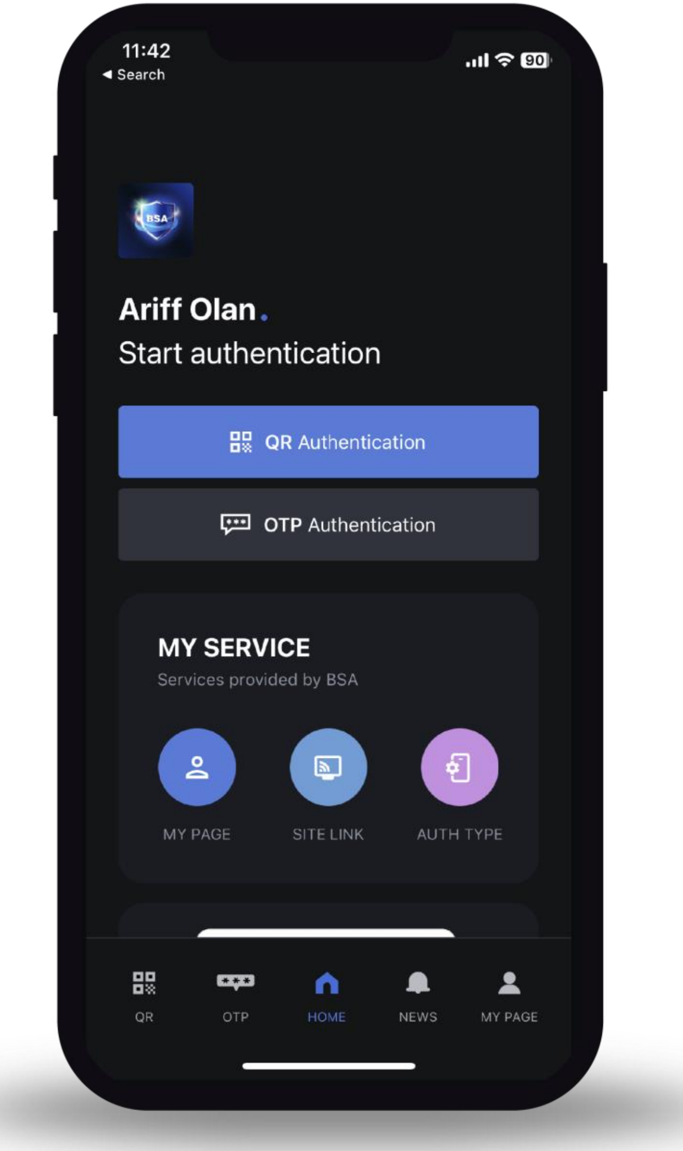
Passwordless Blockchain Secure Authentication

Reinforce Security For Digital Financial Services



Ariff Olan.
Start authentication

MY SERVICE
Services provided by BSA

Table of Contents

1. Introduction
2. Passwordless BSA Overview
3. Passwordless BSA Technology
4. User Experience Demonstration
5. Use Cases
6. Q&A

Introduction

Why use BSA?

Cybersecurity threats are **worryingly high and keeps rising.** Here are some facts and figures about the current state of cybersecurity in 2024, such as:

USD10.5 Trillion

Annual global cost of cybercrime by 2025

Source: Cybersecurity Ventures

130%

Increase in ransomware attacks in Jan 2024

Source: BlackFog

19%

of cyberattacks in 2023 was due to compromised business email

Source: Check Point Research

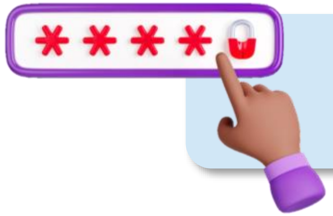
74%

of breaches in 2023 involved the human element

Source: Verizon

Current Access Security measures are not enough

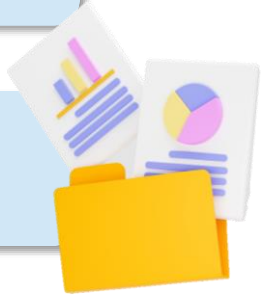
Some challenges and limitations of the current access security measures, such as:



Passwords are easy to forget, steal, or hack.

Multi-factor authentication (MFA) adds complexity and inconvenience for users, devices can be stolen.

Biometrics can be spoofed or compromised.



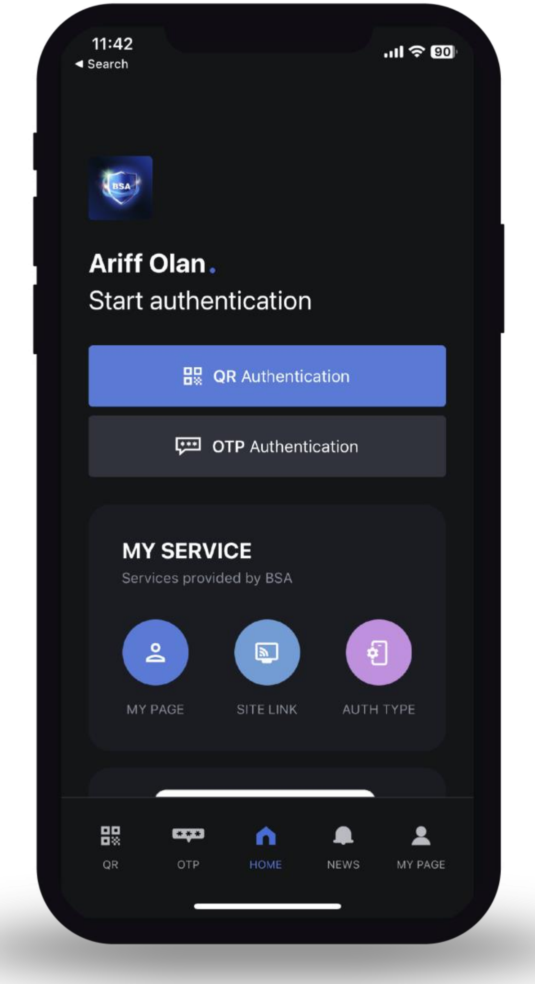
Centralized databases are vulnerable to breaches or attacks.

Passwordless BSA: Overview

What is Passwordless BSA?

A **True-Passwordless Multifactor Authentication (MFA)** Solution

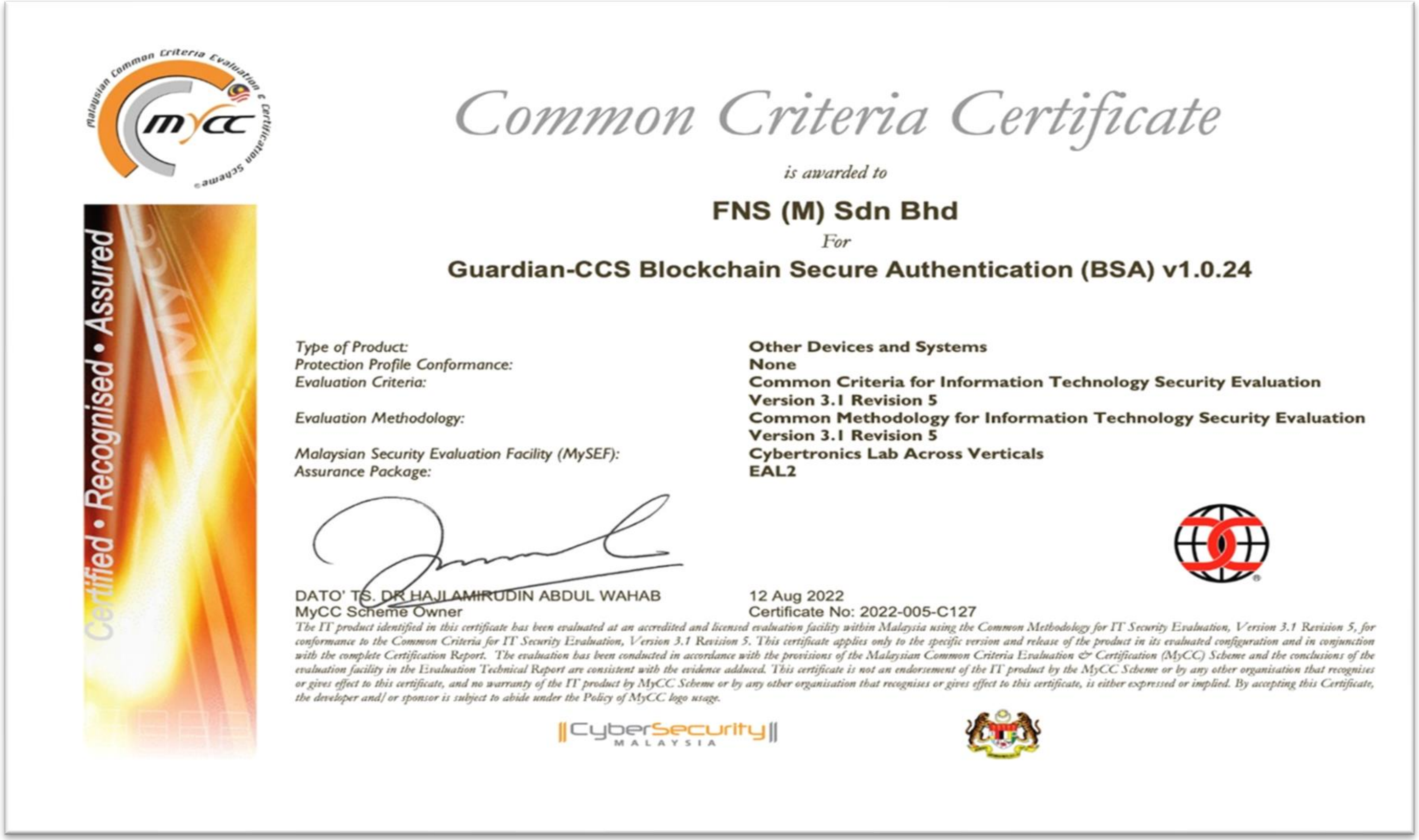
Utilizes **Blockchain Technology** for verification & authentication.



Unique Technologies

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

Common Criteria Certificate



Certified • Recognised • Assured

Common Criteria Certificate

is awarded to

FNS (M) Sdn Bhd

For

Guardian-CCS Blockchain Secure Authentication (BSA) v1.0.24

Type of Product:	**Other Devices and Systems**
Protection Profile Conformance:	**None**
Evaluation Criteria:	**Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5**
Evaluation Methodology:	**Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 5**
Malaysian Security Evaluation Facility (MySEF):	**Cybertronics Lab Across Verticals**
Assurance Package:	**EAL2**

DATO' TS. DR HAJI AMIRUDIN ABDUL WAHAB
MyCC Scheme Owner

12 Aug 2022
Certificate No: 2022-005-C127

The IT product identified in this certificate has been evaluated at an accredited and licensed evaluation facility within Malaysia using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report. The evaluation has been conducted in accordance with the provisions of the Malaysian Common Criteria Evaluation & Certification (MyCC) Scheme and the conclusions of the evaluation facility in the Evaluation Technical Report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by the MyCC Scheme or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by MyCC Scheme or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied. By accepting this Certificate, the developer and/ or sponsor is subject to abide under the Policy of MyCC logo usage.

CyberSecurity MALAYSIA

Evolution of Authentication

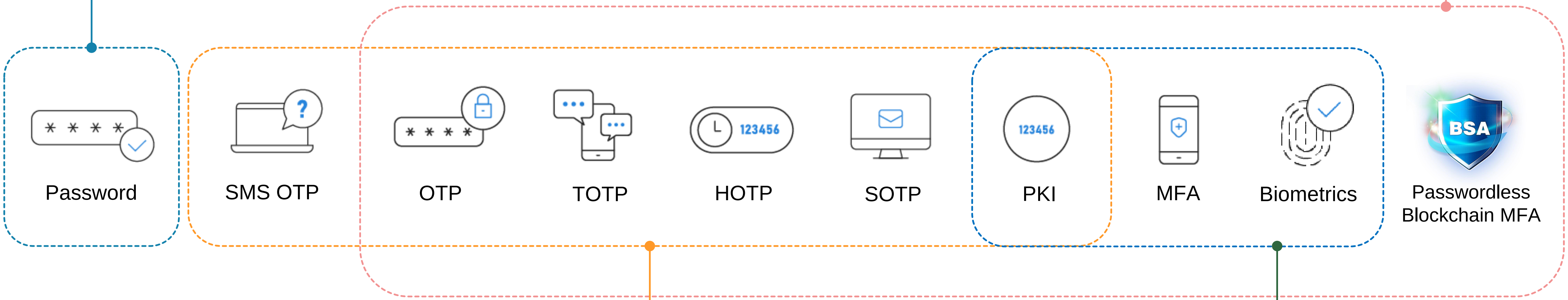
1st Generation

Password-based Authentication

- 1FA (User ID & Password)

4th Generation

Passwordless Blockchain MFA (OTP ~ Biometric)
True-Passwordless (Non-PKI-Based, No Master Key)
True Frictionless (Fast and Convenient)
One-Time Security Key (Decentralized Depository)
Distributed Ledger Technology (DLT) Authentication



2nd Generation

One-Time Password/Token Based Authentication
2FA (SMS, OTP, TOTP, HOTP, SOTP)
Certificate Based Authentication - 2FA (PKI)

3rd Generation

Biometric Authentication - 2FA (Face, Fingerprint)
Multi-Factor Authentication - MFA (PKI, Biometric, Token)
Centralized Depository - Passwordless

Benefits of BSA

Security

- Patented blockchain technology utilizing single device per user
- No penetration points for hackers or insider threats.
- CCRA EAL2 Certified

Convenience

- Fast authentication speed under 3 seconds
- Easy and intuitive user experience
- Customizable application (white labelling)

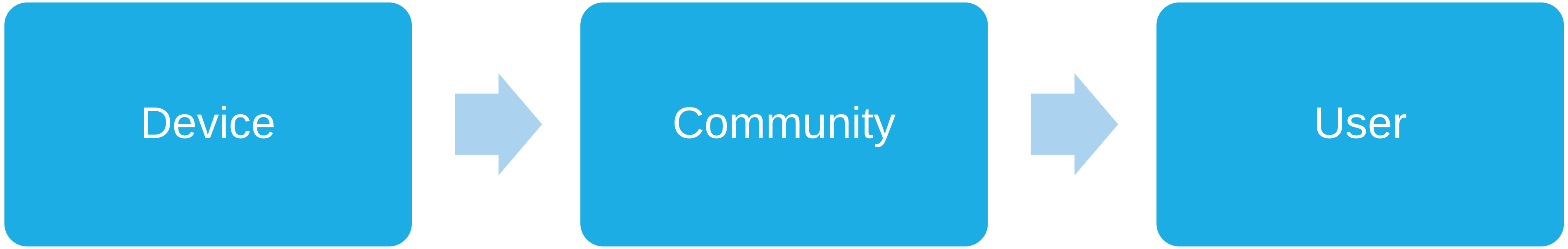
Cost-saving

- Eliminate IT support tickets on password-related issues
- Eliminates the need for password management softwares
- Eliminates the need for password policies

Passwordless BSA: Technology

How Passwordless BSA works?

Passwordless BSA works on 3 levels:



Device

Community

User

(MIRC + OTSK)

(MDV)

(Biometrics)

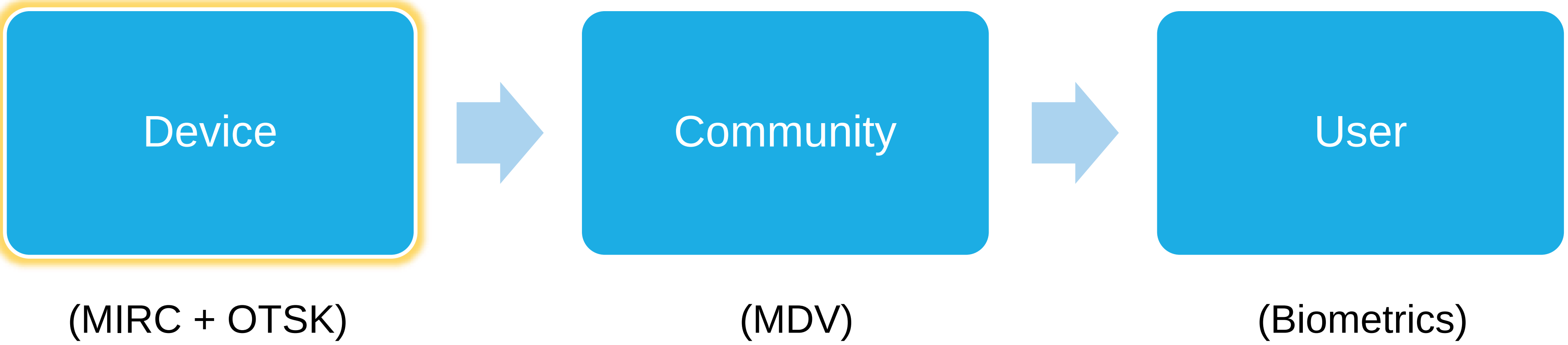
If any of the steps fail, the user will be unable to advance to the next level.

Onboarding Process

Upon onboarding, users will:

1. Provide only 4 unique information:
   1. Full Name
   2. Username
   3. Email address
   4. Mobile number
2. Register one mobile device to act as authenticator
3. Registered users will become a blockchain node which will be used for blockchain authentication

Level 1: Device



Device

(MIRC + OTSK)

Community

(MDV)

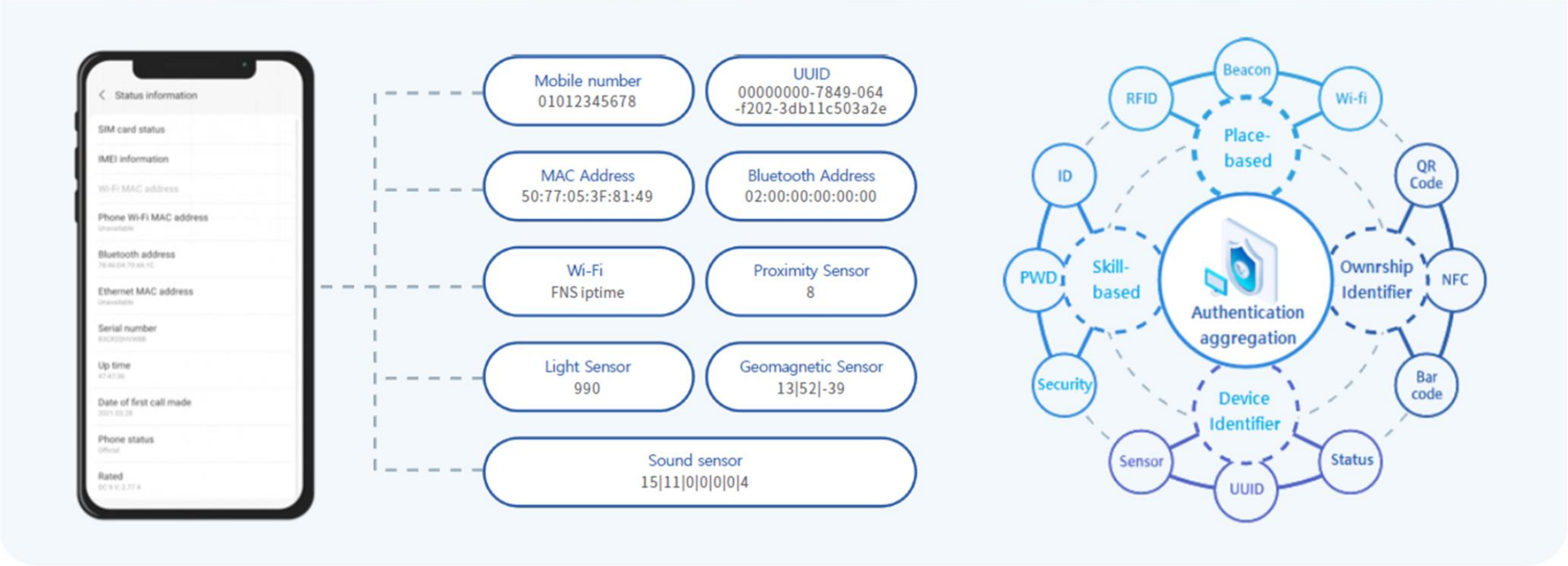
User

(Biometrics)

Level 1: Device Multi Identifier Random Combination (MIRC)

Extract multiple unique identifiers from users' mobile devices to create unhackable unique key.

- 01 Pass the unique identifier of the user's mobile device to the BSA server
- 02 Randomly extract a unique identifier of user device from the server
- 03 Combining location, ownership, device identifiers, and knowledge-based information
- 04 Generate a one-time security key (OTSK) for secure authentication without password



< Status information

SIM card status

IMEI information

Wi-Fi MAC address

Phone Wi-Fi MAC address
Unavailable

Bluetooth address
78:46:D4:70:4A:1C

Ethernet MAC address
Unavailable

Serial number
[illegible]

Up time
47:47:36

Date of first call made
2021.03.28

Phone status
Official

Rated
DC 9 V; 2.77 A

Mobile number
01012345678

UUID
00000000-7849-064
-f202-3db11c503a2e

MAC Address
50:77:05:3F:81:49

Bluetooth Address
02:00:00:00:00:00

Wi-Fi
FNS iptime

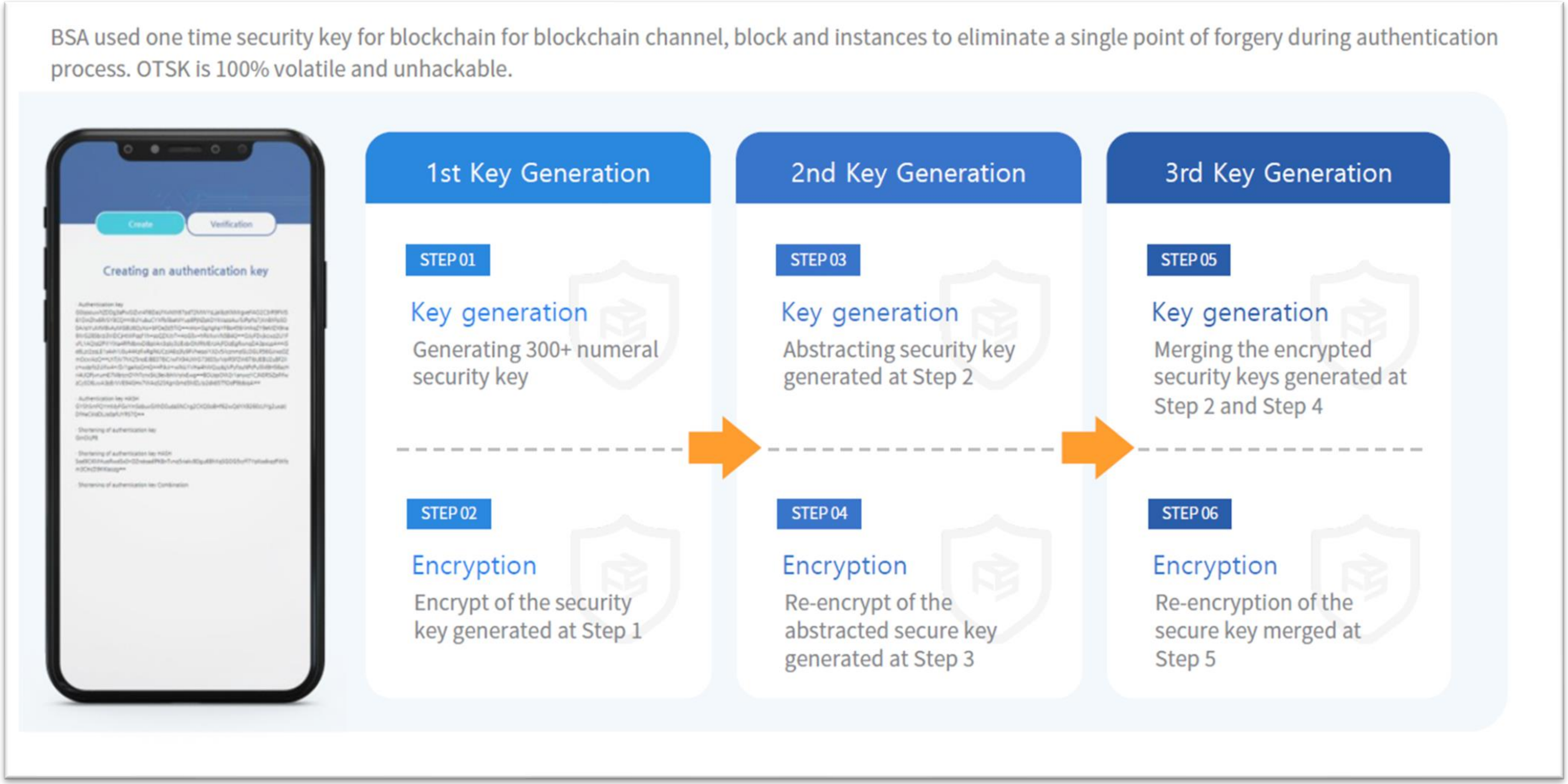
Proximity Sensor
8

Light Sensor
990

Geomagnetic Sensor
13|52|-39

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

Level 1: Device   One-Time Security Key



BSA used one time security key for blockchain for blockchain channel, block and instances to eliminate a single point of forgery during authentication process. OTSK is 100% volatile and unhackable.

1st Key Generation

STEP 01

Key generation

Generating 300+ numeral security key

STEP 02

Encryption

Encrypt of the security key generated at Step 1

2nd Key Generation

STEP 03

Key generation

Abstracting security key generated at Step 2

STEP 04

Encryption

Re-encrypt of the abstracted secure key generated at Step 3

3rd Key Generation

STEP 05

Key generation

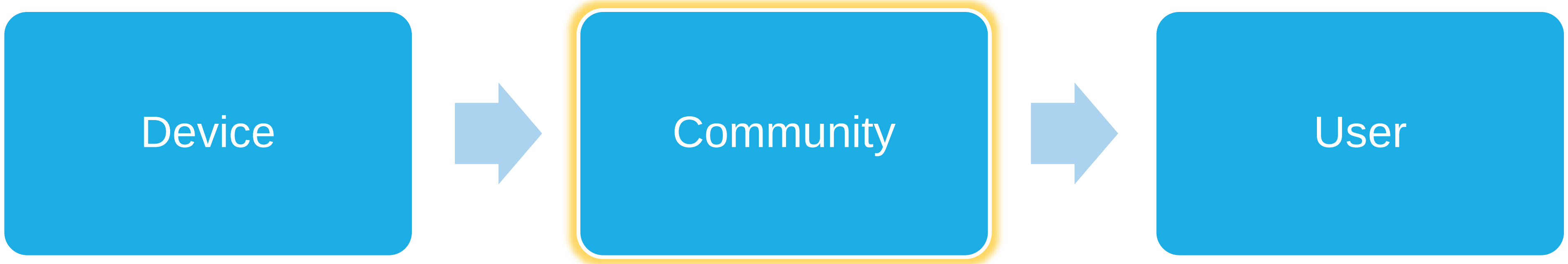
Merging the encrypted security keys generated at Step 2 and Step 4

STEP 06

Encryption

Re-encryption of the secure key merged at Step 5

Level 2: Community



Device

Community

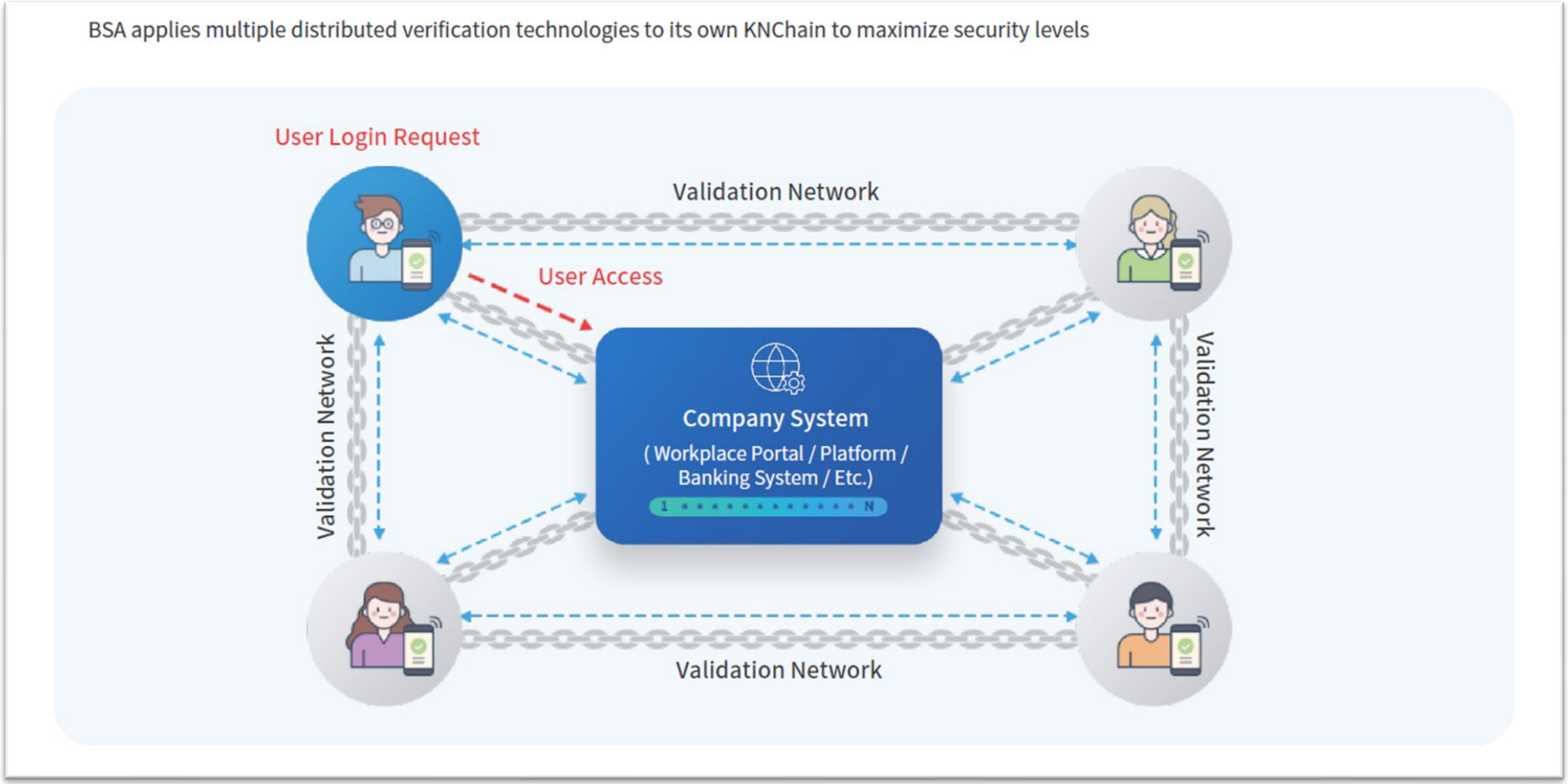
User

(MIRC + OTSK)

(MDV)

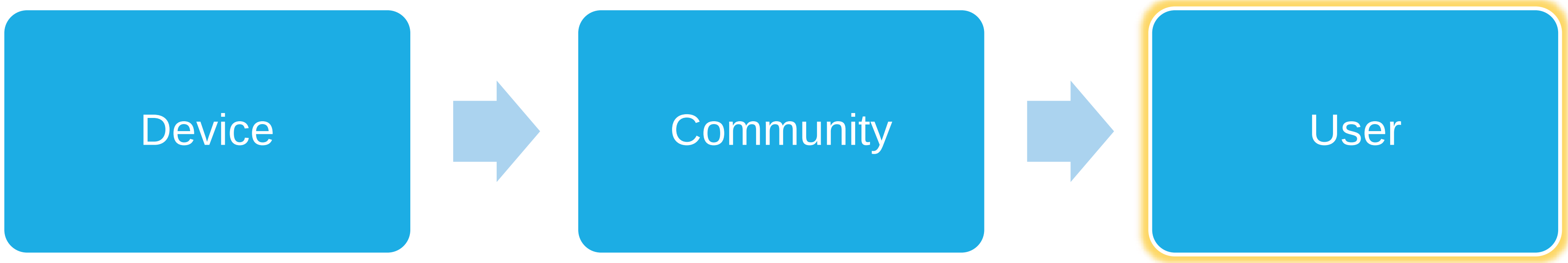
(Biometrics)

Level 2: Community Multilateral Distributed Verification (MDV)



BSA applies multiple distributed verification technologies to its own KNChain to maximize security levels

Level 3: User

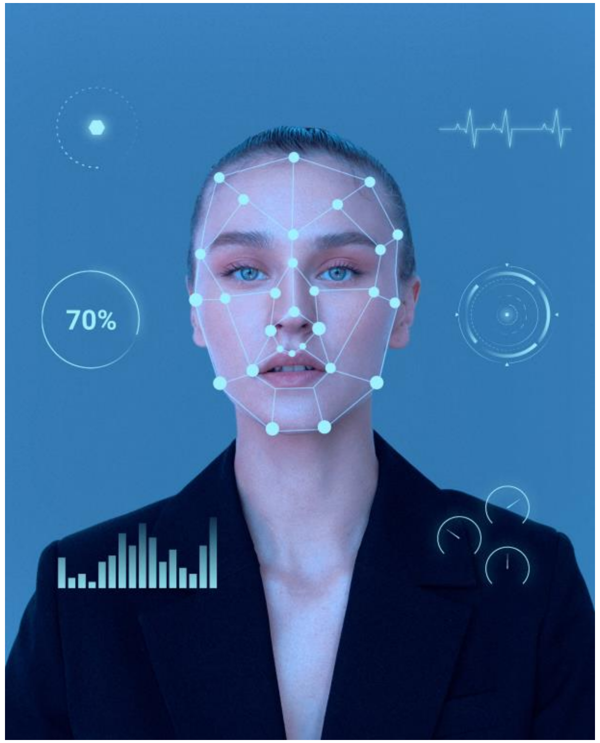


(MIRC + OTSK)

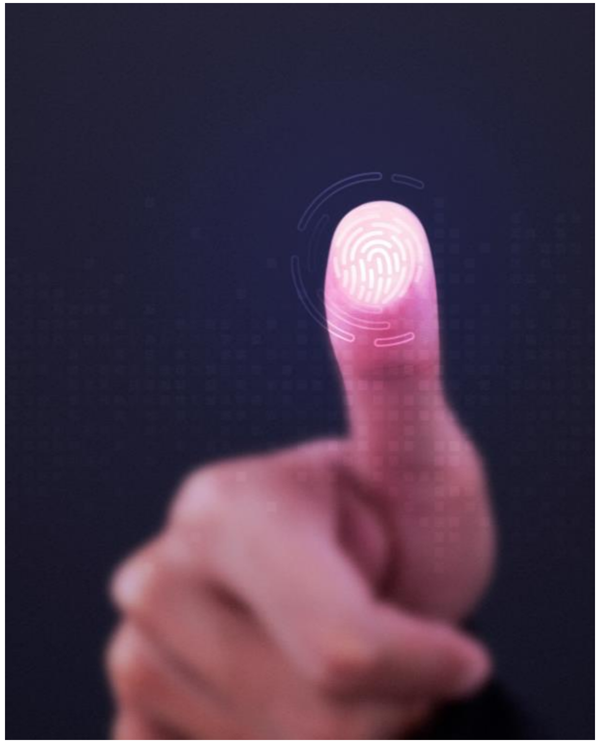
(MDV)

(Biometrics)

Level 3: User Biometrics



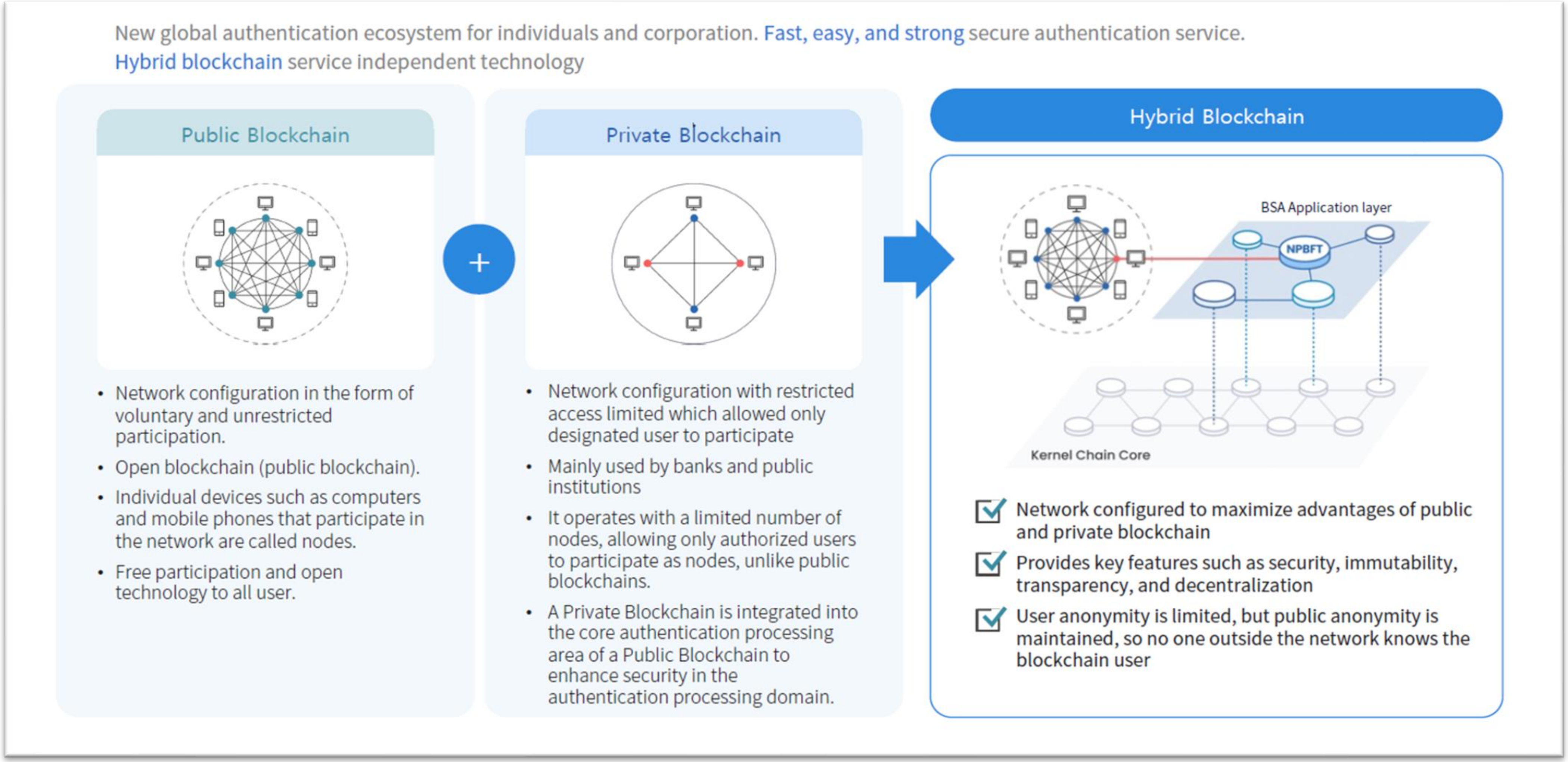
Face ID



Fingerprint

Note: Type of biometrics is dependent on the user’s mobile phone capabilities.

Kernel Chain Network (KNCHAIN) Hybrid Blockchain Network



New global authentication ecosystem for individuals and corporation. Fast, easy, and strong secure authentication service.
Hybrid blockchain service independent technology

Public Blockchain

- Network configuration in the form of voluntary and unrestricted participation.
- Open blockchain (public blockchain).
- Individual devices such as computers and mobile phones that participate in the network are called nodes.
- Free participation and open technology to all user.

+

Private Blockchain

- Network configuration with restricted access limited which allowed only designated user to participate
- Mainly used by banks and public institutions
- It operates with a limited number of nodes, allowing only authorized users to participate as nodes, unlike public blockchains.
- A Private Blockchain is integrated into the core authentication processing area of a Public Blockchain to enhance security in the authentication processing domain.

Hybrid Blockchain

☑ Network configured to maximize advantages of public and private blockchain

☑ Provides key features such as security, immutability, transparency, and decentralization

☑ User anonymity is limited, but public anonymity is maintained, so no one outside the network knows the blockchain user

Product Demonstration

BSA

PASSWORDLESS

BSA Use Cases

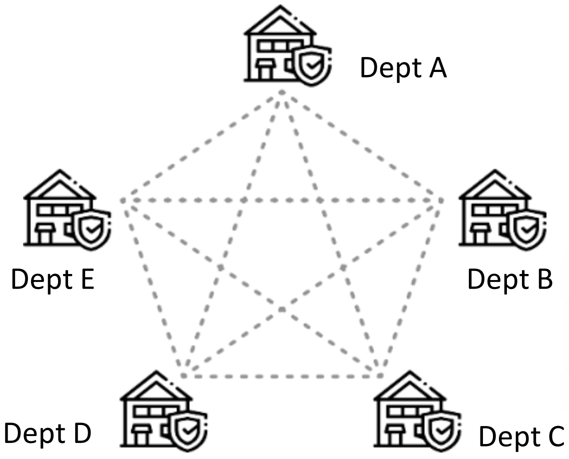
Use Cases

Passwordless BSA is applicable for the following use cases:

1. Managing Policies
2. Secured Application Login
3. Secured Payment Approval
4. Secured Virtual Private Network (VPN)
5. Secured Document Retrieval
6. Secured Digital Signing

Enabling Use Case 1: Managing Policies

As-Is



Challenges in Username ID & Password Management. Longer time user onboarding and exiting. Unproductive of password change management. Authentication interoperability becoming more complex as number of credential providers and relying parties increases.

Challenges

Objective

To enable Mutual Trust between users, devices and applications. Enable common interoperable with enterprise wide Authentication solution.

Value

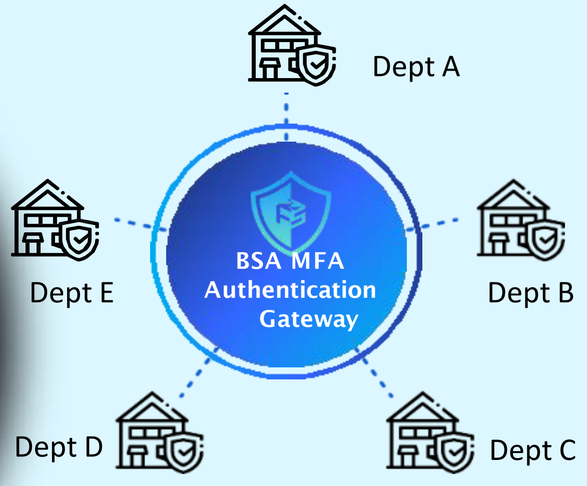
User Value

Trusted, consistent method of identity authentication to employee, customers and partners. Enable protection of confidentiality and sensitivity data.

Organization Value

Advanced authentication capability, reducing operating cost and increase productivity time of users within the organizations.

To-Be



Passwordless BSA MFA Authentication Services as the Secure Identity Authentication Gateway simplifies and unifies interoperability standardization of User Authentication security policy on user and device access.

Enabling Use Case 2: Secured Application Login

USE CASE	DESCRIPTIONS
Secured Portal/Web Login Authentication Access	**Deployed Users:** Administrators, vendors and students. **Previous UI/UX:** Organization and businesses login to the web portal using username and password. Requires a dedicated module to manage and monitor with Password Management Lifecycle Platform. **With Passwordless BSA UI/UX:** Organization integrates Passwordless BSA at their web portal landing page. Organizations are enabled with multiple options of logging into their web portals. Passwordless BSA blockchain technology entirely enhances the security for authentication without the need for passwords or tokens, removing inconvenient password policies. **Value Propositions:** ● Increased Cost Efficiency: Passwordless BSA reduced the cost for managing 3rd party platform to manage UserID and password. ● Decreased Authentication Processing Time: More efficient and effective. ● Improved User Management: Passwordless BSA deployment managed to reduce time and cost to manage organization resources, e.g., lost, stolen or forgotten password, etc.

Enabling Use Case 3: Secured Payment Approval

USE CASE	DESCRIPTIONS
Authentication Approval for Payment	**Deployed Users:** Public users. **Previous UI/UX:** Organization and businesses using conventional SMS OTP to make payments. This leads to possibilities of having other people make transactions without the account owner’s consent. Usually token-based (digital or physical). **With Passwordless BSA UI/UX:** Organization integrates Passwordless BSA at their payment web/mobile app portal. SMS OTP and tokens are replaced with One-Time Security Key (OTSK). **Value Propositions:** ● Reduced Operational Cost: Organization no longer needs to allocate high cost for SMS traffic and costs of managing security token issuance. ● Decreased Processing Time: Authentication processing is more efficient and effective. ● Improved User Management: Passwordless BSA deployment managed to reduce time and cost for managing organization resources, such as lost, stolen, or forgotten password, etc.

Enabling Use Case 4: Secured Virtual Private Network (VPN)

USE CASES	DESCRIPTIONS
Secured Virtual Private Network (VPN) Access	**Deployed Users:** System and Network Administrators, Managers. **Previous UI/UX:** Organization and businesses accessing their VPN Network via Conventional Username and Password. Which requires a dedicated module to manage and monitor with Password Management Lifecycle Platform. **With Passwordless BSA UI/UX:** Organization integrates Passwordless BSA at their VPN secure connection to access their private network. Organization no longer requires to have a Password Manager to monitor and track their password lifecycle. **Value Proposition:** ● **Increased Cost Efficiency: Passwordless BSA reduced the cost for managing 3rd party platform to manage UserID and password.** ● **Reduced Processing Time: Authentication processing is more efficient and effective.** ● **Improved User Management: Passwordless BSA deployment managed to reduce time and cost to manage organization resources, e.g., lost, stolen or forgotten password, etc.**

Enabling Use Case 5: Secured Document Retrieval

USE CASES	DESCRIPTIONS
Authentication for Document Retrieval	**Deployed Users:** Administrators, Managers, Public users. **Previous UI/UX:** Organization and businesses using conventional password locks on documents. Requires a dedicated module to manage and monitor with Password Management Lifecycle Platform. **With Passwordless BSA UI/UX:** Organization integrates Passwordless BSA in their document retrieval modules. At the same time, this solution requires authentication at the portal level prior to retrieving the document. Passwordless BSA creates a 2-layer of verification and authentication before any of the users can access the documents. **Value Proposition:** ● **Eliminate Vulnerabilities: Removes any gaps or openings for attackers to steal user identities.** ● **Increased Cost Efficiency: Passwordless BSA reduced the cost for managing 3rd party platform to manage UserID and password.** ● **There is no risk of key snatching or alteration since Passwordless BSA has an OTAK re-verification procedure.**

Enabling Use Case 6: Secured Digital Signing

USE CASES	DESCRIPTIONS
Secured Approval for Signing	**Deployed Users:** Administrators, Managers, Public users. **Previous UI/UX:** Organizations and businesses used conventional digital signing for approval. This leads to the possibilities of having other people sign documents on behalf of other people with/without the signing owner's consent. Uses Public Key Infrastructure (PKI) or tokens. **With Passwordless BSA UI/UX:** Passwordless BSA verifies a user with the randomized device authentication credentials stored in distributed ledgers. This allows organizations to mitigate the risks of misuse of digital signatures. **Value Proposition:** ● **There is no risk of key snatching or alteration since Passwordless BSA has an OTAK re-verification procedure.** ● **Eliminate Vulnerabilities: Removes any gaps or openings for attackers to steal user identities.** ● **Decreased Processing Time: Authentication processing is more efficient and effective.**

Passwordless BSA Setup

Passwordless BSA can be set up in two ways:

Passwordless BSA On-Cloud

- On-Cloud Security as a Service (SaaS) for both public and private customers.

Passwordless BSA On-Premise

- Provide On-Premise Security as a Service (SaaS) for customer web and mobile applications.
- One-off BSA per site license with unlimited applications.

Note: All Services are on a yearly subscription basis based on per user license.

Passwordless BSA in Malawi

Passwordless BSA holds relevance for Malawi due to the following reasons:

1. Enhance security for online activities and financial transactions
2. Eliminate password-based authentication
3. No gathering of sensitive personal data
4. Eliminate hidden IT support costs
5. Commitment to innovation and technological advancements

Q&A

Passwords are a thing of the past, the future is passwordless.

Thank you.