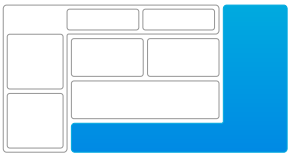
### 질적 가치

- 보안 플랫폼과 빠르고 편리한 서비스로 사용자/고객 효용 증대
- 서비스 제공에 따른 높은 수준의 신뢰와 보안성 획득
- 개인 기기로 인증에 대한 높은 사용자 친화적, 편리성, 신뢰

업계 최초 고객사이나 최종 사용자가 계정에 접근하고,
프라이버시를 보호하는 데에 있어 높은 수준의 보안성과 신속성,
편리성을 보장합니다.

Satisfying customer needs

# Guardian-CCS : 고객 요구 만족

| G-CCS 핵심 가치 | 고객 주요 요구사항 | G-CCS 주요 사항 |
|---|---|---|
| 사용자 경험  | 솔루션 설치와 구동 난이도<br>솔루션에 대한 사용자의 적응 용의성<br>시공간적 접근 및 이용 편의성<br>사용자 선호에 따른 인증방법 선택권 | 안드로이드와 iOS를 간단하고 직관적으로 설치<br>Passwordless 원스톱 인증 경험<br>추가 기기 불필요(BYOD)<br>추가 인증 : 생체인식, 패턴, PIN, OTP |
| 보안  | 사이버 공격 대응력<br>예상되는 취약점<br>현 보안 기준에 대한 적합 여부<br>솔루션 완결성 | 모바일 앱 및 서버 해킹시도로 부터 자유로움<br>취약점 및 해킹 위험 일체 없음<br>REST API로 IdP, eKYC, 3rd Party MFA 등 다른 인증매체와 통합<br>모바일앱, 서버, 관리자 종단간 서비스 |
| 지속가능성  | 구현 및 유지 비용<br>실제 ROI<br>레거시 보안 시스템 통합 능력<br>환경측면의 이차효과 | 클라우드 선결제 비용 없음. 온프리미스 및 사용량 비용 최소화<br>검증된 ROI와 VOI<br>레거시 시스템과 클라우드 서비스로 통합하는 표준 REST API 제공<br>최소한의 서버 스펙을 사용하여 추가 장치 불필요 |
| 프라이버시  | 프라이버시 데이터 저장소: 중앙화 또는 분산화<br>동의 관리 특징<br>프라이버시를 강화 능력<br>데이터 공유범위에 대한 사용자의 선택권 | 블록체인 노드에 최소한의 사용자 데이터만 저장<br>동의 관리 시스템 통합<br>민감한 프라이버시 데이터를 저장하지 않도록 기획<br>사용자 정보 공유를 위한 대안 옵션 제공 |
| 확장성  | 수직적/지리적/인구통계학적 확장성<br>높은 수행능력 요구<br>인증 솔루션의 오차확률<br>연속성 및 복구 전략 | 즉각적, 미래지향적 스케일아웃 기능 제공<br>만 개의 연결망을 3초 내에 처리<br>오차확률 0.02% 미만<br>HA 아키텍처 디자인을 통한 HA 및 DR 전략 제공 |

## Frequently Asked Questions

# Guardian-CCS : **FAQ**

| 문의사항 | 답변 |
|---|---|
| G-CCS의 솔루션 설치와 구동의 난이도가 높은 편입니까? | 안드로이드와 iOS를 간단하고 직관적으로 설치할 수 있습니다. App store 나 구글 플레이 스토어에서 다운로드하여 바로 사용 가능합니다. |
| G-CCS의 솔루션을 처음 접하는 사용자가 다루기 용이합니까? | G-CCS는 Passwordless 원스톱 인증 경험과 사용자 온보딩이 잘 마련되어 있습니다. 고객이 기존의 ID, 비밀번호 사용을 희망할 경우 병존적으로 사용 가능합니다. |
| G-CCS는 편리하고 접근성이 좋은 솔루션입니까? | G-CCS는 기존 기기로 사용할 수 있도록 개발되어, 추가적으로 기기가 필요하지 않습니다. |
| 사용자가 2FA나 인증 요소를 선택할 수 있습니까? | 기기와 사용자 프로필을 사용하는 1단계 인증 뿐만 아니라 추가 인증 요소(2FA/MFA), 얼굴인식 혹은 지문 등의 생체인증이나 패턴, icon, OTP(이메일, SMS)가 있습니다. |
| 사이버 공격에 대응할 수 있는 해결방안이 있습니까? | 해커나 내부 위협으로 부터 안전을 보장합니다. 모바일 앱이나 서버에 침투 시도가 있더라도 해킹할 결정적인 데이터를 저장시키지 않기 때문입니다. |
| 차후의 취약점에 대한 보안 방안이 있습니까? | 솔루션은 취약점없이 개발되었습니다. |
| 솔루션은 현재의 보안 기준에 의거하여 개발되었습니까? | 한국 정부로 부터 소프트웨어 품질관련 인증을 받았으며, 2021년 CSM이 주관 ISO 15408 Common Criteria certification 를 수료하였습니다. |
| 완성도가 높은 솔루션입니까? | API와 SDK 가 제공되며 온클라우드, 온클릭, 온프리미스 솔루션 관리자, 모바일 앱, 서버에서 E2E 관리 보안 서비스를 갖추고 있습니다. |
| 구동과 유지 비용은 어떻게 됩니까? | 선결제 비용이 부과되지 않습니다. 요금은 사용자 라이선스 혹은 클릭당 요금을 부과하는 방식으로 책정됩니다 |
| 투자수익은 어느 정도로 예상하십니까? | 사용 사례와 Passwordless를 토대로 ROI/VOI가 최대 70%까지 절약될 것으로 예상합니다. |
| 레거시 보안 시스템의 통합능력은 어떻습니까? | 레거시 시스템과 3rd party 인증서를 통합한 표준 REST API를 제공합니다 . |
| 솔루션이 환경에 미치는 영향은 긍정적입니까? | 최소한의 서버 스펙을 사용하고 사용자 온보딩도 단시간에 가능하기 때문에 추가적인 장비가 필요하지 않습니다. |
| 데이터 저장소 보호는 중앙화와 분산화 방식 중 어느 방식으로 진행됩니까? | 인증, 확인 및 유효성 검사를 위해 서버와 사용자 장치에 저장되어 있는 최소 데이터는 노드/모바일에 분산되기전에 해시 및 암호화됩니다. |
| 사용자 동의와 동의 관리를 제공합니까? | 앱을 사용하고 이메일 주소, 휴대폰 번호와 같은 최소한의 사용자 정보를 입력하려면 사용자 동의가 필요합니다. 솔루션은 동의 관리 시스템과 GDPR, PDPA 2010 가이드라인에 따라 설계되었습니다. |
| 프라이버시 강화하기 위한 방안이 마련되어 있습니까? | 솔루션은 민감한 프라이버시 데이터를 저장하지 않도록 GDPR, PDPA 조건에 기반해 고안되어 프라이버시 측면의 안전성이 높습니다. |
| 데이터 공유 범위는 사용자가 선택권이 있습니까? | 데이터 공유 범위에 대한 선택권은 사용자가 앱을 등록할 때 직접 설정합니다. 솔루션은 사용자 정보 공유에 대한 대안 옵션을 제시합니다. 2FA나 MFA는 데이터를 중앙관리자에 저장하지 않고, 모바일 기기에 한해 이용합니다. |
| 수직적, 지리적, 인구통계적 측면에서 확장성이 보장됩니까? | 솔루션 기능은 온클라우드/온클릭을 위한 HA, 전체 이중화, DR/백업 용량으로 즉시 확장 가능합니다. 온프리미스의 경우, 기준 HW 스펙은 동시에 최대 10,000개의 커넥션/세션을 수용할 수 있도록 설계되었습니다. |
| 솔루션의 수행능력에 대한 평가는 어떻습니까? | SLA는 만 개 넘는 커넥션/ 세션을 3초 이내에 처리합니다. |
| 인증 솔루션의 오차 범위는 어떻습니까? | SLA는 0.1%의 오차 범위 미만입니다. |
| 솔루션이 DR, 업무 연속성과 복구 방안을 제공합니까? | 온클라우드와 온클릭 관리 서비스에 대한 SLA은 DR과 복제 서비스를 포함합니다. 온프리미스 경우 솔루션에 프로덕션 및 DR 사이트에 대해 2개의 G-CCS 현장 라이선스가 필요합니다. |

## VALUE USP/UVP

사용자 경험 (Value)

사용자 경험 (Value)

사용자 경험 (Value)

사용자 경험 (Value)

보안 (Value)

보안 (Value)

보안 (Value)

보안 (Value)

지속유지성 (Value)

지속유지성 (Value)

지속유지성 (Value)

지속유지성 (Value)

프라이버시 (USP/UVP)

프라이버시 (USP/UVP)

프라이버시 (USP/UVP)

프라이버시 (USP/UVP)

확장성 (USP/UVP)

확장성 (USP/UVP)

확장성 (USP/UVP)

확장성 (USP/UVP)

CIAM solution

# Guardian-CCS : 정확한 고객 신원 및 접속 관리 (CIAM) 솔루션

## 01
### 신용 & Passwordless

모바일 폰은 사용자가 가장 신뢰하는 기기입니다. G-CCS 인증 서비스에 가입한 여러 사용자가 서비스를 이용하는 데에 있어 모바일 폰은 단 한대만 있어도 충분합니다. 사용자, 고객, 협력업체가 새로운 로그인 비밀번호 전체를 새로 생성하는 것이 아니라 기존의 모바일 폰 정보를 재사용할 수 있기 때문입니다.

## 02
### 데이터 투명성

사용자가 고유 ID를 가진 하나의 기기로 다수의 비즈니스 앱과 조직 시스템을 사용하므로, G-CCS는 데이터 사용과 접근성을 검토하기에 더욱 효과적인 방법입니다. 프라이버시 규정과 국제 기준을 준수하는 G-CCS 는 사용자 프로필 업데이트나 기록 삭제 측면에서 우수성을 자랑합니다.

## 03
### 감사 추적 및 과학수사

기기내에 고유 ID별로 사용 로그가 남기 때문에 규정 준수 보고, 감사 추적, 과학수사 등에서도 유리합니다. 부가적으로 이로 인해 규정 준수 보고 활동이 간소화되는 장점도 있습니다.

## 04
### 특화된 보안성

Guardian-CCS는 블록체인을 활용한 차세대 보안 인증 MFA로서의 우수성을 인정받았습니다. Guardian-CCS 는 추가적인 보안과 인증을 위해 파트너사와 고객이 자신의 ID를 eKYC, 제 3의 MFA, 전자 서명 같은 특화된 기술이나 비밀번호, 기업급 보안에 연접할 수 있도록 설정했습니다.

## 05
### 고객 경험 강화

세계적으로 가장 인정받고 효과적인 기술은 일상 생활과 비즈니스를 단순하게 만드는 기술입니다. Guardian-CCS 는 보안과 프라이버시 보호 뿐만 아니라 신속하고 편리한 사용자/고객 경험을 제공합니다. Guardian-CCS 는 블록체인, 인공지능, 머신러닝, 알고리즘에 걸쳐 다양한 기술을 지원합니다.

Go passwordless with Guardian-CCS!

# 차세대 보안 인증 솔루션 G-CCS

**01** G-CCS는 보안 액세스 인증 **MFA기반 passwordless 블록체인의 선두주자**입니다.

**02** 디지털 액세스 수명 주기 관리 전반에 걸쳐 **안전성, 프라이버시, 신뢰를 바탕으로 클라우드와 온프리미스에 설계**되었습니다.

**03** 당사 솔루션은 **차세대 Passwordless 보안 다중 요소 인증을 제공**하여 ID/비밀번호, 신용보안로 인해 생성되는 위험을 줄입니다.

**04** G-CCS는 **내외부 공격을 효과적으로 보호**하여, 정부, 금융, 금융, ICT 서비스, 기업 & SME 등 뿐만 아니라 100만명 이상의 사용자와 25개의 고객사에서 높은 신뢰를 얻고 있습니다.

**05** 디지털 환경에서 위험 부담을 현저히 줄이고 **국제 기준과 법안에 따라 고객 니즈를 만족**시킵니다.

**06** 솔루션 서비스 제공자로써 우리는 **높은 수준의 보안 절차와 다음을 포함한 정책을 철저히 준수합니다**

- ISO/IEC 27001:2013 certified Information Security Management System (2021)
- ISO/IEC 15408-1:2009 certified Common Criteria for Information Technology Security Evaluation (2022)
- SOC 2 Type 2 compliant (2023)
- PDPA, BNM RMiT, MAS TRM, PCI-DSS, HIPAA, EU GDPR 에 따른 컴플라이언스 조건 충족
- 최상급 시스템과 기술 솔루션을 포함한 네트워크, 앱, 인프라 보안
- 엄격한 절차와 정책의 물리적 보안
- 지속적인 교육과 백그라운드 점검을 통한 보안
- 지속적인 위험, 규정 준수 및 보안 평가
- SLA/SLG 로 서비스 등급 관리
- 비즈니스 연속성 관리 및 재해 복구 계획



Quality Management Certificate


Software Quality Certificate


FNSV Outstanding Award Certificate


Copyright Certificate


Main-Biz Certificate


Inno-Biz Certificate


KOIST Certificate

COMMON CRITERIA CERTIFIED

ISO 27001

AICPA SOC

fnsvalue
FEASIBLE NETWORK SYSTEM VALUE

www.fnsvalue.co.kr

[Sangam-dong, Nuri Dream Square 7th floor] 396, World Cup buk-ro, Mapo-gu, Seoul, Republic of Korea

E. fnsvalue@fnsvalue.co.kr
T. 02 - 303 - 3885
F. 02 - 304 - 3885