Blockchain Secure Authentication(BSA) for Digital Financial Services(DFS)

Passwordless BSA DFS

Cybersecurity threats are inevitable

The current state of cybersecurity in 2023

USD8 Trillion

Cost of cybercrime predicted in 2023

Source: Cybersecurity Ventures

4,741

Cases of cyber threats in Malaysia, 2022

Source: Cybersecurity Malaysia

USD6 Million

Malaysia’s total loss as of February 2023

Source: Cybersecurity Malaysia

8th /165

Malaysia’s ranking in terms of cyberattack vulnerability

Source: NordVPN

Why target cloud environments?

Multi-cloud environments are complex and therefore

more difficult to protect

Rapid software delivery processes make cloud-native apps

susceptible to vulnerabilities and misconfigurations

Rogue and shadow cloud environments

lack security controls and oversight

Siloed security point products leave blind **spots**

adversaries can slip through unnoticed

Threat actors are cloud-savvy and refine their tactics to Abuse cloud services and exploit cloud vulnerabilities. Here Are the top three cloud attack techniques observed by the CrowdStrike Threat Intelligence team over the past year while tracking 200+ threat actors.

Identity is a Key Cloud Access Point

Threat actors are seeking new ways to leverage identities in the cloud

43%

Adversaries are becoming more reliant on valid accounts, which were used to gain initial access in **43%** of cloud intrusions observed

67%

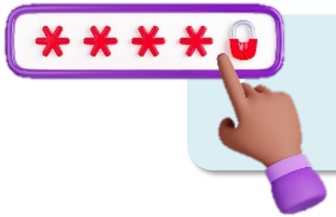
In **67%** of cloud security incidents, CrowdStrike found identity and access management roles with elevated privileges beyond what was required – indicating an adversary may have subverted the role to compromise the environment and move laterally

47%

Nearly half **(47%)** of critical misconfigurations in the cloud were related to poor identity and entitlement hygiene

How effective are the current access security measures?

The challenges and limitations of the existing access security controls:



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. Deep Fake.

Centralized databases are vulnerable to breaches or attacks. Insider Threats.

Challenges and Issues on Authentication Security

1FA: User ID and Password

Issues: Human Error, Too many passwords

Known Attacks:
Keylogger attacks, phishing attacks, and Man-In-The-Middle attacks (MITM)

1FA: User ID and Password
2FA: Certificate or Token-Based

Issues: Managing and Tracking PKI, Costs of operating (SMS, etc.)

Known Attacks:
Malware disguised as software update, Spyware for SMS Divert and MITM

1FA: User ID + Device + Password / User ID + Device + OTP Codes
2FA: Biometrics

Issues: Centralized user data & information, Credentials & Master Key/Password

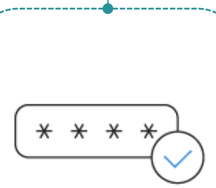
Known Attacks:
Compromised assets and devices

What is BSA?

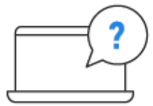
- BSA is a 4th generation authentication system – **Passwordless Blockchain Secure Authentication**
- BSA used hybrid blockchain technology with distributed verification to create a secure, fast and best passwordlesss user experience
- BSA can be used as the default passwordless secure authentication or can be treated as a 2nd factor authentication for digital services.
- BSA is based on Zero Trust Framework and developed with security (blockchain), privacy and trust by design

The Evolution of Authentication System

1st Generation



Password



SMS OTP

OTP

TOTP

HOTP

SOTP

PKI

MFA

Biometrics

DLT
Blockchain MFA
True Passwordless

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

3rd Generation

Biometric Authentication - 2FA (Face, Fingerprint)
Multi-Factor Authentication - MFA (PKI, Biometric, Token)
Centralized Depository – Master Key, Password or Passwordless

Why Passwordless?

SECURE

Strengthens security by eliminating risky password management practices and reducing attack vectors

LESS HASSLE

No passwords to memorize or security question answers to remember

RELIABLE

Improves user experiences by eliminating password and secrets fatigue

Why Blockchain?

SECURE

Strengthened by patented technology

PERFORMANCE

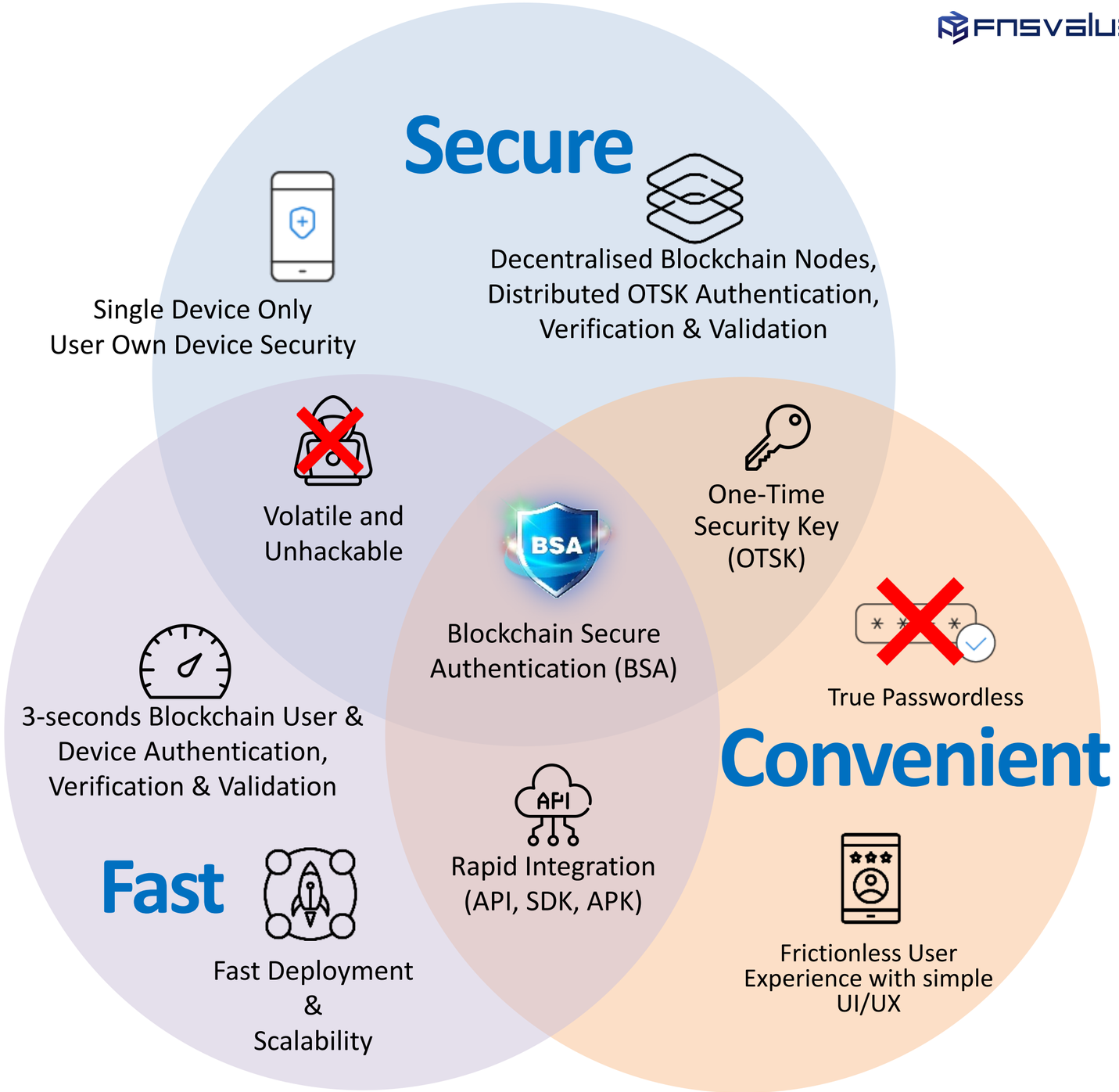
Fast, easy and convenient user experience

RESILIENT

High availability, confidentiality, integrity

Passwordless Blockchain Secure Authentication (BSA) SECURE, FAST & CONVENIENT

- Revolutionizes access security in the digital landscape.
- Ensures maximum security, faster deployment, scalable and convenient UI/UX.
- Provide an effective and efficient solution for safeguarding the crown jewels of organization's data with security, trust, resiliency.

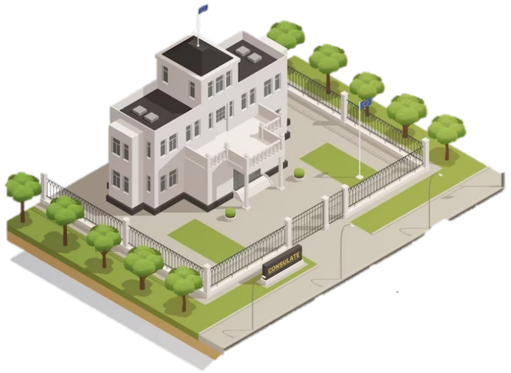


BSA is ready for Web 3.0 Digital Access Security

DLT with blockchain passwordless based authentication will revolutionize access security in the digital world:

Financial Institutions

Protect from unauthorized access or tampering – Bank Negara revised RMiT, regulated to comply with highest level of authentication technology & process possible.



Government

Protect government data from unauthorized access and tampering – many government assets and data is sold to dark web due to weak authentication

Information & Communications

Protect privacy of data through decentralization to secure from unauthorized access – comply to Privacy Regulations, GDPR, PDPA, etc.

Healthcare

Protect access to critical data – cannot be protected with current centralized way of authentication

Sources: Forbes, World Economic Forum, Harvard Business Review

BSA Technology Overview

1 – Multiple Identifier Random Combination (MIRC)

Extract and combine unique identifiers from user's mobile device

2 – One-Time Security Key (OTSK)

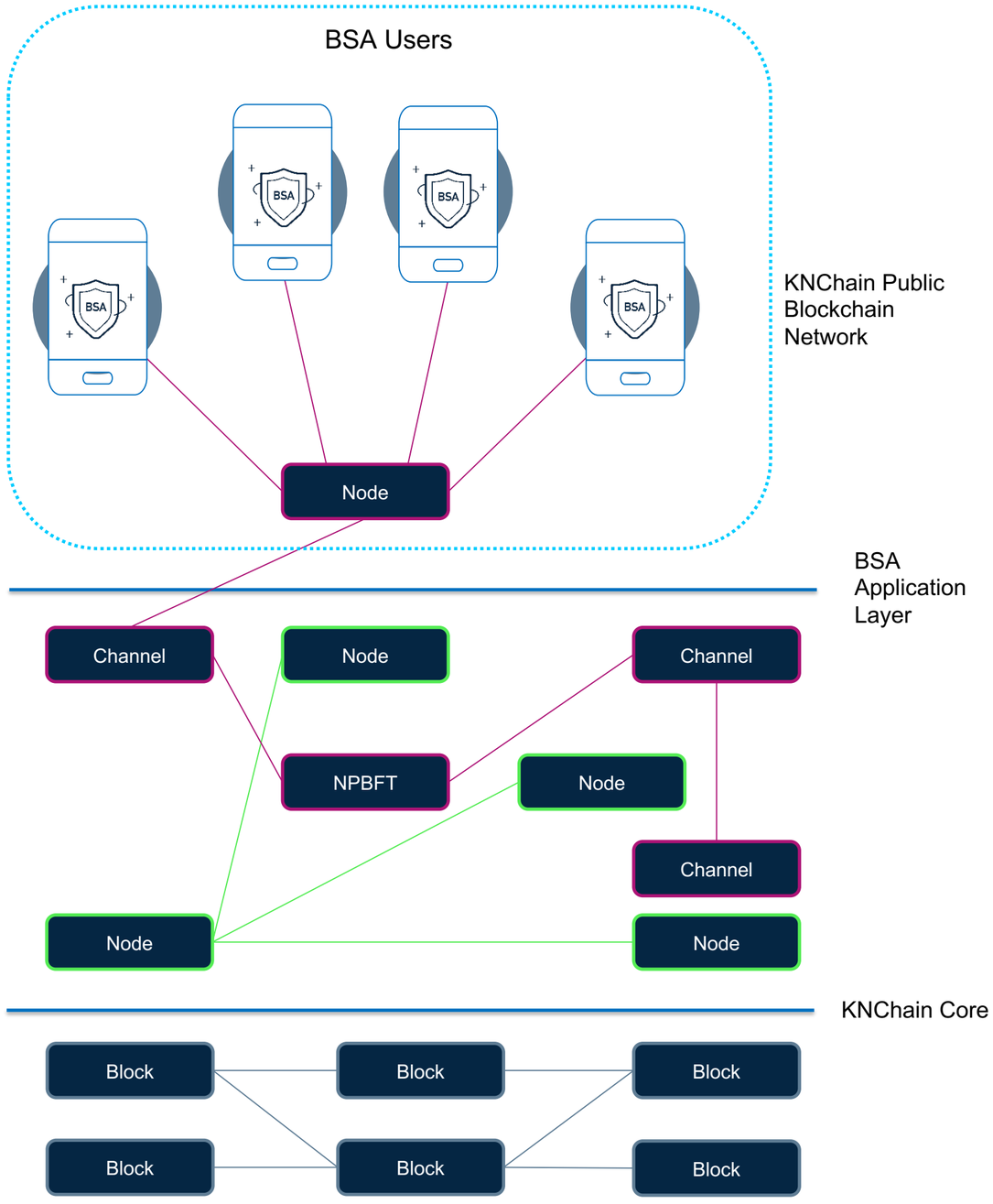
Generate a set of hashed and encrypted volatile security key from collected MIRC's data

3 – Multilateral Distributed Verification (MDV)

Distributed and decentralized verification based on KNCHAIN to maximize security level during authentication

4 – Kernel Chain Core (KNCHAIN)

BSA core engine - homegrown hybrid (Public and Private) blockchain technology



BSA Technology

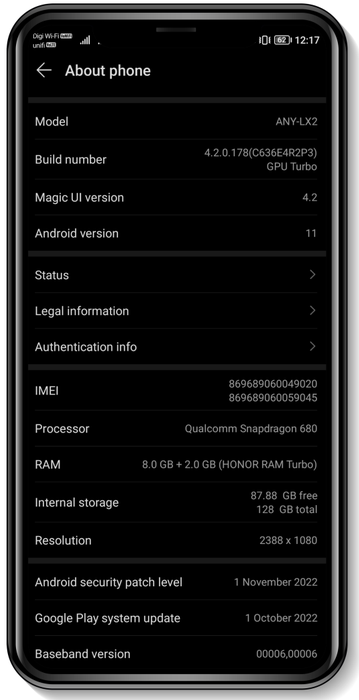
MIRC

OTSK

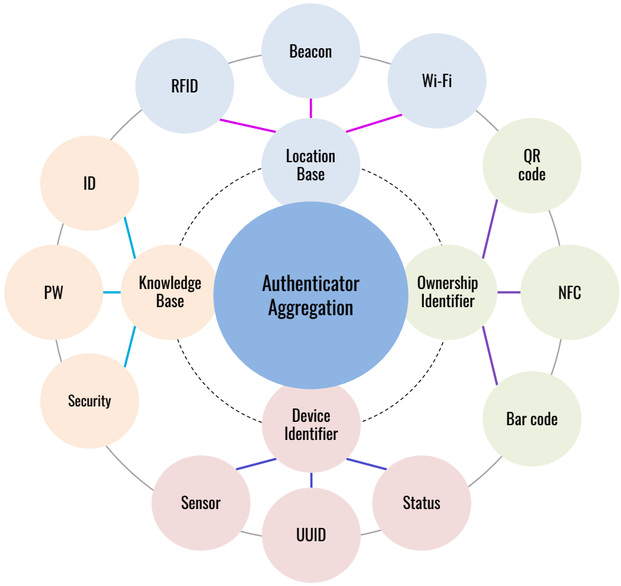
MDV

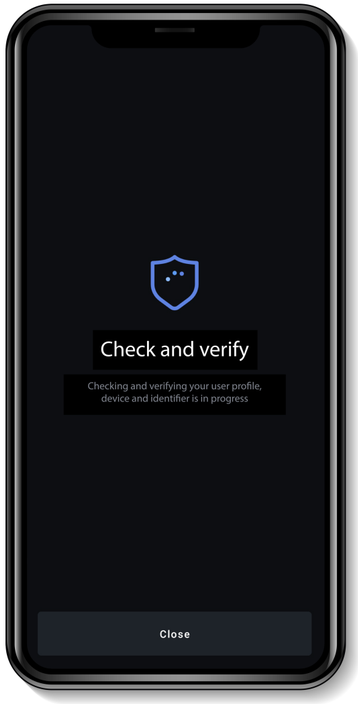
KNChain

Multiple Identifier Random Combination (MIRC)



Mobile number	01012345678
Device unique No	00000000-7849-0649-f202-3db11c503a2e
MAC address	50:77:05:3F:81:49
Bluetooth address	02:00:00:00:00:00
Wi-Fi info	FNS iptime
Proximity sensor	8
Brightness sensor	990
Terrestrial magnetism sensor	13|52|-39
Sound sensor	15|11|0|0|0|0|4





Gathering authentication elements using information values for each device

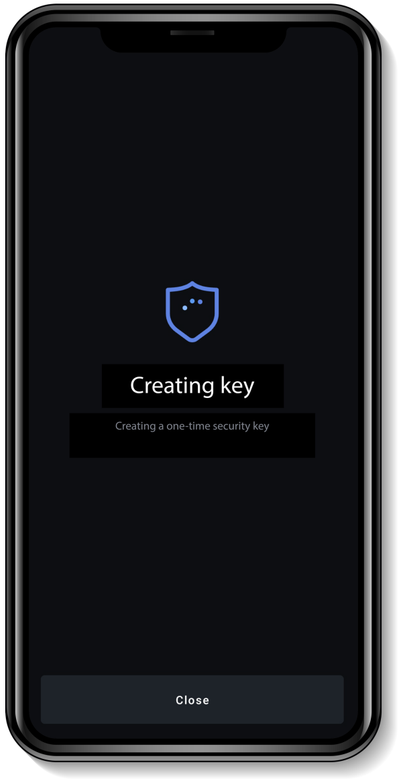
BSA Technology

MIRC

OTSK

MDV

KNChain



One Time Security Key (OTSK)

LEVEL 1

STEP 01

Generating 300+ numeral security key

STEP 02

Encryption of the security key generated at STEP 01

LEVEL 2

STEP 03

Abstracting security key generated at STEP 02

STEP 04

Re-encryption of the abstracted security key generated at STEP 03

LEVEL 3

STEP 05

Merging the encrypted security keys generated at STEP 02 and STEP 04

STEP 06

Re-encryption of the security key merged at STEP 05

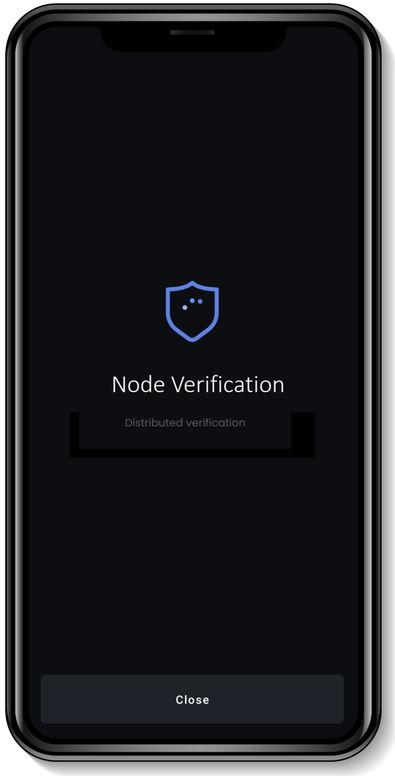
BSA Technology

MIRC

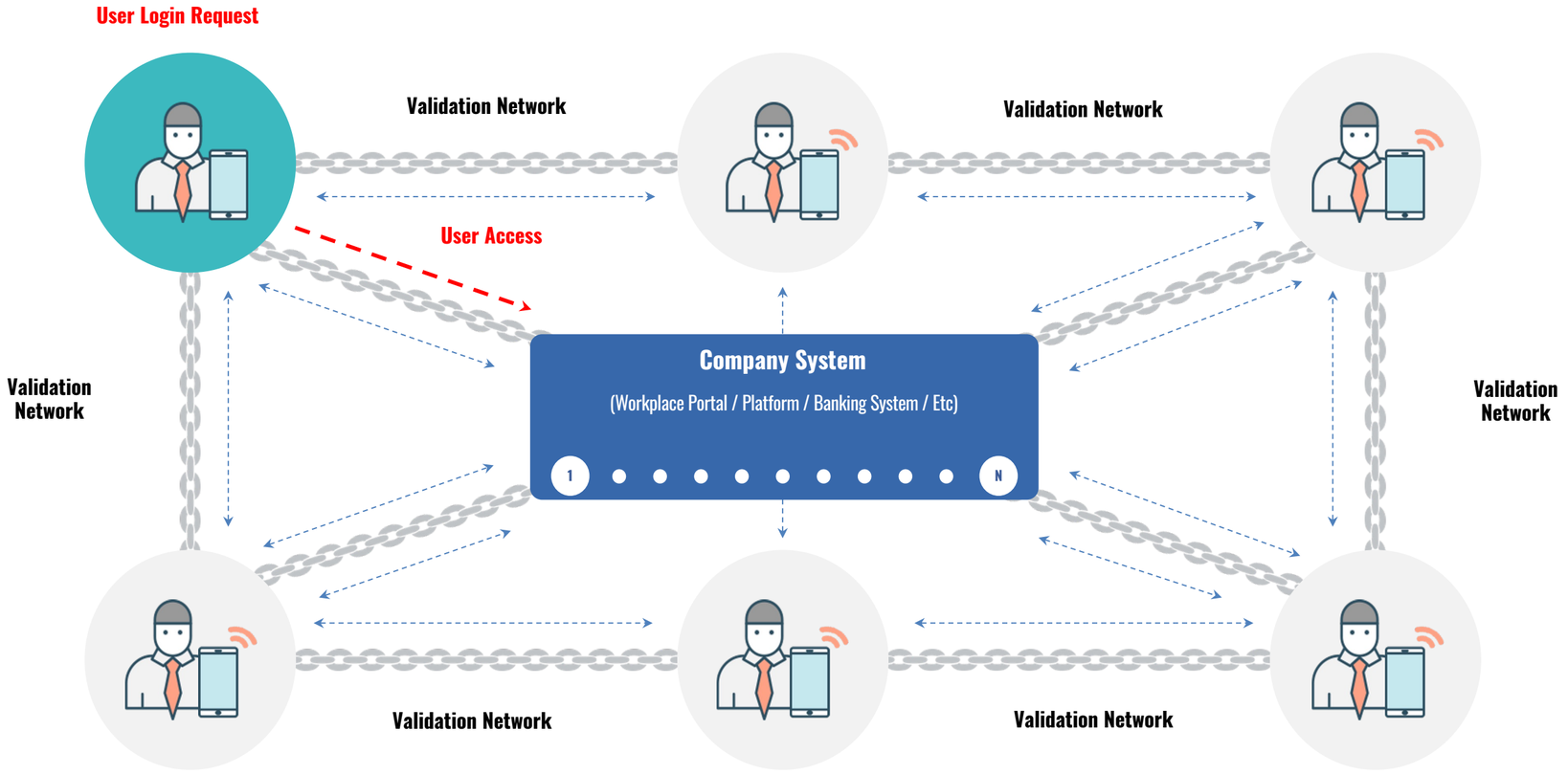
OTSK

MDV

KNChain



Multilateral Distributed Verification (MDV)



BSA Technology

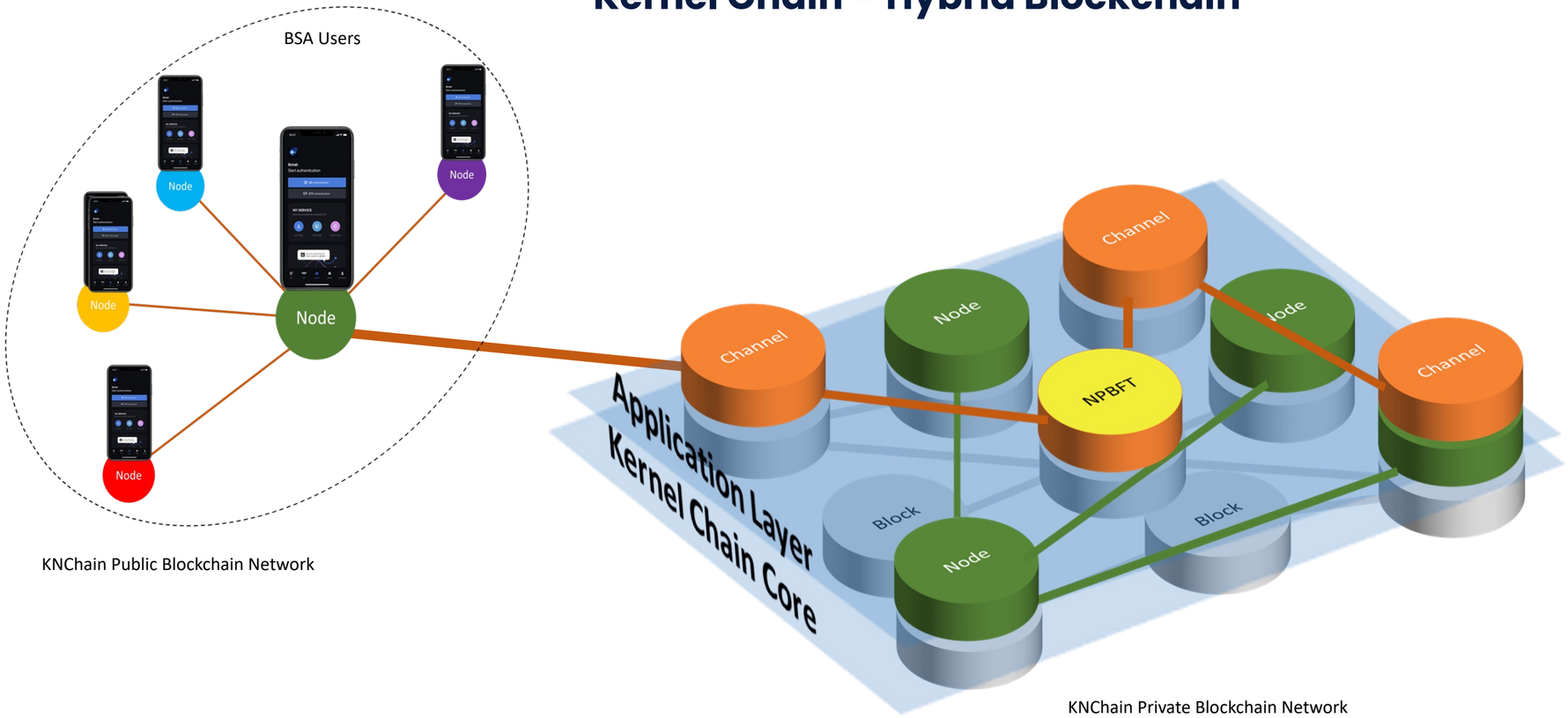
MIRC

OTSK

MDV

KNChain

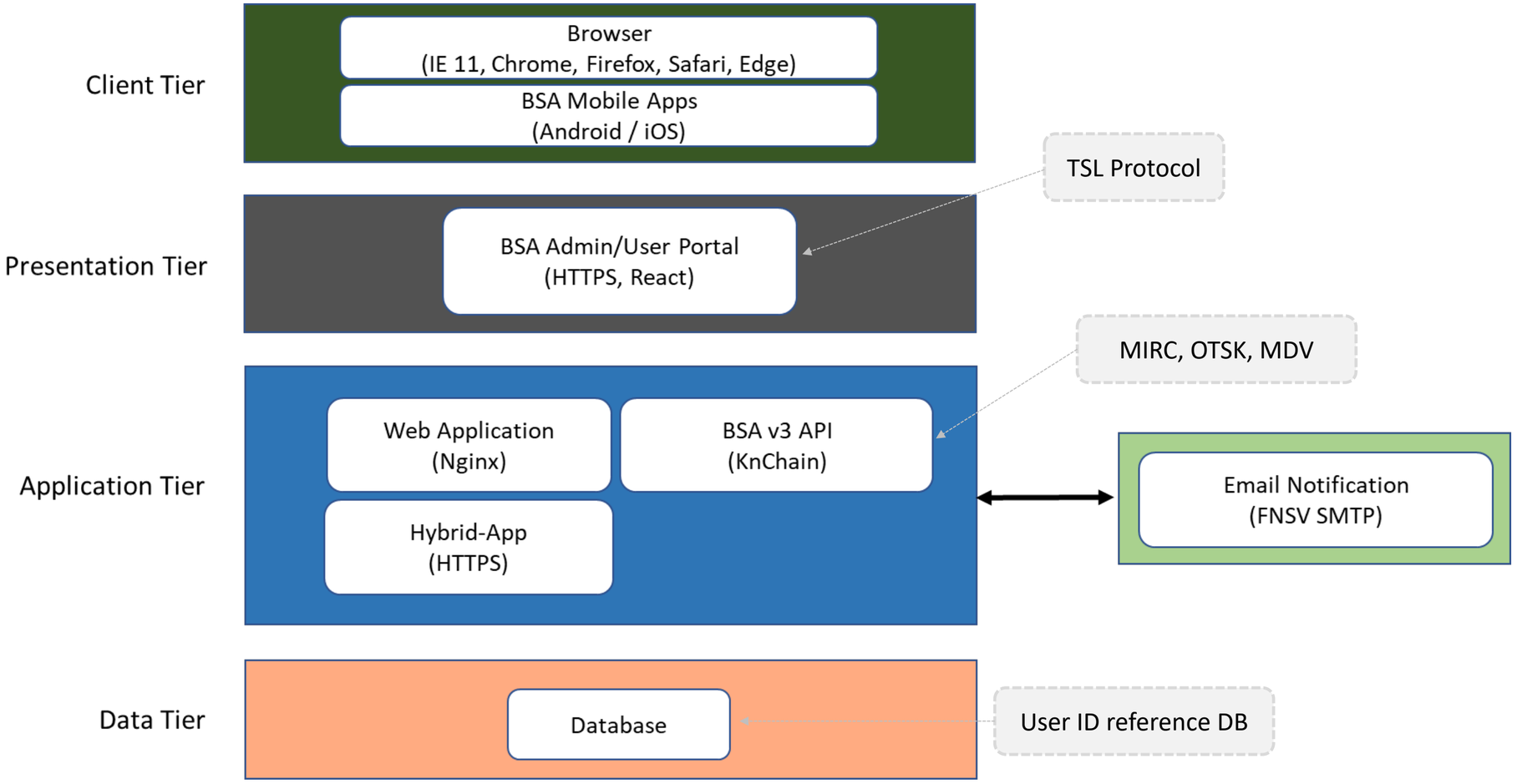
Kernel Chain – Hybrid Blockchain



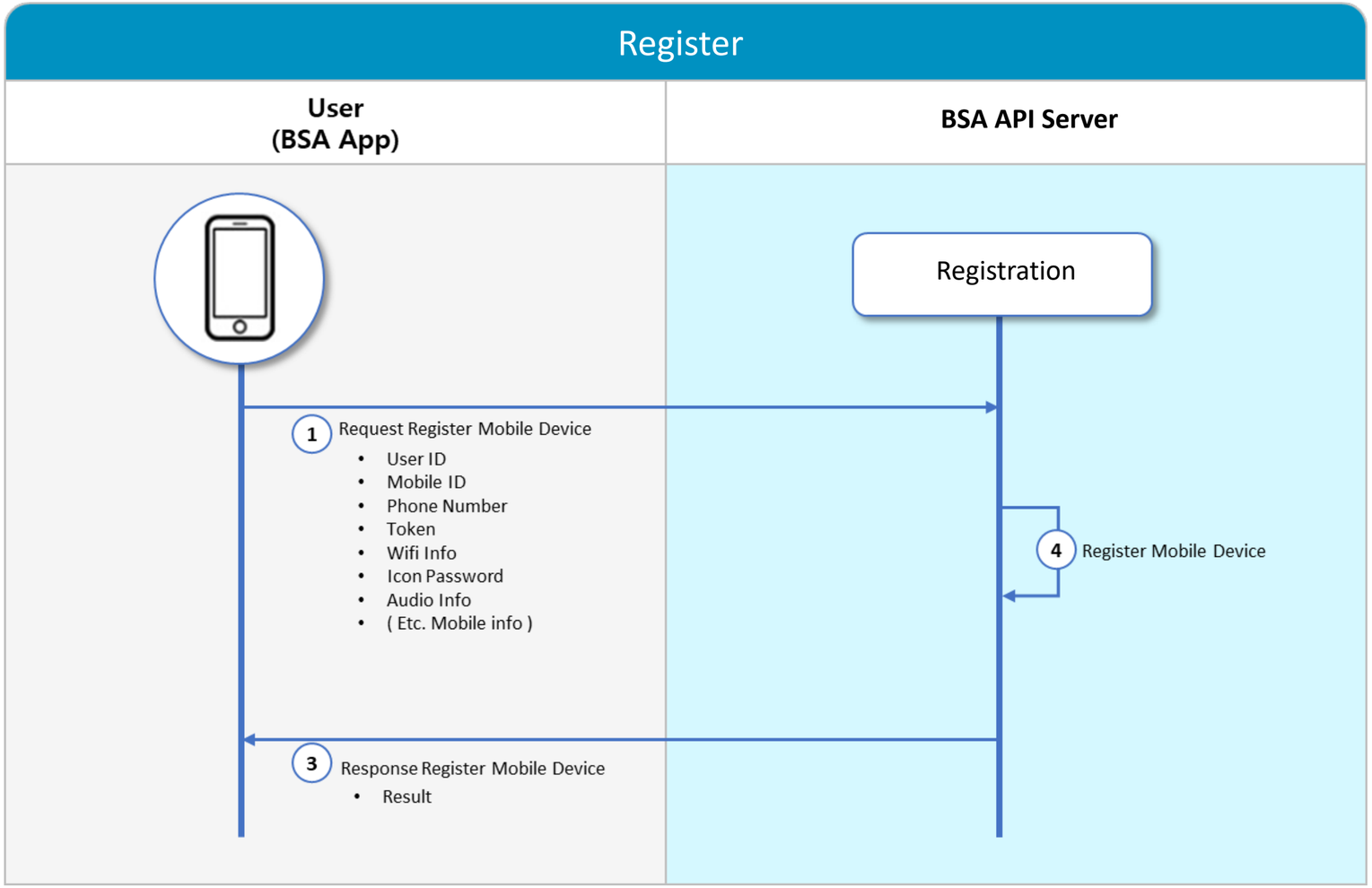
KNChain Public Blockchain Network

KNChain Private Blockchain Network

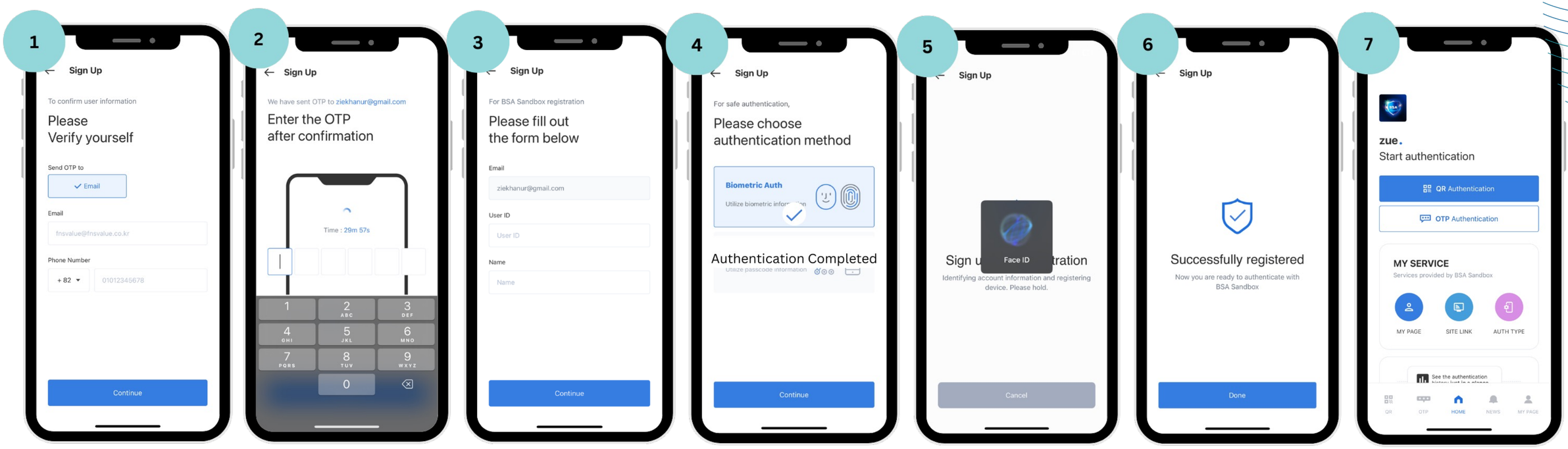
BSA Architecture



BSA User Registration



BSA Demo : User Registration



Key-in email and phone number

Email OTP verification (only registration)

Key-in user name and name

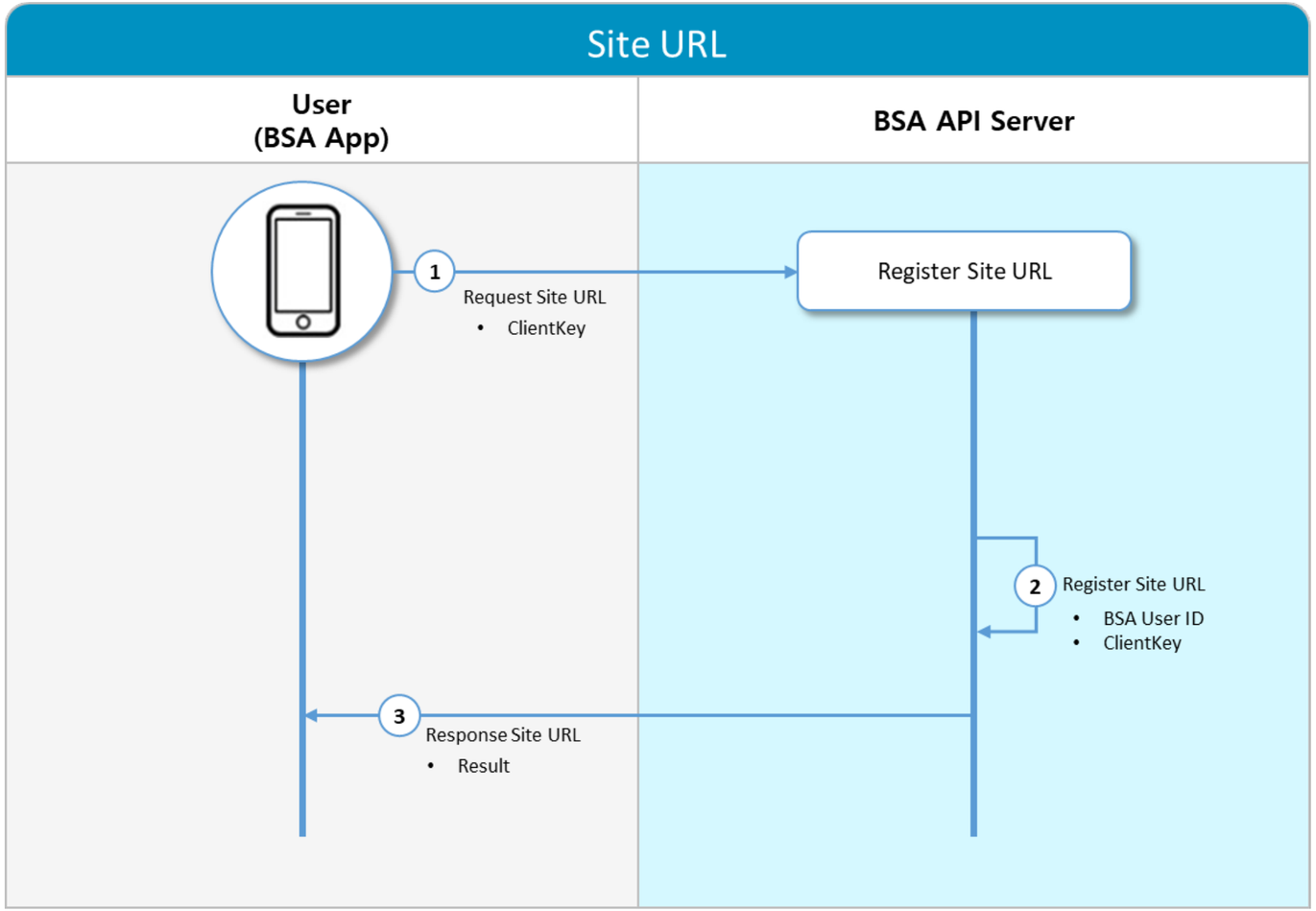
Choose authentication method

Register chosen authentication method

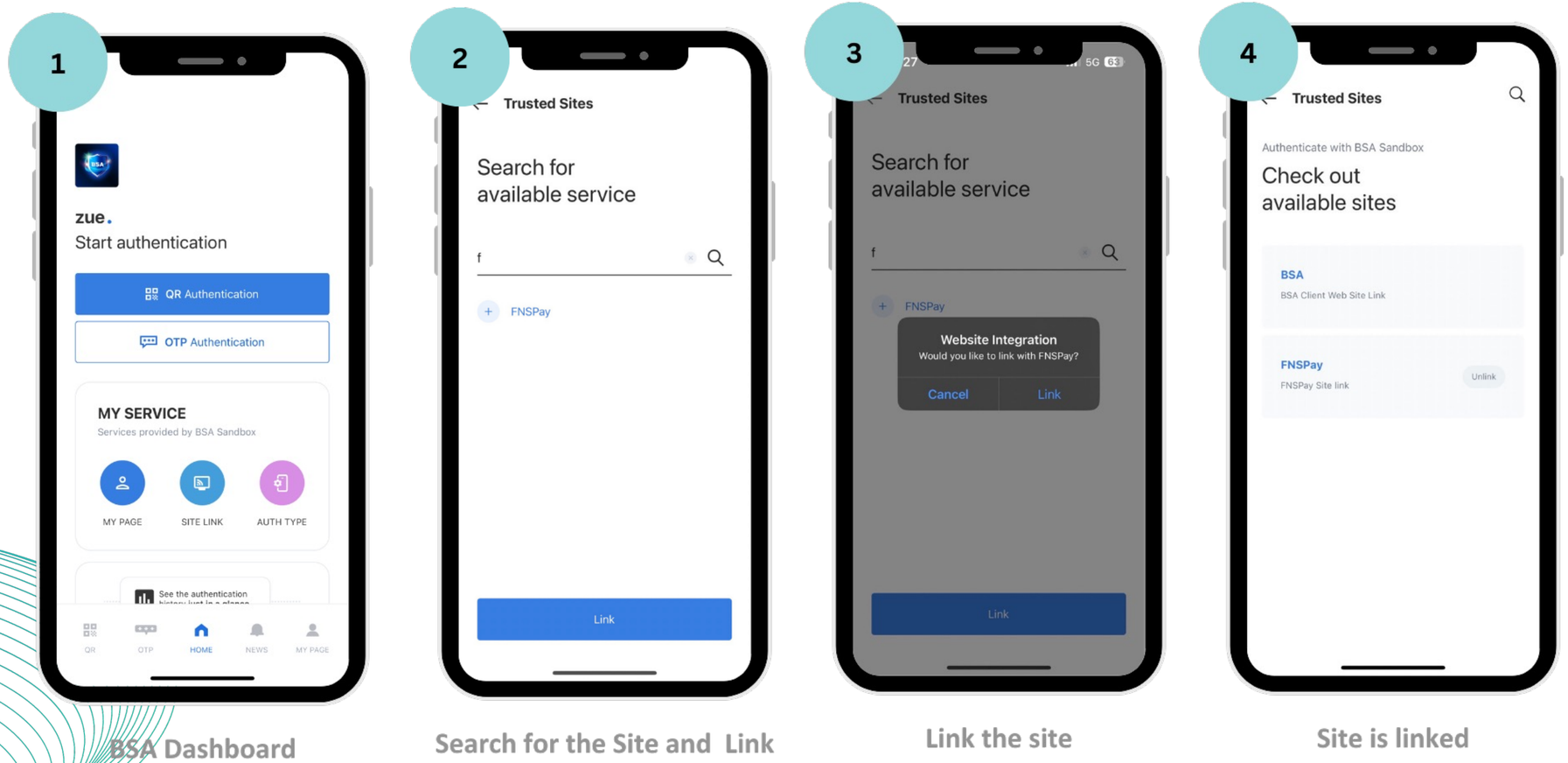
Completed

BSA Dashboard

BSA Site Link



BSA Demo : Site Link



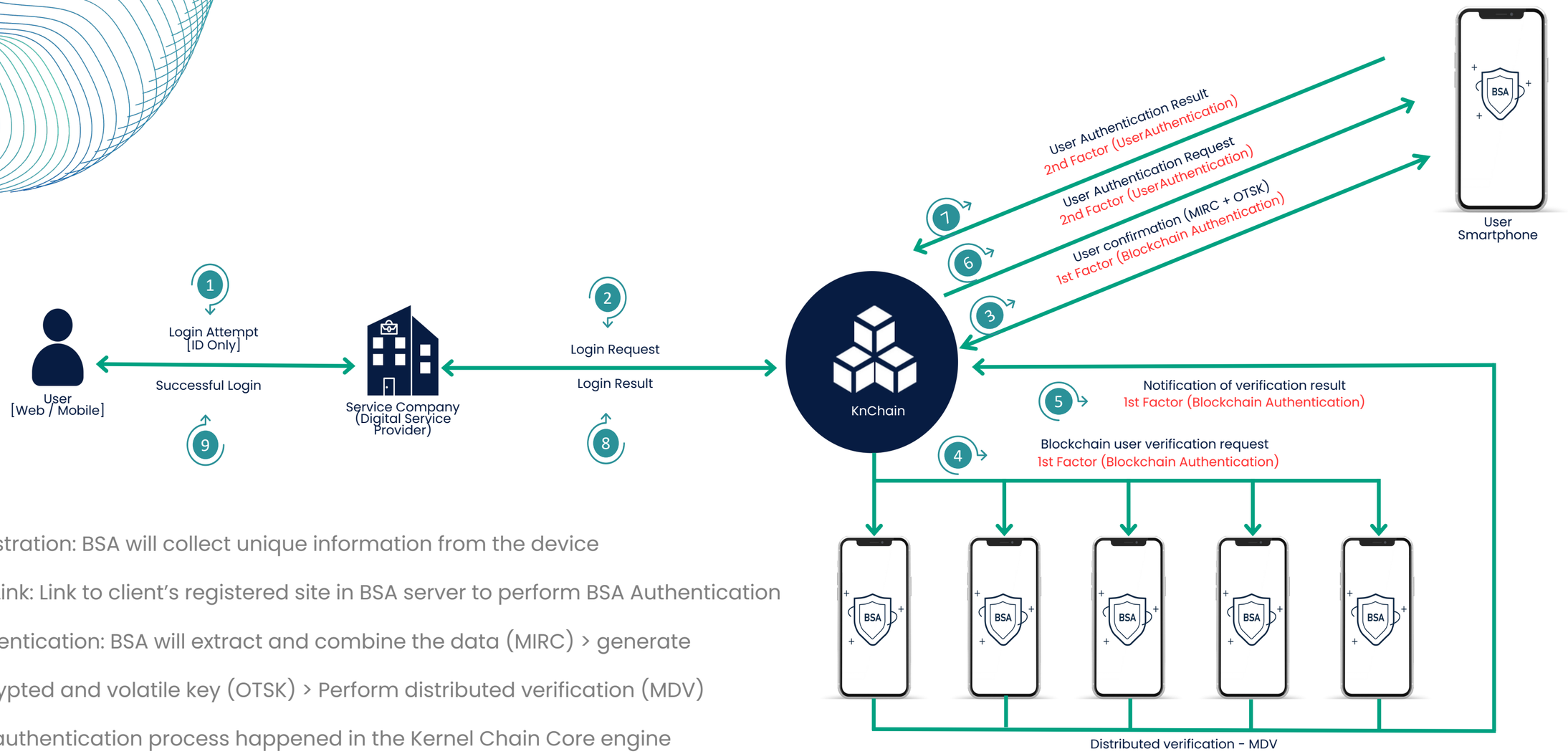
BSA Dashboard

Search for the Site and Link

Link the site

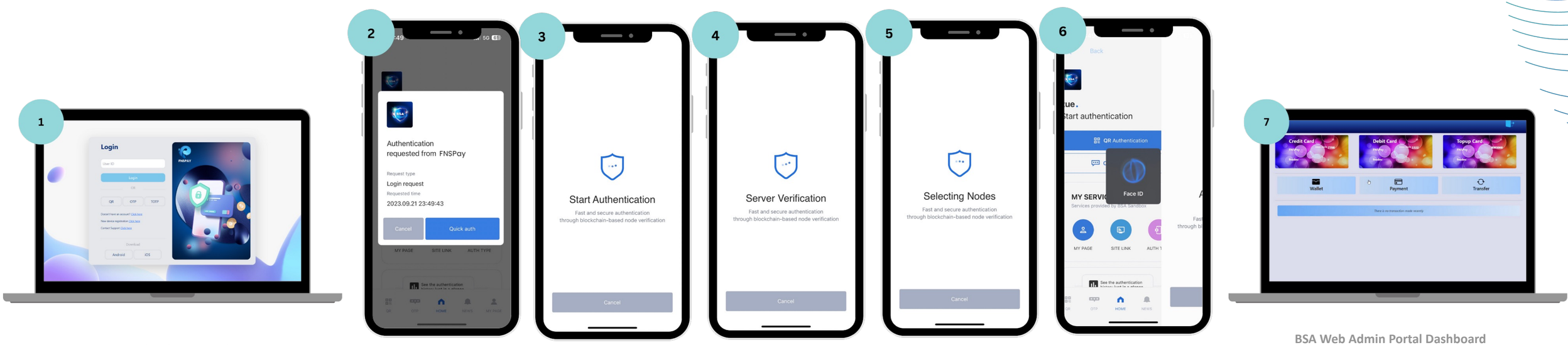
Site is linked

BSA Login Authentication



- Registration: BSA will collect unique information from the device
- Site Link: Link to client's registered site in BSA server to perform BSA Authentication
- Authentication: BSA will extract and combine the data (MIRC) > generate encrypted and volatile key (OTSK) > Perform distributed verification (MDV)
- The authentication process happened in the Kernel Chain Core engine

BSA Demo : Login Authentication



BSA Web Admin Portal (Browser)

Authentication Request Notification

Start Authentication

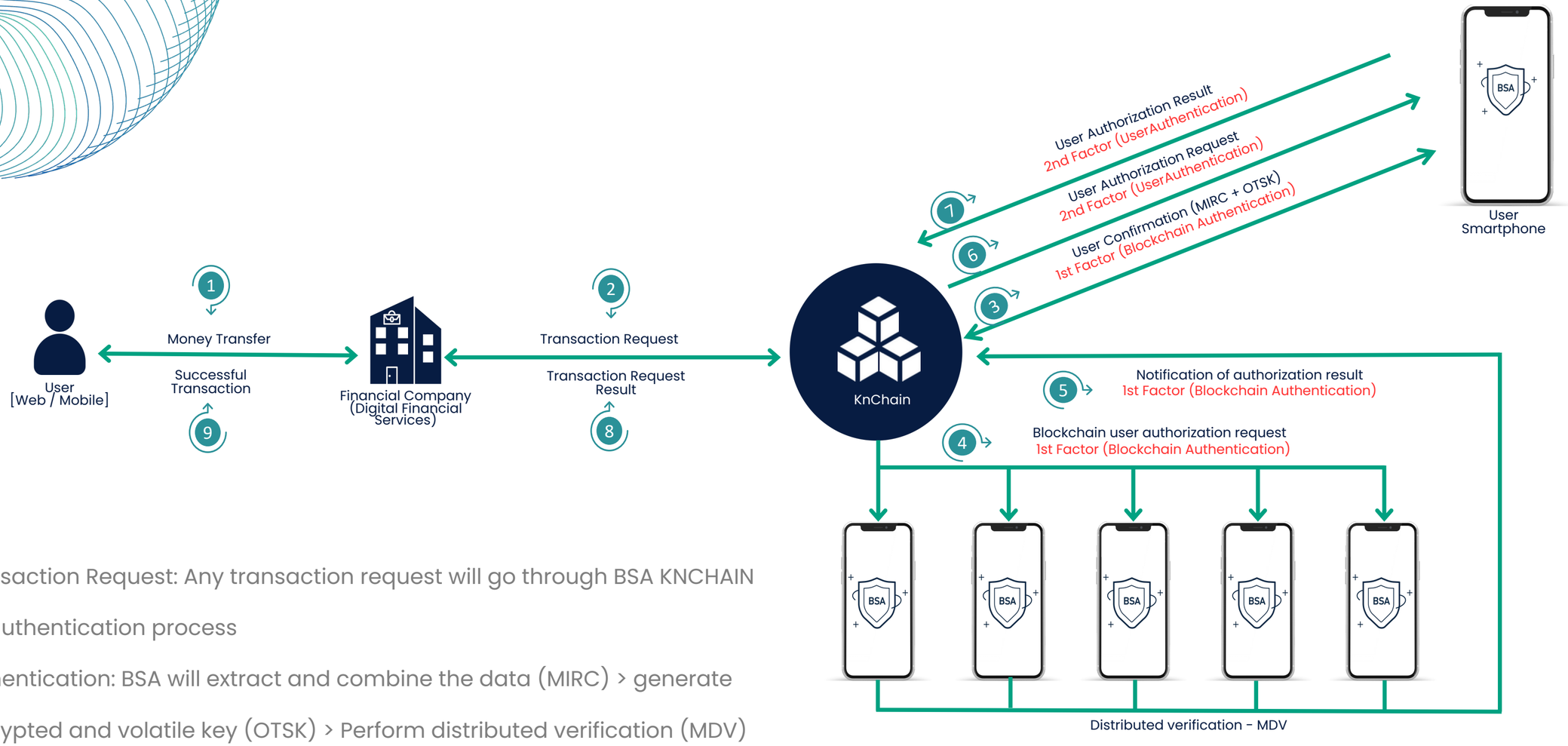
Server Verification

Selecting Nodes (Node Verification)

Face Recognition (Biometrics Authentication)

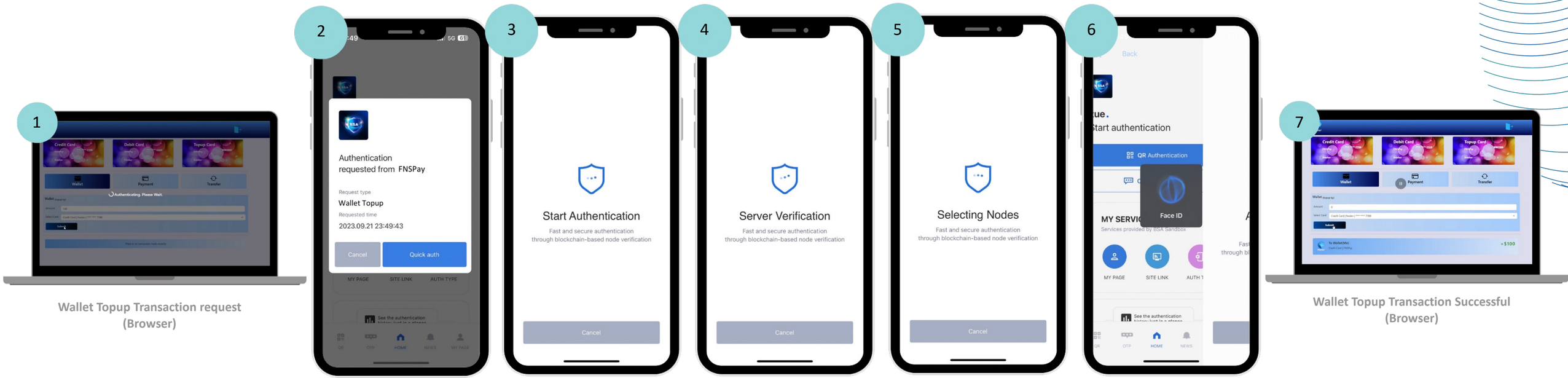
BSA Web Admin Portal Dashboard (Browser)

BSA Transaction Authorization



- Transaction Request: Any transaction request will go through BSA KNCHAIN for authentication process
- Authentication: BSA will extract and combine the data (MIRC) > generate encrypted and volatile key (OTSK) > Perform distributed verification (MDV)

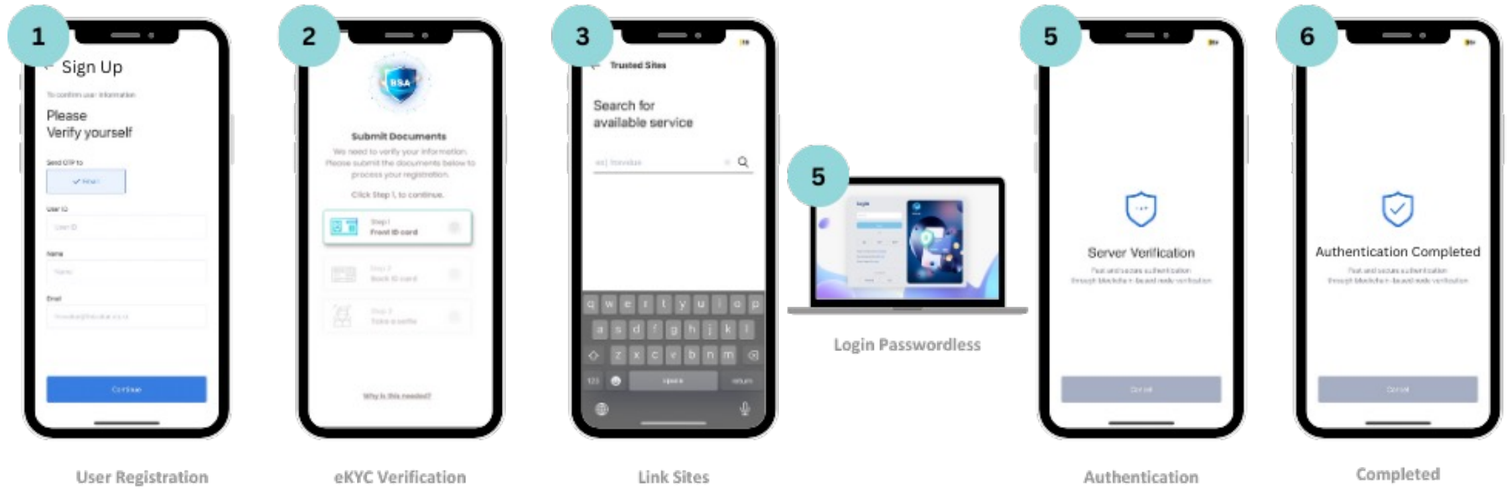
BSA Demo : Transaction Authorization



BSA Implementation in DFS

Financial Applications, transaction and payment confirmation

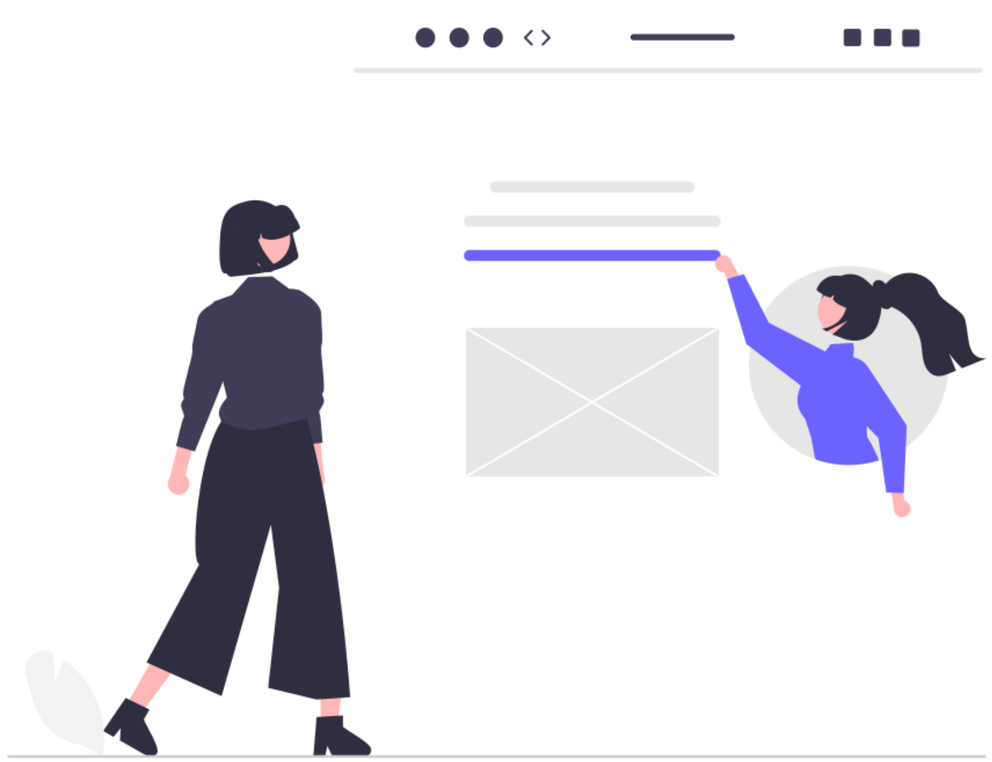
- **Registration:** BSA integrated with eKYC for paperless registration and to verify customer's identity and create digital ID
- **Site Link:** To link any financial web services that is integrated with BSA
- Login Passwordless in WebAuth or transaction verification in mobile
- **Authentication:** Use BSA kernel chain core (incl. MIRC, OTSK, MDV) to verify and authorize any of the login, transaction and payment process



BSA SANDBOX

BSA Sandbox Objective

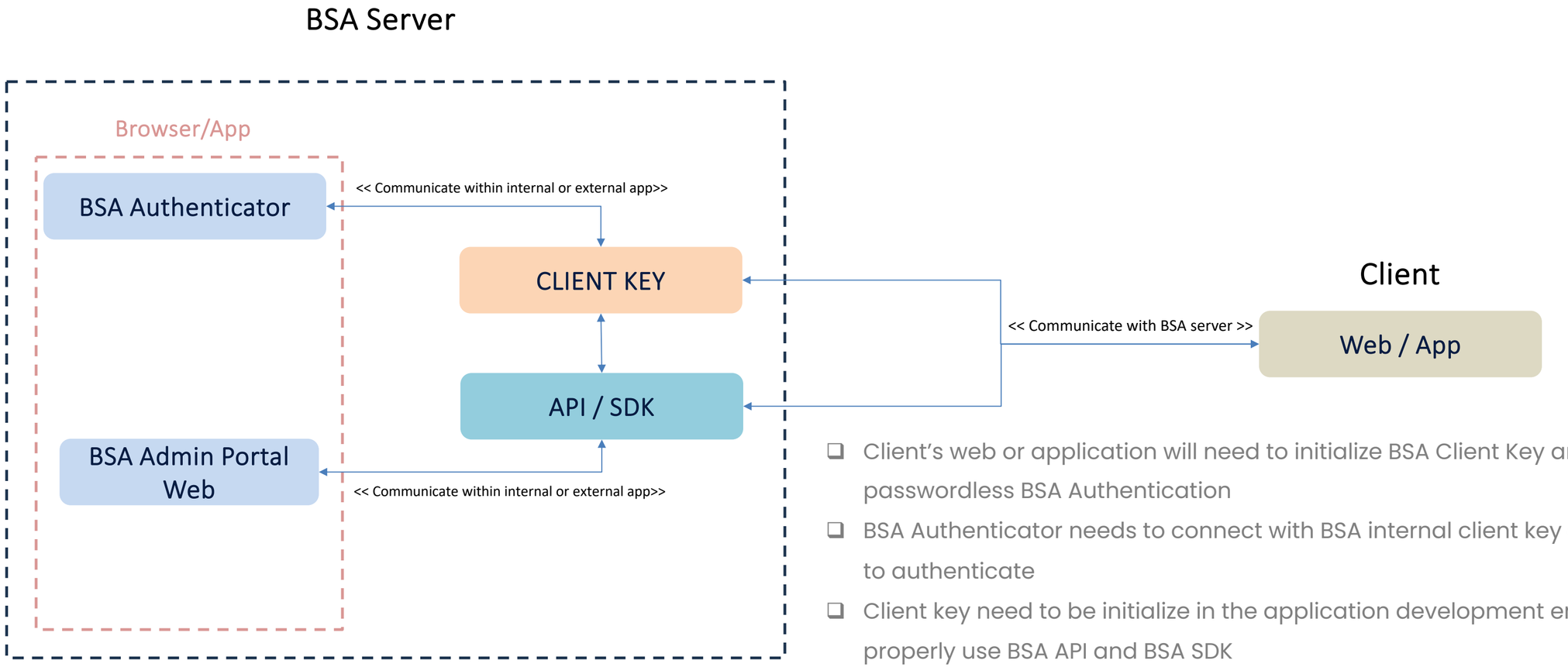
- ✓ BSA Sandbox will be used for any of ITU activity:
  - ❖ ITU Workshops
  - ❖ ITU Application Challenges
  - ❖ Test environment for regulators, developers, academia for application with BSA



BSA Sandbox Entities

- **BSA Authenticator:** Mobile App integrated with BSA SDK – to register and authenticate using KNCHAIN (Hybrid Blockchain) technology
- **Client:** Web App or client's application integrated with BSA API to send auth request to BSA Authenticator
- **BSA Server:** Contains BSA API (incl. KNCHAIN) to register and verify user request / transaction
- **BSA Client Key:** Used to create communication channel between BSA Authenticator and BSA Client

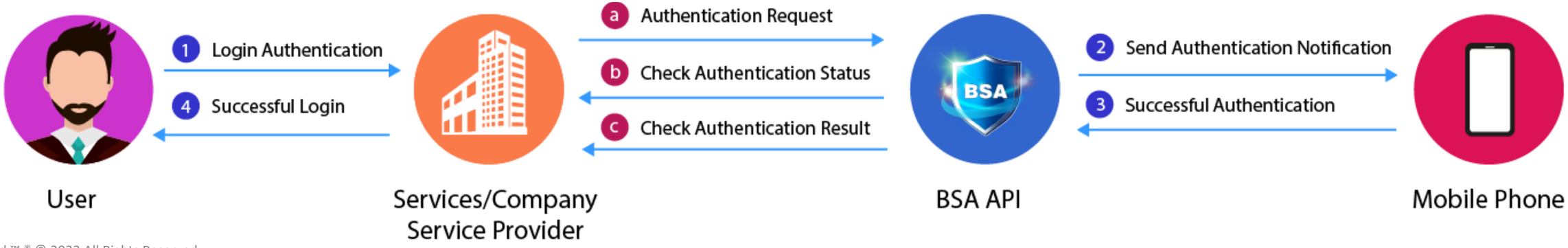
BSA Sandbox Entities Architecture



- Client's web or application will need to initialize BSA Client Key and API to use passwordless BSA Authentication
- BSA Authenticator needs to connect with BSA internal client key or client's client key to authenticate
- Client key need to be initialize in the application development environment to properly use BSA API and BSA SDK

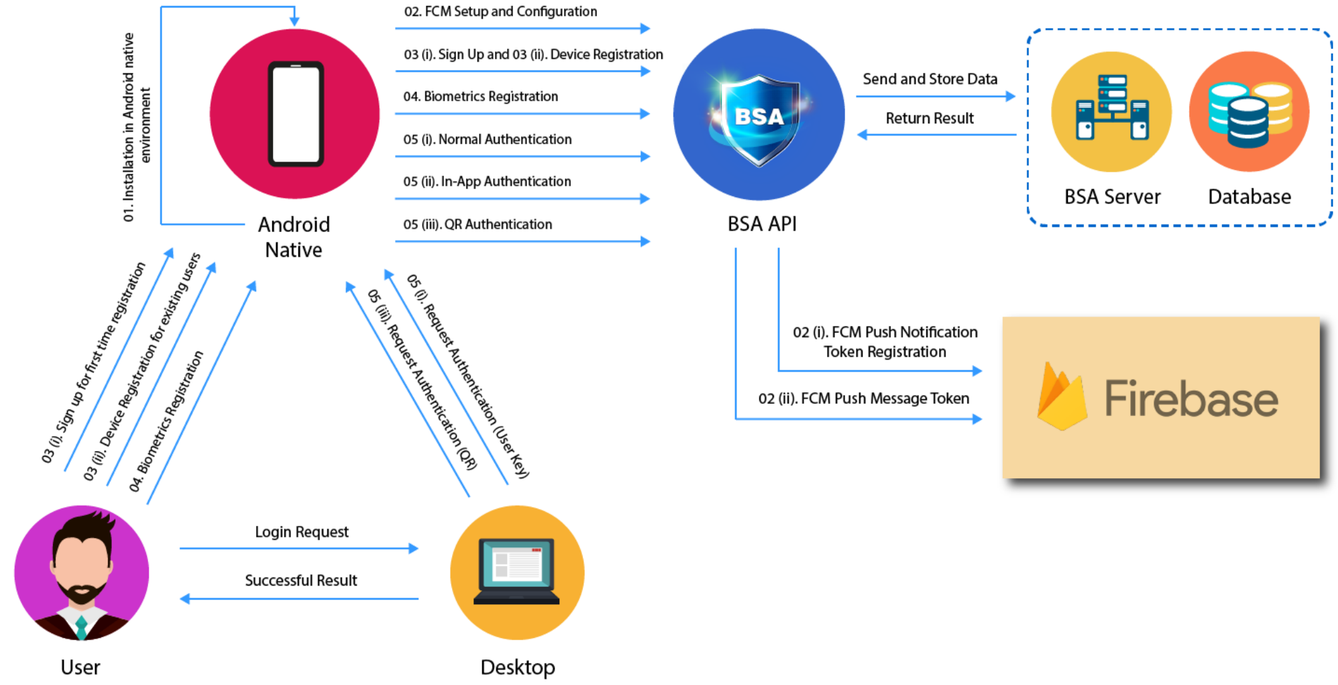
BSA Sandbox WEB Component

- **Web Functions: (a)**Authentication request, **(b)** check authentication status, **(c)** check authentication status
- **Web Protocols:** REST API
- **Web Transports:** HTTPS, WebSocket
- **Security Mechanism:** Client Key



BSA Sandbox SDK (aOS, iOS) Component

- **App Module:** BSA SDK Dependencies
- **App Functions:** Sign up, device register, biometrics registration, request authentication, in-app authentication, normal authentication, QR authentication, OTP authentication, TOTP authentication, Site link
- **App Notification:** Firebase Cloud Messaging (FCM)
- **Security Mechanism:** Client Key, FCM Key



THANK YOU!

Scan here to access

www.fnsbsa.com