

Secure Authentication Solution

Guardian-CCS



About **Company**

Since its birth, FNSV supports building customised system and operation management for our customers. We are leading the next generation secure authentication market by developing our proprietary technology, 'Guardian-CCS', the simple and secured authentication solution.

CEO Jeon Seung Ju **Address** [Sangam-dong, Nuri Dream Square 7th floor] 396, World Cup buk-ro, Mapo-gu, Seoul, Republic of Korea
Established 03 Apr 2012 **Business** SI/SM, security consulting, integration system, cyber secure solution
Certification Main-BIZ, Inno-Biz, Good Software, ISO 9001, ISO 27001, Public Procurement Service



FNSVALUE

History

● 2021

appointed as an IPO of Mirae Asset Securities, and listed on KOSDAQ
contracted for PT VADS solution of Indonesia and license supply
7th Korea Excellent Company Awards, and Excellent Technology Award in Security Authentication Solution
appointed as a SW High Growth Club by MIST
appointed as a consulting business for overseas expansion by FCK
appointed as an export voucher enterprise by MSS
OIC-CERT Global Cybersecurity Award 2021
Certificate of Designation of Excellent Product-G-CCS v1.0
2021 Korea Best Companies Award, Best Technology Award
ISO/IEC 27001:2013 certification

● 2020

contracted for Telekom Malaysia (TM) solution and license supply
establishment of FNS[M], corporate company in Malaysia
a business selected by KOIPA
selected as a consulting business for overseas expansion by FCK
appointed as an export voucher enterprise by MSS

● 2019

signed MOC with Telekom Malaysia
completed global accelerating program (SG) [KISED]
ISO 9001 QM certificate
a simple and security authentication solution, [Guardian-CCS v1.0] GS certificate
obtained Main-Biz
registered Hong Leong Bank Vendor of Malaysia
completed fintech security consulting [FSI]

● ~2018

certified as a family-friendly company by the MOGEF
got POC by Malaysian Defense and completed
obtained Inno-Biz

● 2012

establishment of FNSV

Next Generation Secure Authentication Solution

PASSWORDLESS Guardian-CCS



FAST



EASY



SAFE

A Secure, Fast, Convenient and Trusted Solution in the Digital World

01. Guardian-CCS is the world-class secure authentication solution with high confidence.
02. Guardian-CCS transforms the world a safer place with passwordless blockchain secure authentication.
03. Guardian-CCS has emerged as a technology that leads digital transformation with its excellent security, speed and convenience in account access and authentication.
04. Guardian-CCS provides the best user experience, privacy protection, security, sustainability and scalability in digital authentication services.
05. Guardian-CCS is designed for security, privacy and reliability based on Zero Trust.
06. Guardian-CCS solves the global issues about identity and password such as identity theft, phishing, ransomware, brute force and password theft.



Increase cybersecurity agility

Cybersecurity Agility of Guardian-CCS

Security

- ▶ Zero Trust Framework (ZTF)
- ▶ Active Cyber Defense (ACD)
- ▶ Defense in Depth (DID)



Privacy & Regulatory

- ▶ Local & international privacy standards and regulations
- ▶ Data & national sovereignty



User & Customer Experience

- ▶ Superfast and convenient
- ▶ Less than 3 seconds



Operation & ROI

- ▶ Simplify IT operation & user support
- ▶ Reduced cost of operations
- ▶ Increased user productivity
- ▶ Increased customer experience & satisfaction



Passwordless blockchain security

Passwordless Blockchain Security for Your Business, Customer and Supply Chain

Governance & Risk Management

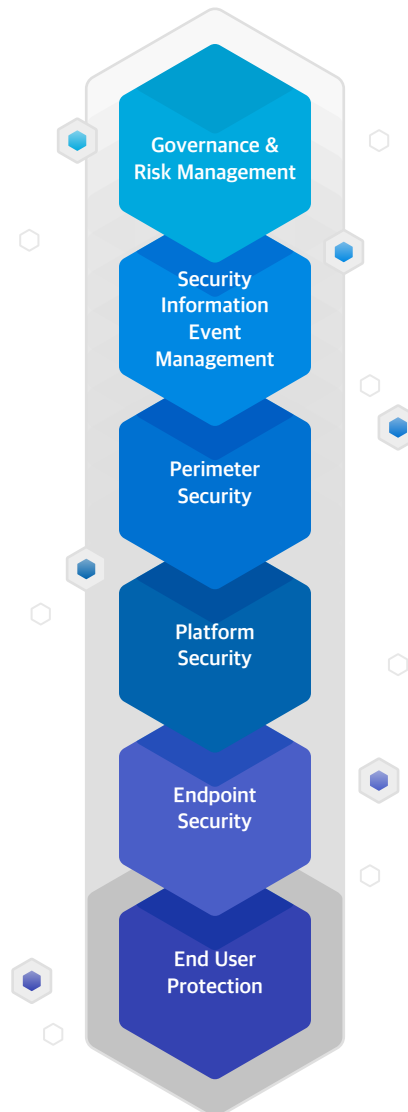
- ISO 27001 Compliant
- Center for Internet Security (CIS) Controls
- 3 Annual Pen Tests
- Privacy Shield Certified
- GDPR / CCPA Compliant
- Enterprise Risk Register
- NIST SP 800-53 Compliant
- SSAE 18 SOC 1 Type 2 Certified
- Standard Information Gathering (SIG)
- Information Security Audit Reports
- Enterprise Incident Response

Platform Security

- Next Generation Firewalls
- Antivirus for Servers
- AES 256 Encryption at REST
- Segregated Active Directory & VLANs
- Privileged Account Vaulting
- Continuous Vulnerability Scanning & Patch Management
- Secure Data Backups and Disaster Recovery
- Operating Systems Hardening

End User Protection

- Cybersecurity Awareness Training
- Multi-factor Authentication
- Role-based Access Control
- Simulated Phishing Campaigns



SIEM

- Raw Logs, Endpoint Data & Network Traffic Analytics
- Unified Log Data
- User Behavior Analytics (UBA)
- Suspicious Activity Detection & Alerts

Perimeter Security

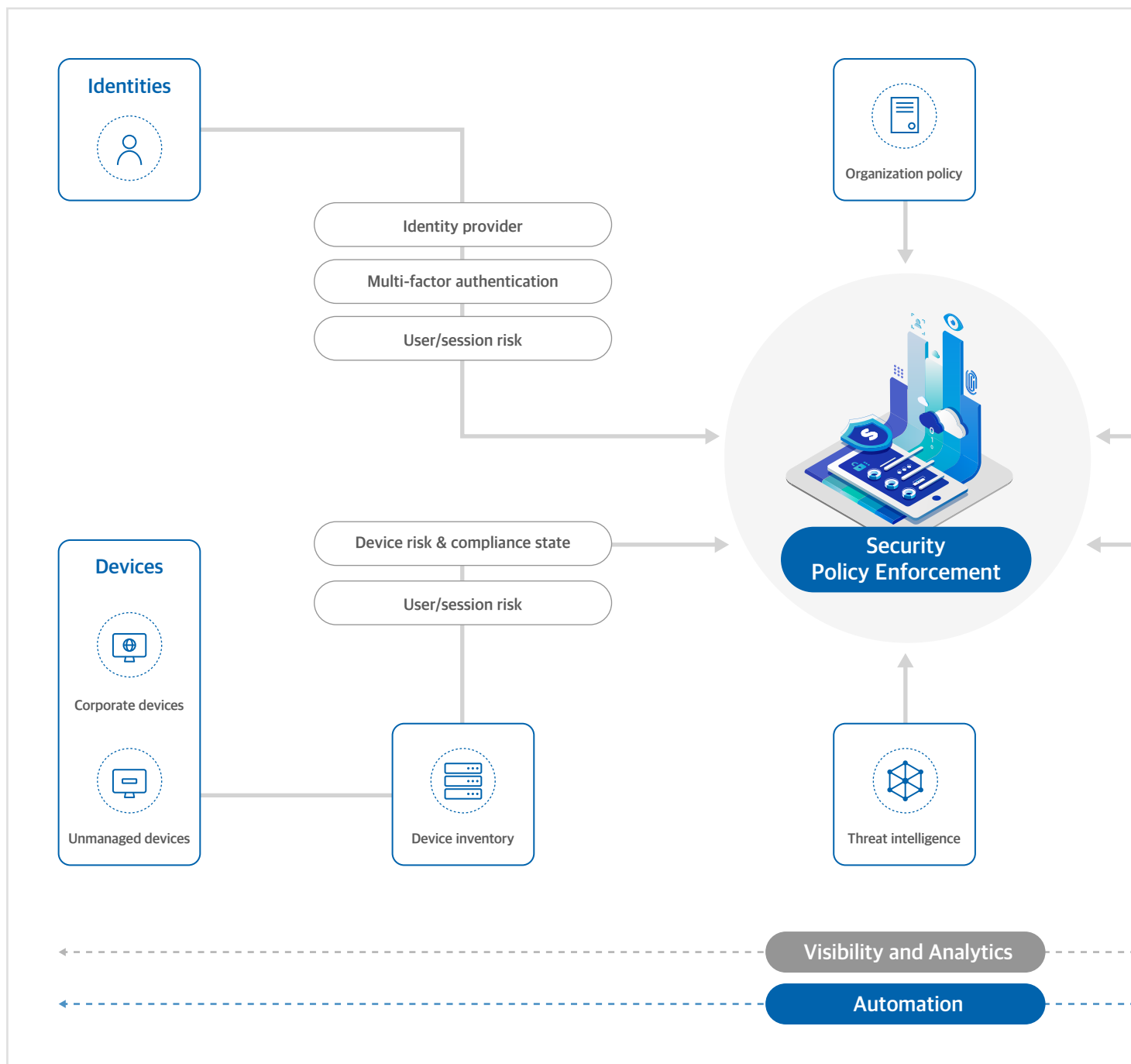
- External Firewalls
- Remote Access
- Spam Filtering
- Threat Intel Feeds
- Remote Authentication Reporting
- Brute Force and DoS Detection
- Data Center Physical Security

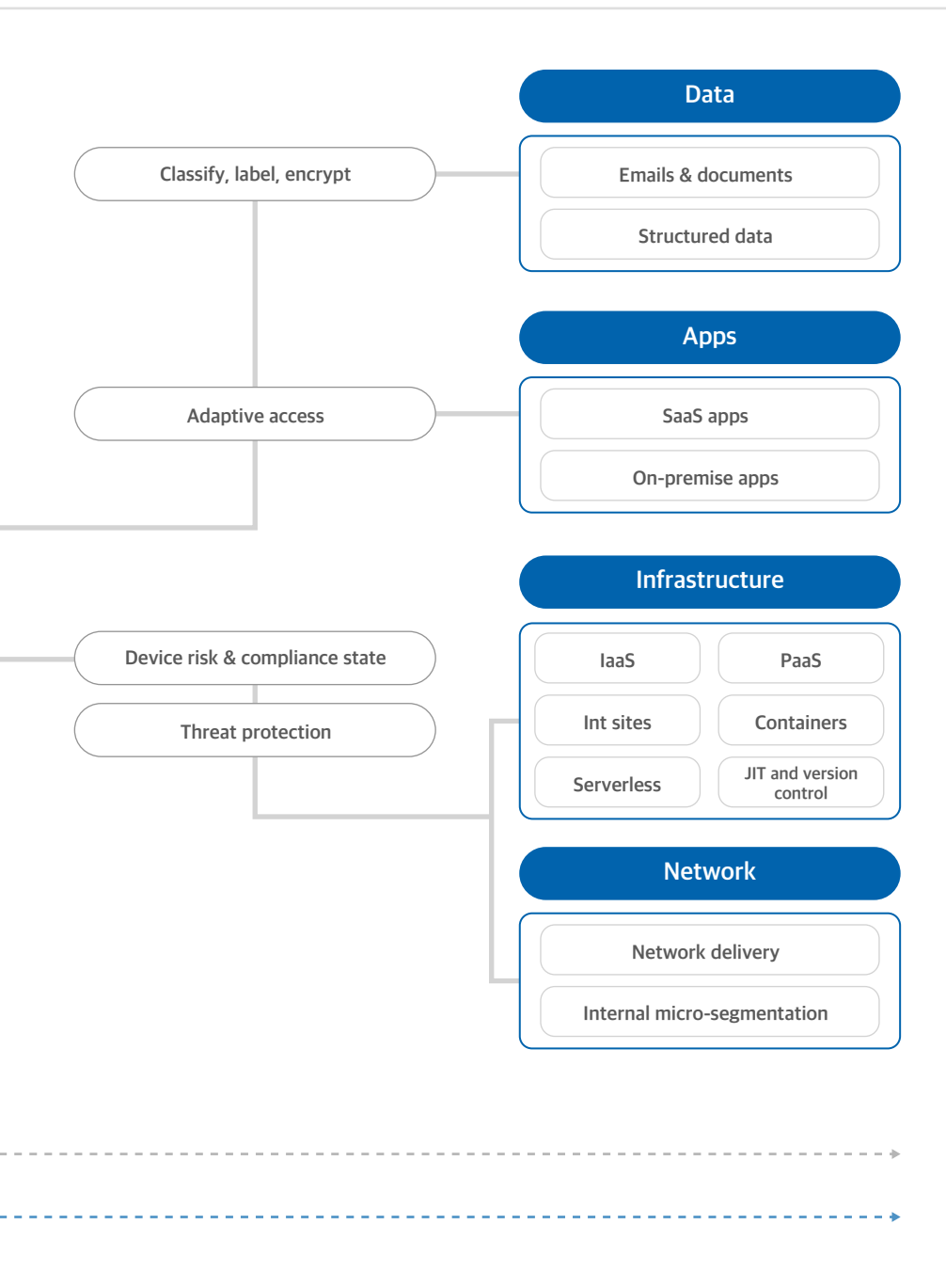
Endpoint Security

- Automated Microsoft Windows and 3rd Party Application Patch Management
- Antivirus and Endpoint Detection & Response (EDR)
- Remote Monitoring & Management System
- Local Admin Password Solution
- Full Disk Encryption
- Mobile Device Management
- Group Policy Enforcement
- Password Complexity
- Brute Force Prevention

Never trust, always verify

Zero Trust : Securing Access to Identities, Devices, Applications, Data, Infrastructure and Networks





G-CCS MFA the next generation leader

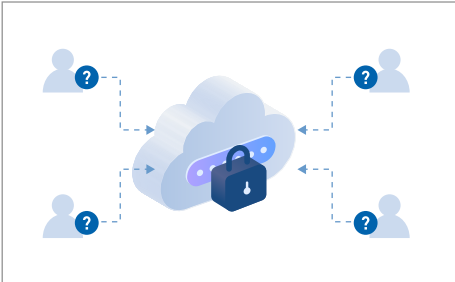
The Next Generation Passwordless **Guardian-CCS MFA**

PASSWORDS & LEGACY MFA

“80% of security breaches involve compromised passwords”

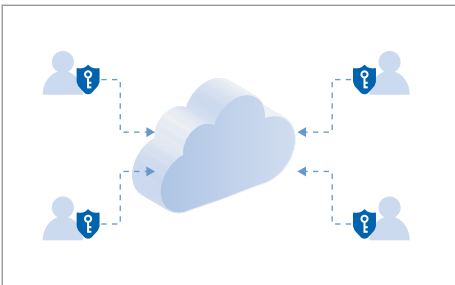
Data Breach Investigations Report, Verizon, via DBIR Interactive

- ▶ High friction login & user disruption
- ▶ Rely on passwords and shared secrets
- ▶ Susceptible to credential reuse & 2FA phishing
- ▶ Adoption gaps for customer & desktop MFA



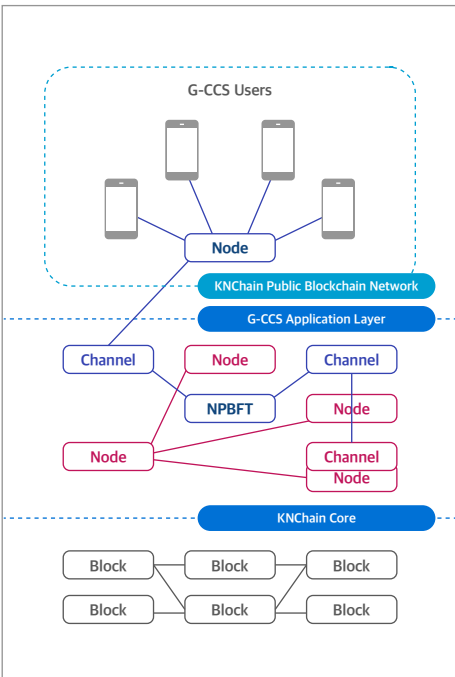
TRUE PASSWORDLESS MFA

- ▶ Provide a lightning-fast user experience
- ▶ Replace passwords with public key encryption
- ▶ Prevent credential stuffing, fraud, phishing and ransomware
- ▶ Solve customer & desktop MFA gap



TRUE PASSWORDLESS MFA

- ▶ Provide a lightning-fast user experience
- ▶ Replace passwords with blockchain OTSK
- ▶ Prevent credential stuffing, fraud, phishing and ransomware
- ▶ Solve security, customer & desktop MFA gap



Design for security, trust, privacy and UX

Guardian-CCS for **Security, Trust and Privacy**

01 User Experience

Guardian-CCS, the world's first technology, allows enterprise customers and end users to access their accounts in easy, fast and safe method with securing their privacy.

02 Security by Design

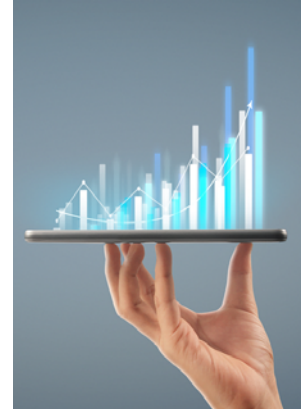
Guardian-CCS ensures high level of security with lowering level of errors of 0.02% and within 3 seconds. Its patented technologies, MIRC, OTSK, MDV and KNChain, enable hybrid blockchain verification and authentication. It completely eliminates opportunities for internal and external threats such as phishing, ransomware, ATO, credential theft and fraud.

03 Privacy by Design

Guardian-CCS is designed according to national and international data protection and privacy regulations such as PDPA 2021, GDPR, RMIT, PCI-DSS, HIPAA, etc.

04 Trust by Design

Guardian-CCS verifies device through user or device profile in authentication process. It guarantees to store necessary data only and uses them according to security regulations. It never store 2FA data that contain biometrics information like face/fingerprint in device or created by end users.



Digital service through technology

Digital Service via Security, Performance, Convenience and ROI



Security

- Multiple Distributed Verification (MDV)
- One Time Security Key (OTSK)
- Security blockchain core



Performance

- One-click authentication within 3 sec
- Support 100,000+ connections
- Horizontal scale out



Convenience

- Mobile Device based Authorization
- Passwordless authentication integrated UX
- Mobile and web services



ROI

- Save operational cost
- Prevent loss from data breach
- No need for OTP or hardware token

World's first core technology

Patented Technology, Guardian-CCS > MIRC, OTSK, MDV, KNChain

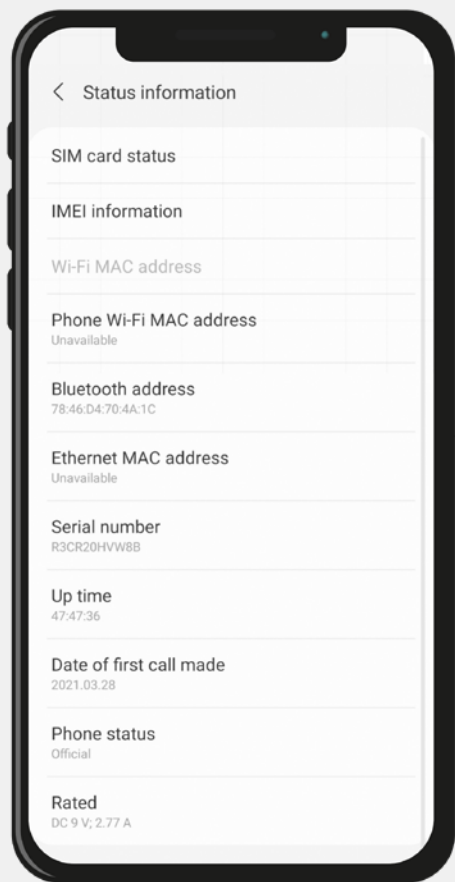
Multiple Identifier Random Combination (MIRC), One-Time Security Key (OTSK), Multiple Distributed Verification (MDV), Hybrid Blockchain - Kernal Chain Core (KNChain)

01

Mobile Device :
Major Source of Authenticator

02

Extract Multiple Unique
Identifiers from User's
Mobile Device



Mobile number
010-1234-5678

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

MAC address
50:77:05:3f:81:49

Bluetooth address
20:00:00:00:00:00

Wi-fi info
FNS iptime

Proximity sensor
8

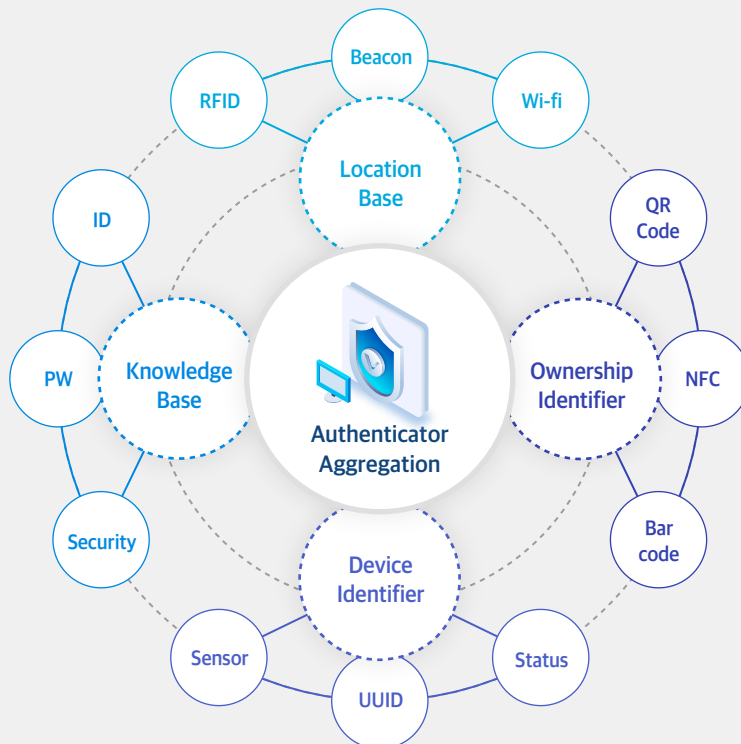
Brightness sensor
990

Terrestrial magnetism sensor
13|52|-39

Device unique No
00000000-7849-0649-f202-3db11c503a2e

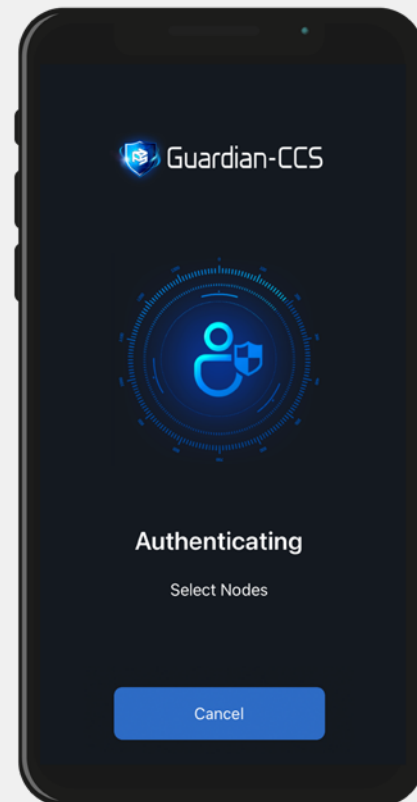
03

Combination from Identifier
Ecosystem across Location, Ownership
Identifier, Device Identifier &
Knowledge Base Information



04

Unhackable Passwordless
Authentication



Authenticate with unique user device



Guardian-CCS **Product & Service**

On-Cloud

On-Click

On-Premise

Value Added Service (VAS)

Consulting Services

On-Cloud

- ▶ Secure authentication platform hosted by TM ONE Alpha Cloud
- ▶ Provide On-Cloud Security as a Service (SaaS) for both publics & privates
- ▶ Fully managed services with SLA/SLG
- ▶ Service is on a yearly subscriptions basis based on per user license
- ▶ Service is for web/mobile app, cloud app and white label app login
- ▶ Inclusive of API and SDK, admin portal
- ▶ Apply terms and conditions



On-Click

- ▶ Secure authentication platform hosted by TM ONE Alpha Cloud
- ▶ Provide On-Cloud Security as a Service (SaaS) for both publics & privates
- ▶ Fully managed services with SLA/SLG
- ▶ Service is on a yearly subscriptions basis based on per click license
- ▶ Service is for web/mobile app, cloud app and white label app login
- ▶ application login
- ▶ Inclusive of API and SDK, admin portal
- ▶ Apply terms and conditions



On-Premise

- ▶ Secure authentication platform hosted by TM ONE Alpha Cloud
- ▶ Provide On-Premise SaaS for customer web/mobile app
- ▶ Fully customised services with SLA/SLG
- ▶ Service is on one-off G-CCS per site license with unlimited applications
- ▶ Service is on yearly subscription basis based on per user/click license
- ▶ Service is for web/mobile app, cloud app and white label app login
- ▶ application login
- ▶ Inclusive of API and SDK, admin portal
- ▶ Apply terms and conditions



Value Added Service (VAS)

- ▶ G-CCS Secure Authentication Gateway (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)
- ▶ Apply terms and conditions



Consulting Services

- ▶ Project management services
- ▶ Systems integration services
- ▶ Deployment & services delivery
- ▶ API Development & customization
- ▶ SDK & plugins development & customization
- ▶ Design, development, customisation, testing, deployment & RFS
- ▶ Training & certification
- ▶ Post implementation, maintenance & support services (L1, L2, L3)
- ▶ Apply terms and conditions

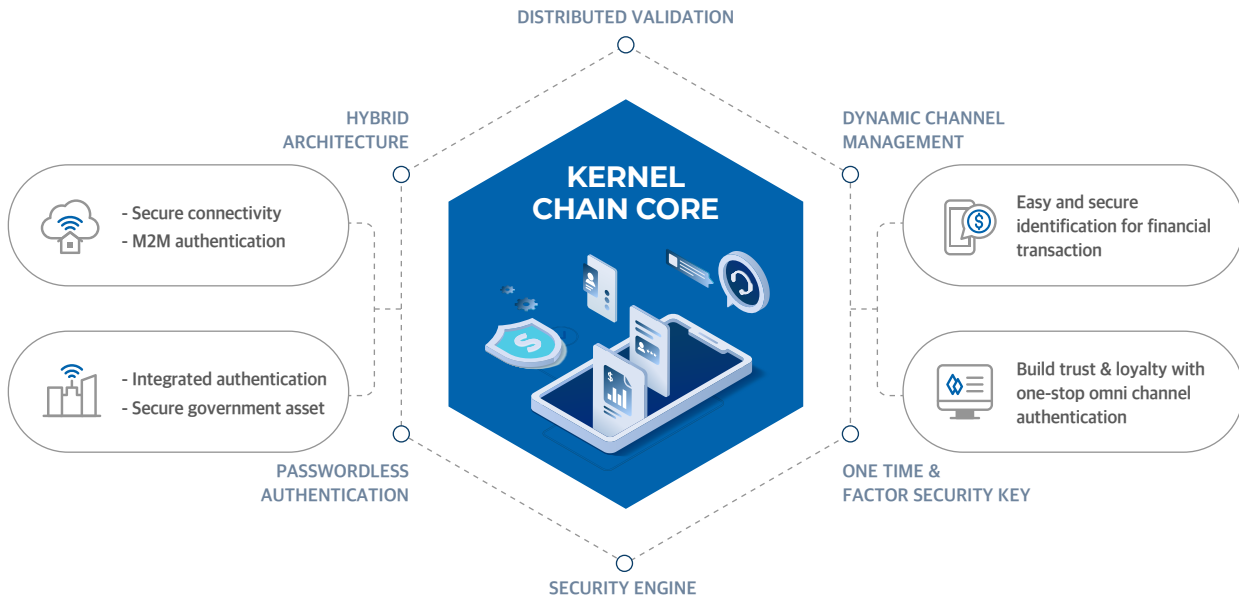


Guardian-CCS Case of Use

- 01 UX in Private & Public Sectors
- 02 Single Secure Authentication as a Service
- 03 2FA Secure Authentication Gateway (SAG)
- 04 Financial Services
- 05 SDWAN/SSL VPN 2FA
- 06 eKYC for Seamless User Onboarding

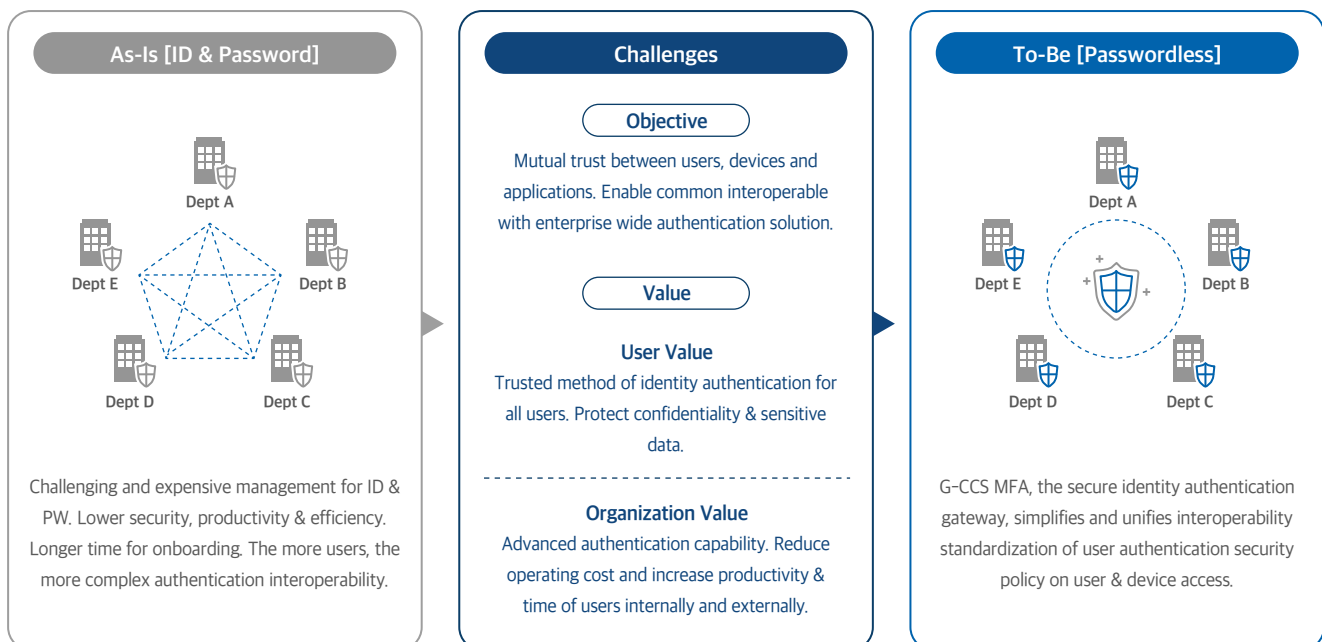
Guardian-CCS Case of Use 1.

UX in Private & Public Sectors



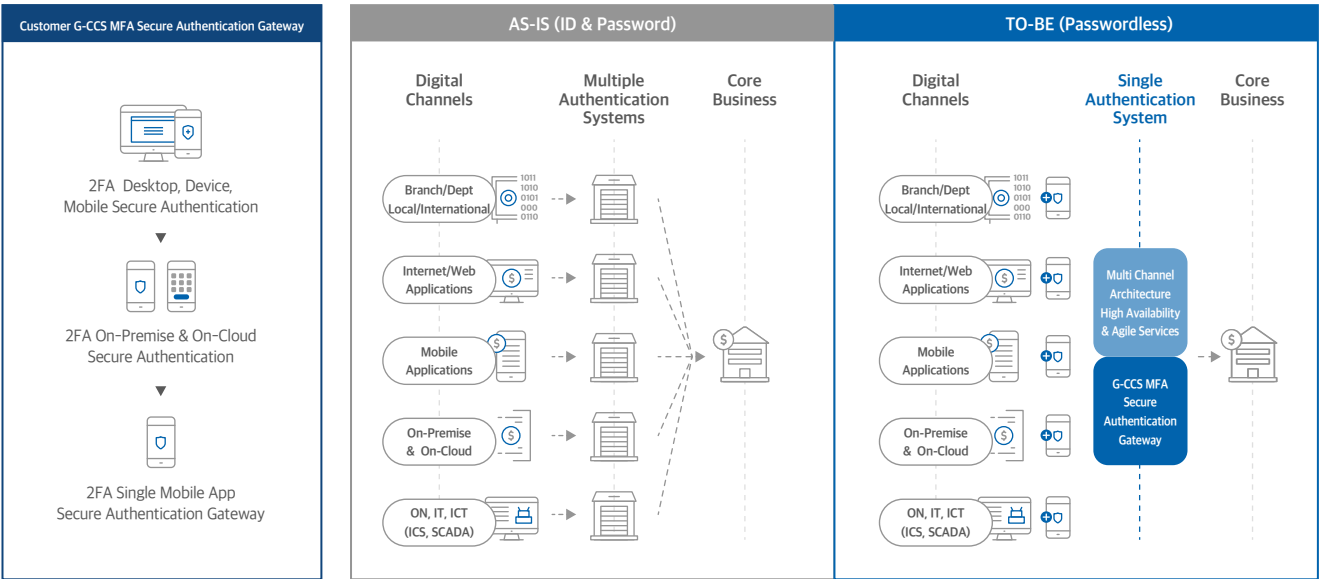
Guardian-CCS Case of Use 2.

Single Secure Authentication as a Service



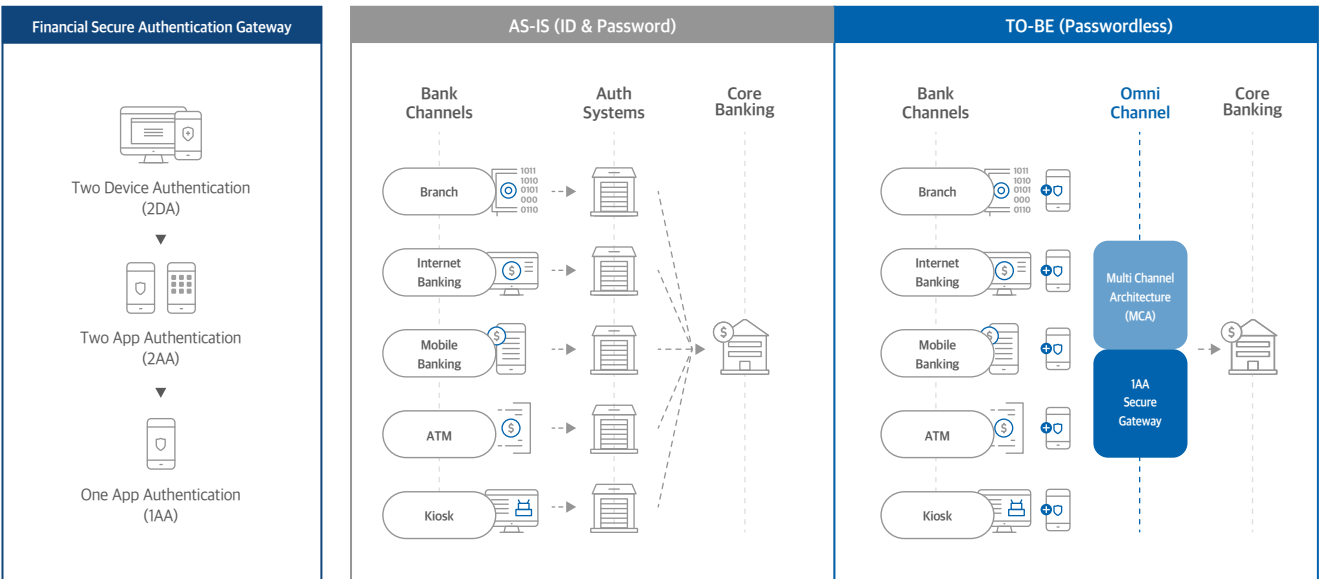
Guardian-CCS Case of Use 3.

2FA Secure Authentication Gateway (SAG)

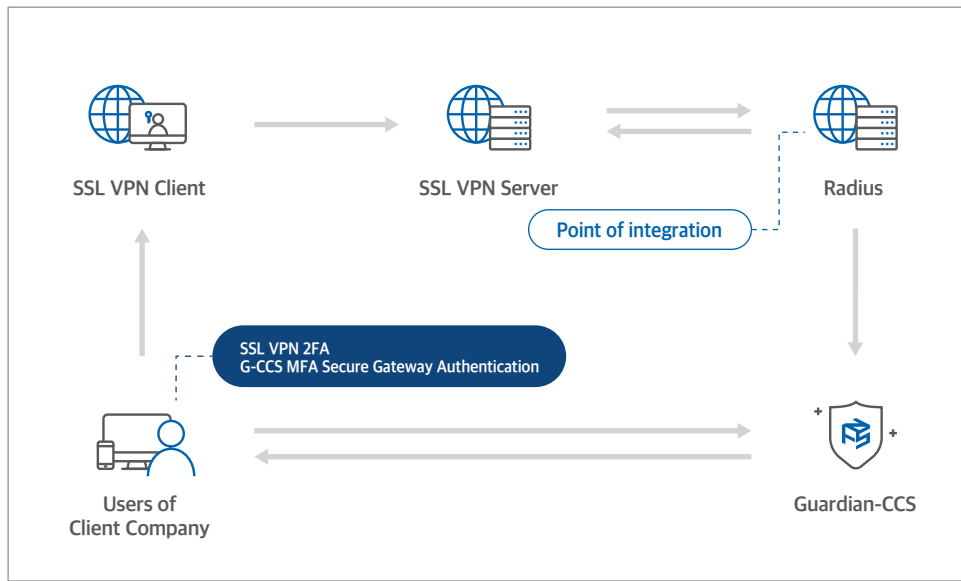


Guardian-CCS Case of Use 4.

Financial Services

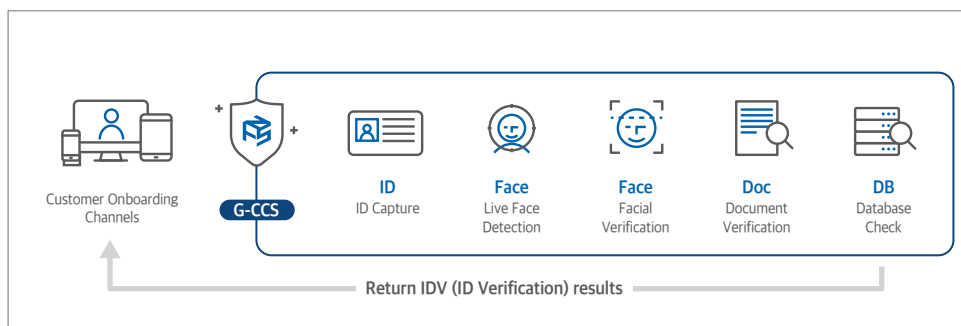


Guardian-CCS Case of Use 5.

SDWAN/SSL VPN 2FA

It offers integration with SSL VPN for better network security and trusted user authentication, and meets stringent secure requirements using various GCCS-MFA authentication methods.

Guardian-CCS Case of Use 6.

eKYC for Seamless User Onboarding

User onboarding experience G-CCS MFA & eKYC journey meets stringent ID verification requirements such as capture, facial verification, MFA & post-transaction identity document check

- 1. G-CCS MFA** Passwordless blockchain user authentication with MFA for first time user onboarding and login
- 2. OkayID** To automatically extract identity details, facial photo and image through OCR
- 3. OkayFace** Face anti-spoofing API to ensure that live face is present in remote or non-face-to-face transaction, 1:1 facial verification if live face matches ID photo
- 4. OkayDoc** AI-powered identity document image checking and authentication, through visual compliance, security feature detection and content tempering detection methods
- 5. OkayDB** Country-specific data sources to help strengthening identification and verification of a remotely-present ID

Customer value : Next generation

Customer Value of the **Next Generation Passwordless MFA**

01

We are locally hosted at TM ONE Cloud, a certified Malaysian government Cloud Services Provider. We also provide On-Premise customised solutions to meet our local customers in the region.

02

Transaction is made in 3 seconds by SLA/SLG, which is nearly impossible to be penetrated.

03

Our On-Cloud and On-Premise solutions provide assurance for full data residency, locality and sovereignty with compliance to government regulatory requirements such as PDPA, RMIT, etc.

04

We transform the world a safer place with passwordless blockchain secure authentication and G-CCS, which leads high protection for organizations and individuals from cyber criminals.

05

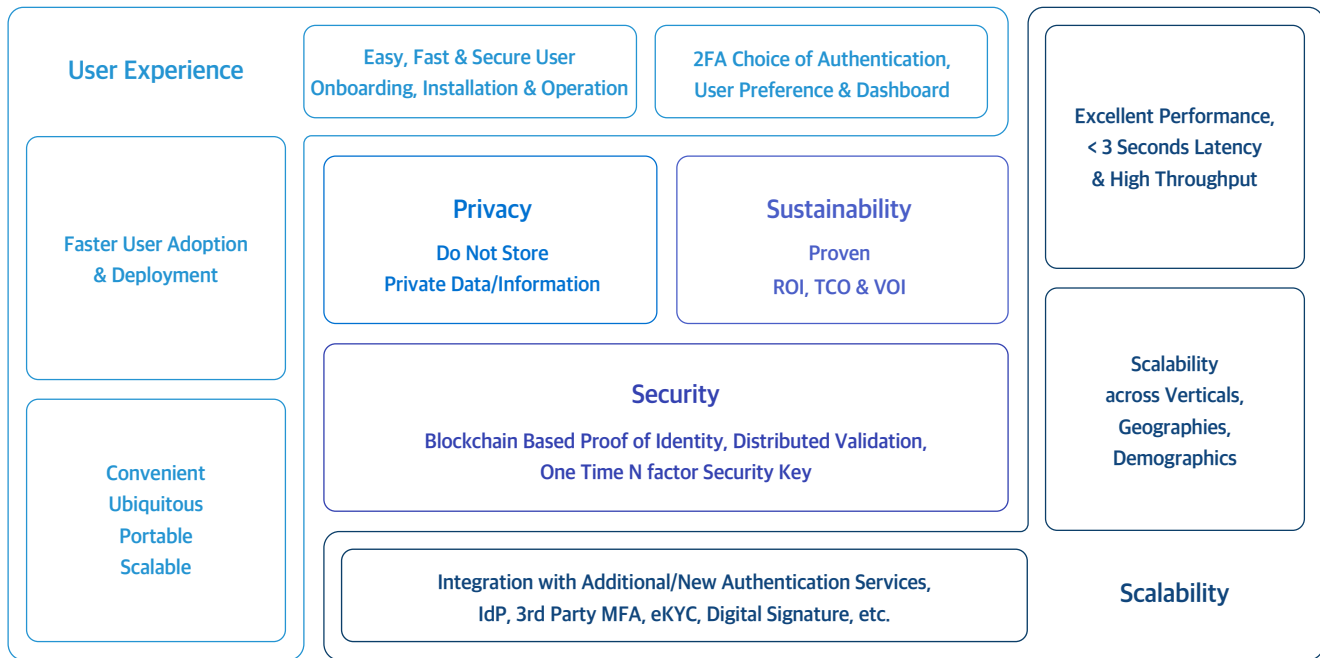
We also work with cloud-based authentication providers such as Google, Microsoft, Alibaba, AWS, FIDO2, HPR & DUO and other solution providers.

06

Currently, we do not have competitors in the authentication market but only similar technologies and service platforms such as Google Authenticators, DUO, HPR, FIDO2, Samsung and Microsoft.

Realizing security, trust and privacy

Passwordless Guardian-CCS, Realizing Security, Trust and Privacy



Sales value proposition

Value proposition of Guardian-CCS



Convenience

- Passwordless one-stop authentication
- Convenient user installation
- Superfast authentication with SLA/SLG
- User friendly & reliable
- User & admin dashboard records for audit logs
- Fast onboarding & exiting management process



Security

- No penetration point for hackers/inside threats
- No vulnerability
- Distributed blockchain MFA
- OTSK for blockchain channel & node instances
- Never hackable OTSK due to volatile runtime object
- CCRA Certification EAL2 (2022)



Proof of Trust

- Zero trust hybrid architecture
- Minimum personal data
- Blockchain distributed verification & consensus
- Meet BNM RMIT, MCMC INS, PDPA, GDPR requirements



Cost Saving

- No upfront cost for On-Cloud and On-Click
- No additional MFA cost
- User license, usage base pricing
- ROI & VOI with up to 70% operational cost savings
- No additional device
- Standard REST API for Integration & SDK

Value matrix analysis

Guardian-CCS : Quantitative & Qualitative Value Matrix



Satisfy customer needs

Guardian-CCS : **Satisfying Customer Requirements**

G-CCS KEY VALUES

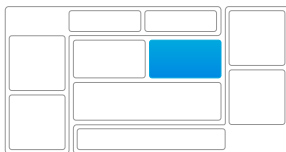
User Experience



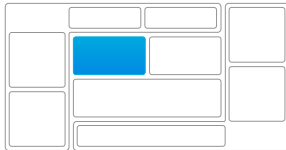
Security



Sustainability



Privacy



Scalability



CUSTOMER KEY REQUIREMENTS

How easy is it to install and operate the solution?

How does it assist with user adoption?

How convenient, ubiquitous and portable?

Choice of authenticators for user preference?

Resist most common cyber attack?

Expected vulnerability in the near future?

Comply with current security standards?

How complete is the solution?

Cost of implementation and maintenance

Actual ROI

Integration capability with legacy security system

Secondary effect from environmental aspect

Privacy data storage: Central or Distributed?

Consent management feature

Capability to enhance privacy

Choice for users regarding how much data to share?

Vertical/Geographical/Demographic Scalability

Performance for high demand

Error rate of the authentication solution

Continuity and recovery strategies

G-CCS KEY FEATURES

Simple and Intuitive installation in Android and iOS

One-stop passwordless authentication experience

Do not require additional device (BYOD)

Additional authenticators : Biometrics, Pattern, PIN, OTP

Free from hacking attempts toward Mobile App and Server

No single point of vulnerability and hacking opportunity

Rest API to integrate other authenticators, IdP, eKYC, 3rd Party MFA

End-to-end services with mobile app, server and admin.

No upfront cost for Cloud. Minimum cost for On-premise and usage

Proven ROI and VOI from passwordless features

Provide standard REST API for Integration with legacy and cloud

Require minimum server spec

Store Non-critical user data in blockchain nodes

Integration capability with consent management system

By Design, G-CCS doesn't store sensitive privacy data

Provide alternative options to share user information

Provide scale out capability on the fly basis and future proof

SLA of 3 seconds of latency @10,000 concurrent connections

SLA of 0.02% of error rate

Provide HA and DR strategies with HA architecture design

Frequently Asked Questions

Guardian-CCS : **FAQ**

Questions

How easy is it to install and operate G-CCS?

How does the solution support user adoption?

Is G-CCS convenient and portable?

Do users have choice for 2FA or authentication factors?

How does the solution resist cyber attacks?

How does G-CCS protect the current and future vulnerability?

Does the solution comply with security standards?

How complete is the solution?

How much is the cost for implementation and maintenance?

How much is the expected ROI?

How is the integration capability of legacy security systems?

What is the environmental impact of the solutions?

Is data privacy protection at the storage centralized or distributed?

Does the solution consider user consent and consent management feature?

What is the solution capability to enhance privacy?

What is the choice for users regarding how much data to share?

How is the solution scalability for vertical, geographical and demographic?

How is the performance of the solution measured?

What is the error rate of the authentication solution?

Does the solution provide DR, business continuity and recovery plan?

Clarification

Very simple and intuitive installation in Android and iOS. Just install G-CCS from App Store or Google Play Store.

It provides passwordless one-stop authentication experience and user onboarding. It can be also used as both of existing ID/Password and G-CCS.

The solution doesn't require additional device (BYOD). Just use existing mobile phone as your personal and private authenticator.

The device and user profile are the 1st level authentication. Additional authentication factors are biometrics, pattern, icon and OTP.

No penetration point for hackers or insider threats. No critical data for hackers to penetrate at the mobile app and server.

The solution is designed without any single point of vulnerability.

It has been certified as Good Quality software in Korea, and received ISO 15408 Common Criteria certification in 2021, hosted by CSM.

End-to-end managed security services from mobile app, server and admin for On-Cloud, On-Click and On-Premise solutions. Provided with REST API and SDK for integration services.

No upfront cost. The cost charges per user license or per click license (usage base) based on usage pricing model.

The estimated ROI/VOI is up to 70% depending on the use cases and with passwordless.

G-CCS provides standard REST API which integrates legacy systems and third party authenticators.

No need for additional device. Minimum server specs is enough.

2FA or MFA data is not stored centrally. Minimal data from server and device are hashed and encrypted before being distributed for authentication.

User consent is required for minimum user information like email and mobile number. It can be also integrated with consent management system.

It is designed to focus on privacy so that does not store any sensitive data. The features ensure compliance to GDPR & PDPA 2010 requirements.

Users can permit the consent level at the registration step. It provides alternatives how much to share information. It only uses data locally provided on the device.

Its capability is scalable on the fly basis with HA, full redundancy and DR/backup in On-Cloud and On-Click.

For On-Premise, the baseline of HW specification is available for 10,000 concurrent connections/sessions, which is made in 3 seconds.

The SLA is under 0.02% of error rate.

The SLA for On-Cloud and On-Click management services includes DR & replication services. For On-Premise, it is highly recommended for two onsite licenses for production & DR site.

Value USP/UVP

User Experience (Value)

User Experience (Value)

User Experience (Value)

User Experience (Value)

Security (Value)

Security (Value)

Security (Value)

Security (Value)

Sustainability (Value)

Sustainability (Value)

Sustainability (Value)

Sustainability (Value)

Privacy (USP/UVP)

Privacy (USP/UVP)

Privacy (USP/UVP)

Privacy (USP/UVP)

Scalability (USP/UVP)

Scalability (USP/UVP)

Scalability (USP/UVP)

Scalability (USP/UVP)



CIAM Solution

A Trusted Customer Identity & Access Management Solution



01

Trust & Passwordless

Mobile phone is the most trusted device by the user and only one mobile phone is enough for multiple applications registered on G-CCS authentication. Users, customers and partners can reuse their mobile phone identity without creating a new login and password. This results in less friction and higher security.

02

Data Transparency

As users use the same device with a unique ID across multiple business applications and organizational systems, this is a more efficient method for both of reporting data usage and access. G-CCS, based on international standards, privacy laws and regulations, shows excellent performance to update user profile and to process their history.

03

Audit Trails & Forensics

Using the same device with a unique ID also supports compliance reporting, audit trails, and forensic investigations. This also streamlines compliance reporting processes.

04

Advanced Security

G-CCS is already the next generation secure authentication MFA with blockchain. It allows partners and customers to connect their own ID with password or other preferred robust, enterprise-ready security and advanced technologies such as eKYC, MFA, conditional access and authentication.

05

Enhanced User Experience

G-CCS is not only about security and privacy protection but also offers fast, convenience and frictionless user experiences. G-CCS supports varied technologies over blockchain, Artificial Intelligence, Machine Learning and algorithms.

Go passwordless with Guardian-CCS!

The Next Generation Secure Solution, G-CCS

- 01 G-CCS is the global leader in passwordless blockchain-based secure access authentication MFA.
- 02 G-CCS is designed for security, privacy and trust in the cloud and on-Premise throughout digital access lifecycle management.
- 03 Our solution delivers the next generation passwordless secure multi-factor authentication to reduce risks created by ID, password, credentials and secrets.
- 04 Our solution is trusted in leading organizations including government, financials, education, ICT Services, enterprise & SME with more than 1 million users and 25 customers to prevent external attackers and malicious insiders.
- 05 G-CCS empowers our customers to significantly reduce their risks in digital environment and complies with international standards and regulatory requirements.
- 06 As the solution services provider, we strictly adhere to high security practices and fully comply with corporate policies including:
 - 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)
 - Support PDPA, BNM RMIT, MAS TRM, PCI-DSS, HIPAA, EU GDPR compliance requirements
 - Network, applications and infrastructure security including best-in-class systems and technology solutions
 - Physical security with stringent policies and procedures
 - People security including ongoing training, education and background checks
 - Ongoing risk, compliance and security assessments
 - Services Level Management with SLA/SLG
 - Business Continuity Management and Disaster Recovery Plan



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



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