Deep Dive on Blockchain Secure Authentication (BSA) and deployment for Passwordless Authentication for Digital Financial Services (DFS)

Nurzulaikha Binti Zulkifli

FNS(M) Sdn Bhd

Cybersecurity Threatscape of African Countries 2022 – 2023

There are **4 critical areas on access security** that impact directly on organizations **State of Access Security**:

Source: Positive Technologies

1 No Cybersecurity Protocols

- According to African Business, there are about 90% of African Business conducted business without cybersecurity protocols.
- About 78% IT department heads believe that they are not ready to fend-off cyber attacks.

2 Financial sector is the main target

In the year of 2022 until the beginning year 0f 2023, with the total of 68% of successful attacks finance sector became the primary victim of cyber attacks and telco fall in to second place of the attacks.

3 Perception and Beliefs

35% - Completely secure

53% - Mostly secure

12% - Somewhat secure

Majority of IT and security leaders believes their organization to be completely or mostly secured.

4 True Passwordless Authentication

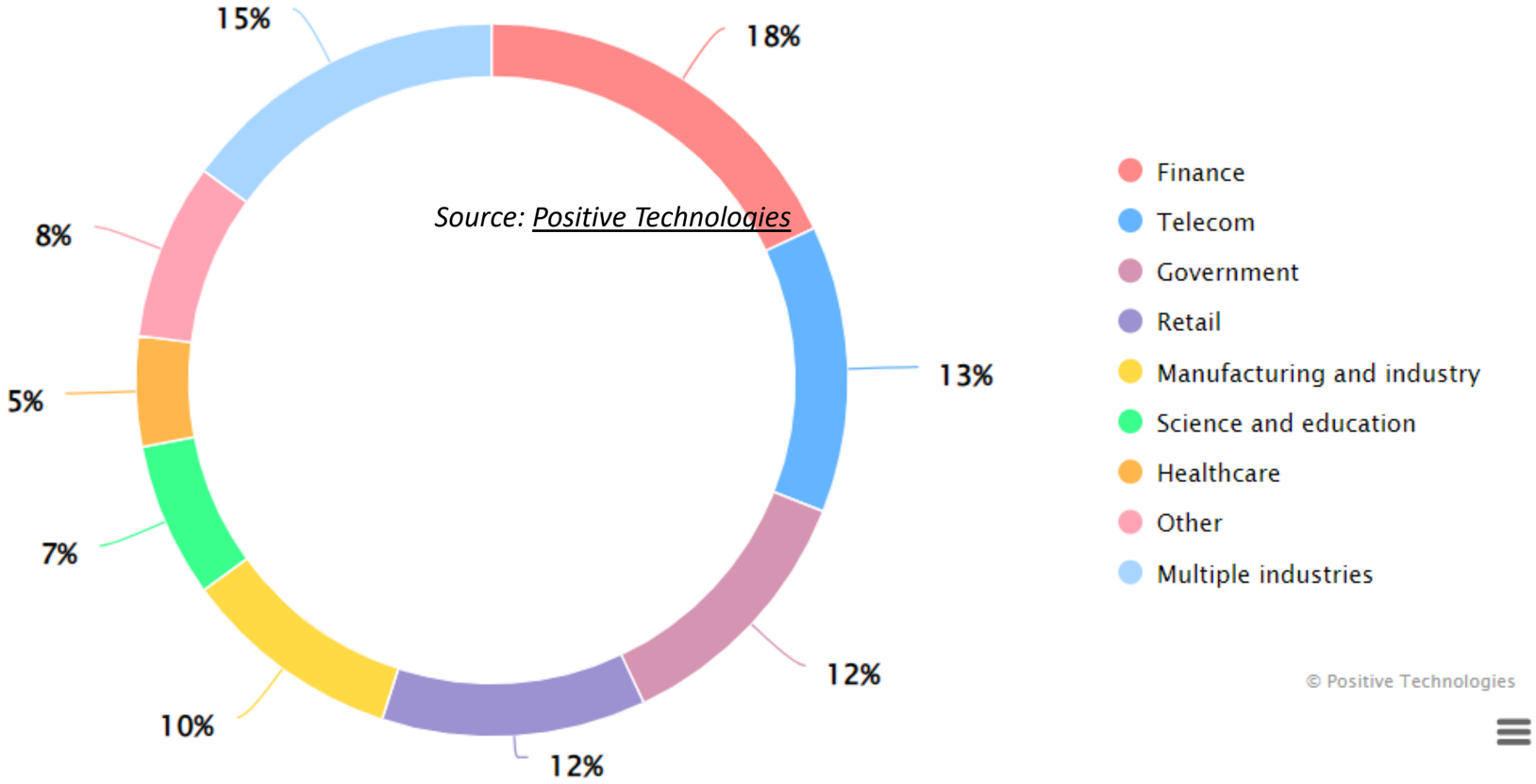
97% of ‘passwordless’ solutions deployed are susceptible to **phishing** and **push attacks.**

A True Passwordless Authentication enhances security layers without requiring a centralized based primary security key or a 'Master' key.

Cybersecurity threatscape of African countries 2022–2023

The main targets of attackers

1. Financial sector (18% of attacks on organizations),
2. Telecommunications companies (13%),
3. Government agencies (12%)
4. Organizations from the trade (12%)
5. Industrial (10%) sectors.



Source: Positive Technologies

Figure 1. Categories of victim organizations

Source: Positive Technologies

Cybersecurity threatscape of African countries 2022–2023

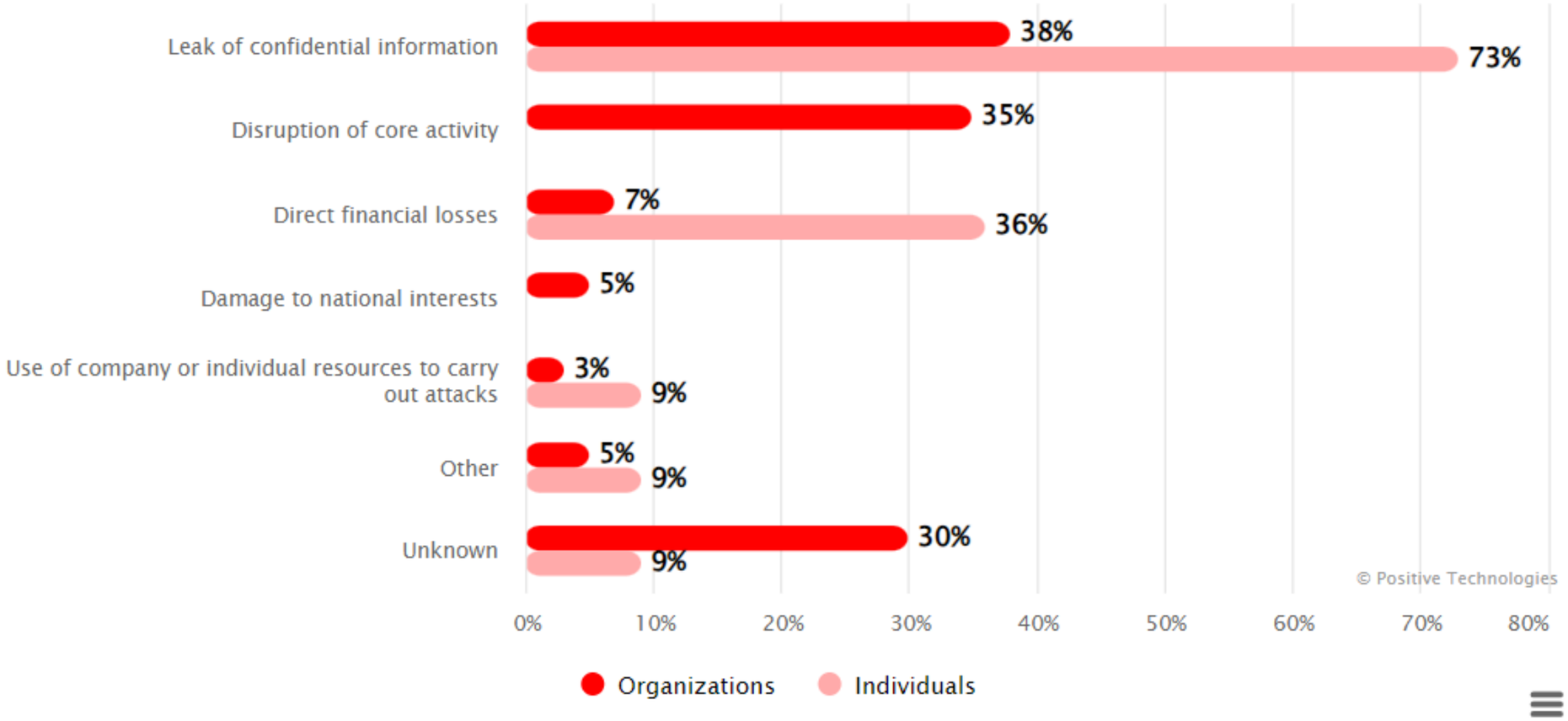


Figure 2. Consequences of attacks (percentage of successful attacks)

The consequences of attacks

1. To obtain confidential information (38%)
2. Criminal actions that caused disruptions (35%)
3. Direct financial losses (7%)

Source: Positive Technologies

Hackers is targeting cloud environment

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 critical for Cloud Access Security

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%

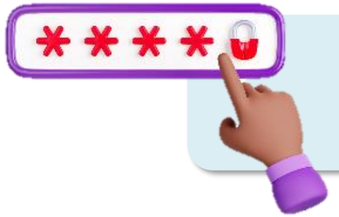
In **67%** of cloud security incidents, CrowdStrike found identity and access management roles with elevated privileges beyond what was required – indicating an adversary may have subverted the role to compromise the environment and move laterally

47%

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

How effective are the current identity and access security measures?

The challenges and limitations of the existing access security controls:



Passwords are easy to forget, steal, or hack.

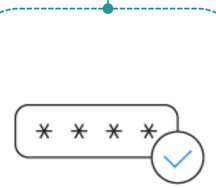
Multi-factor authentication (MFA) adds complexity and inconvenience for users. Devices can be stolen.

Biometrics can be spoofed or compromised. Deep Fake.

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

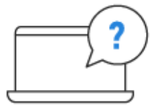
The Evolution of Authentication System

1st Generation



Password

2nd Generation



SMS OTP

OTP

TOTP

HOTP

SOTP

3rd Generation

PKI

MFA

Biometrics

Biometric Authentication - 2FA (Face, Fingerprint)

Multi-Factor Authentication - MFA (PKI, Biometric, Token)

Centralized Depository – Master Key, Password or Passwordless

4th Generation

DLT
Blockchain MFA
True Passwordless

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

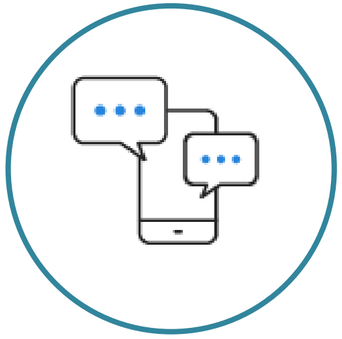
Challenges in Multifactor Authentication (MFA)

Single Factor Authentication

1FA: User ID and Password

Challenges: Human Error, Too many passwords

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

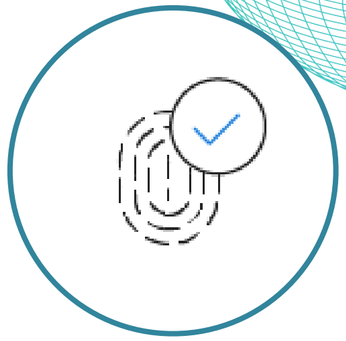


MFA – PKI / Token

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

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

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



MFA – Device/OTP/Biometrics

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

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

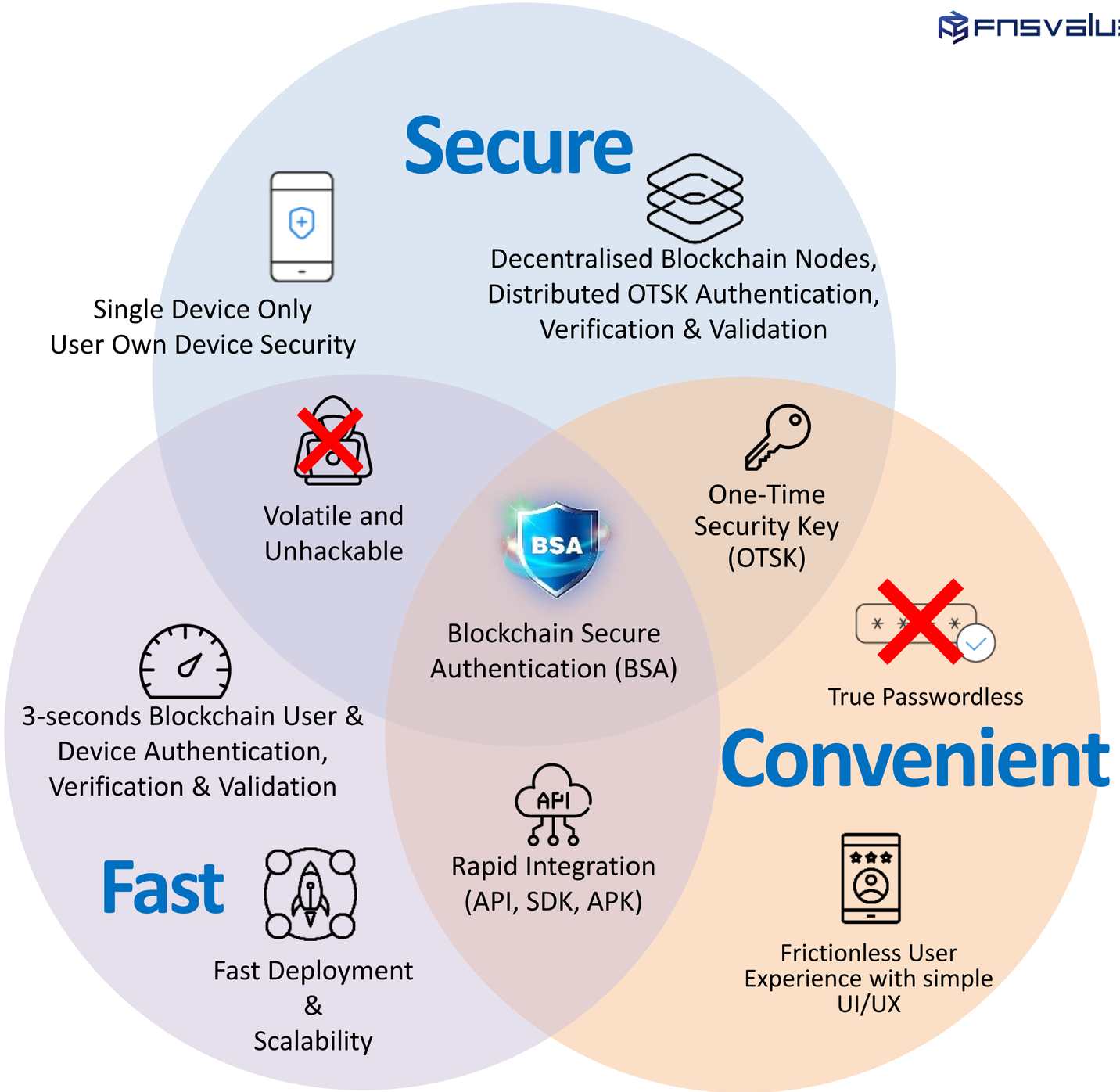
Known Attacks:
Compromised assets and devices

What is Blockchain Secure Authentication (BSA)?

- BSA is a 4th generation authentication system – **Passwordless Blockchain Based Multifactor Authentication** for secure identity and access management
- BSA used hybrid blockchain technology with distributed verification to create a secure, fast and convenient 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, privacy and trust by design

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.

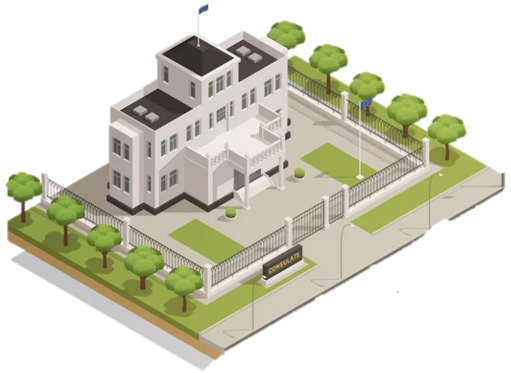


BSA is ready for Web 3.0 Digital Access Security

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 – Kernel Chain Core (KNCHAIN)

BSA core engine - Hybrid (Public and Private) blockchain technology

2 – Multiple Identifier Random Combination (MIRC)

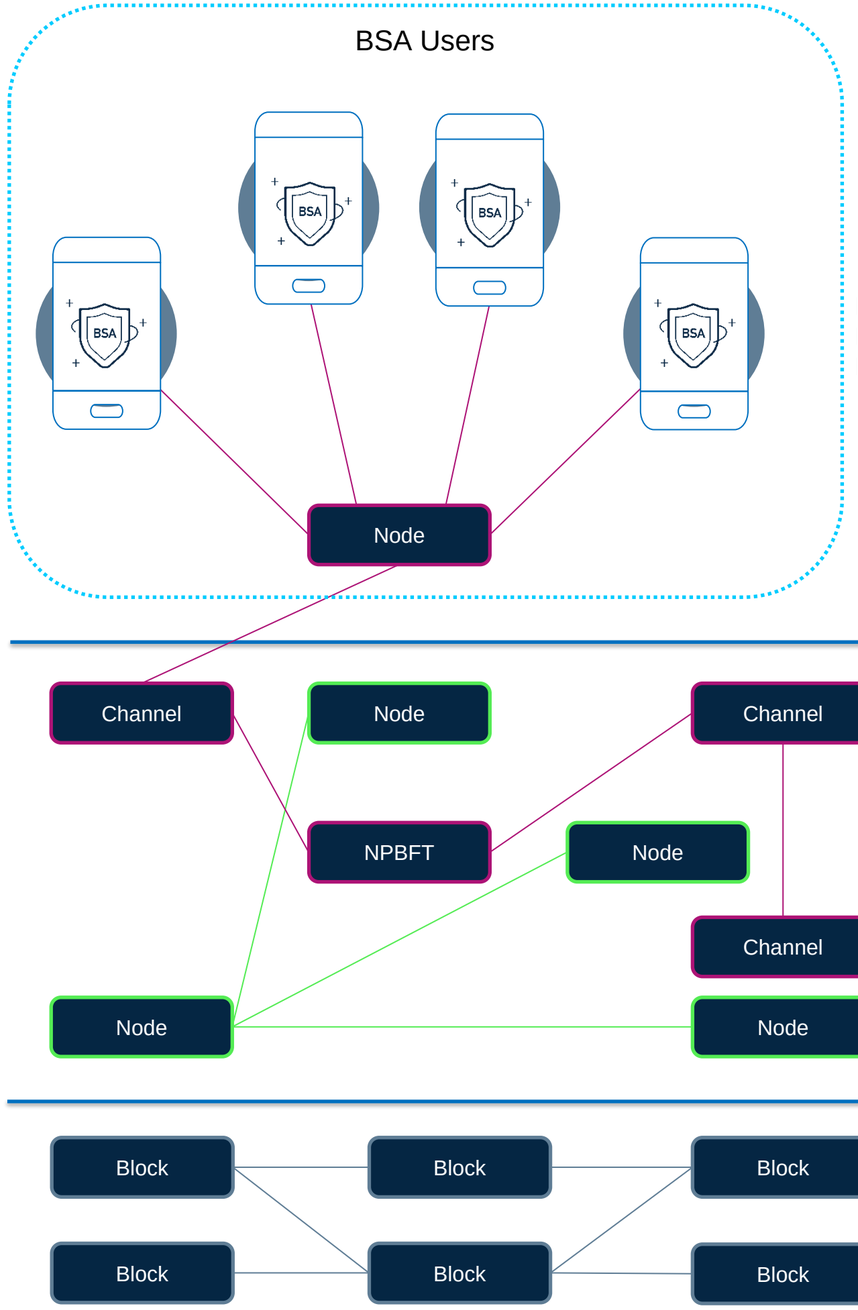
Extract and combine unique identifiers from data collected in user's mobile device

3 – One Time Security Key (OTSK)

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

4 – Multilateral Distributed Verification (MDV)

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



BSA Technology – KNCHAIN

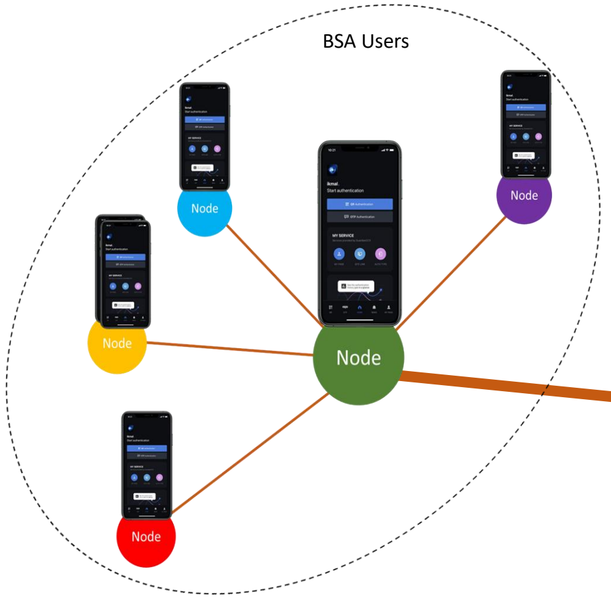
KNChain

MIRC

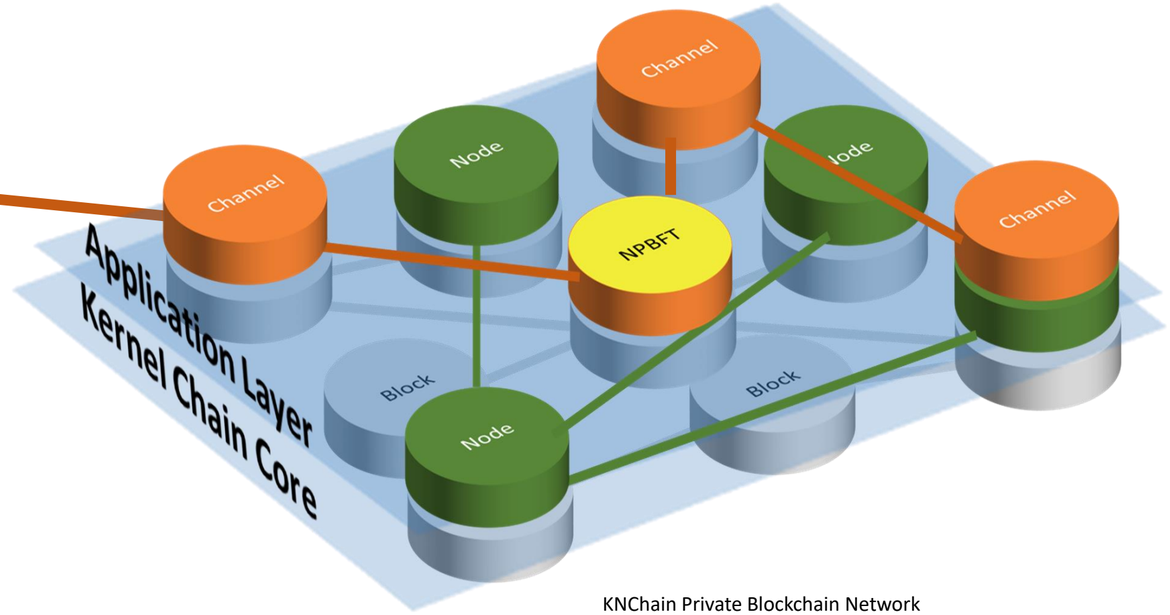
OTSK

MDV

Kernel Chain – Hybrid Blockchain



KNChain Public Blockchain Network

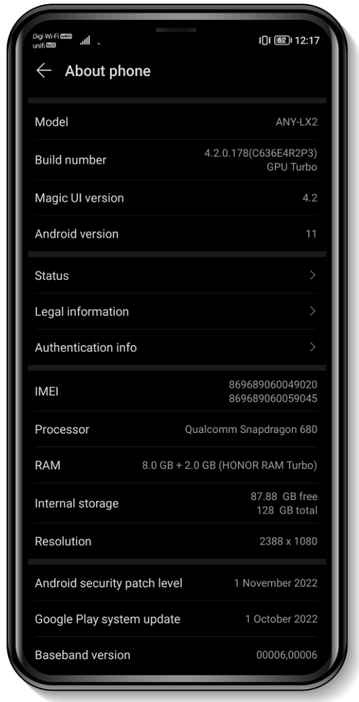


KNChain Private Blockchain Network

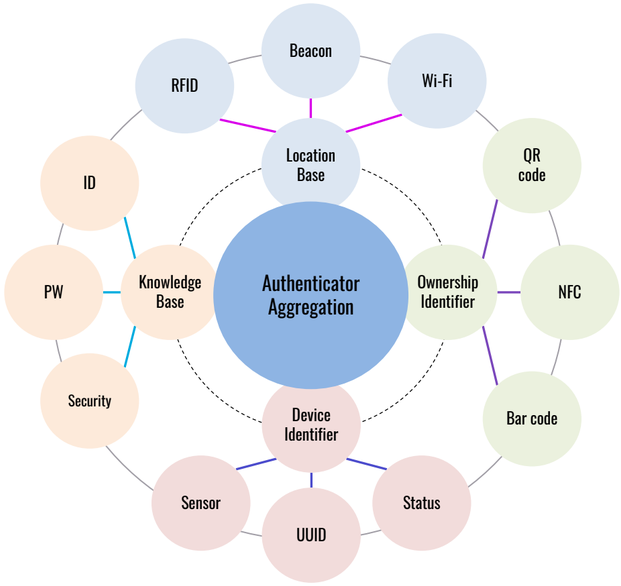
BSA Technology - MIRC

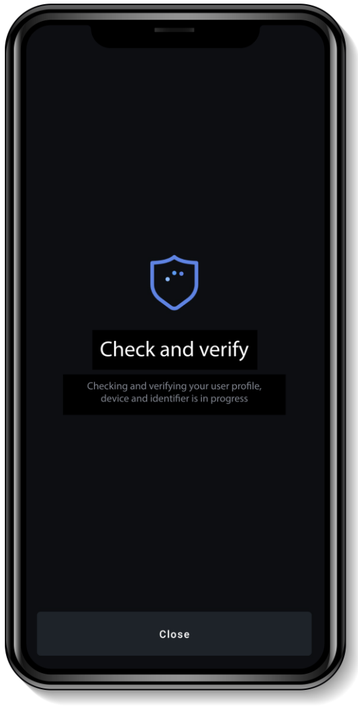
KNChain | MIRC | OTSK | MDV

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

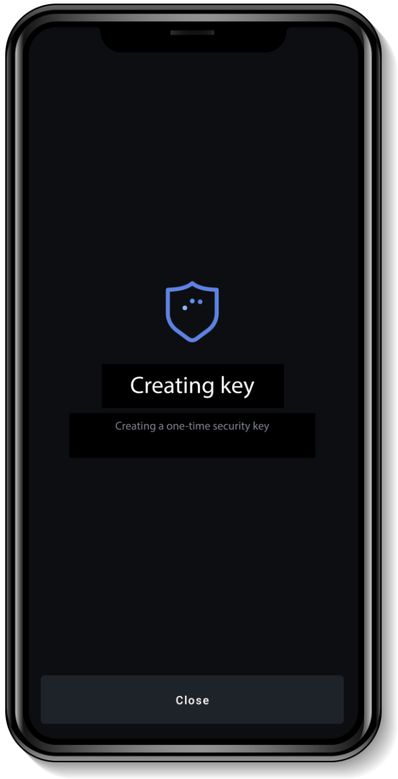




Gathering authentication elements using information values for each device

BSA Technology - OTSK

KNChain | MIRC | OTSK | MDV



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

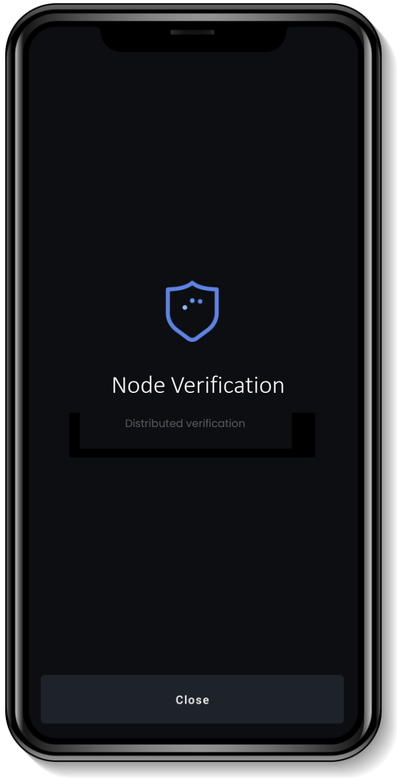
Merging the encrypted security keys generated at STEP 02 and STEP 04

STEP 06

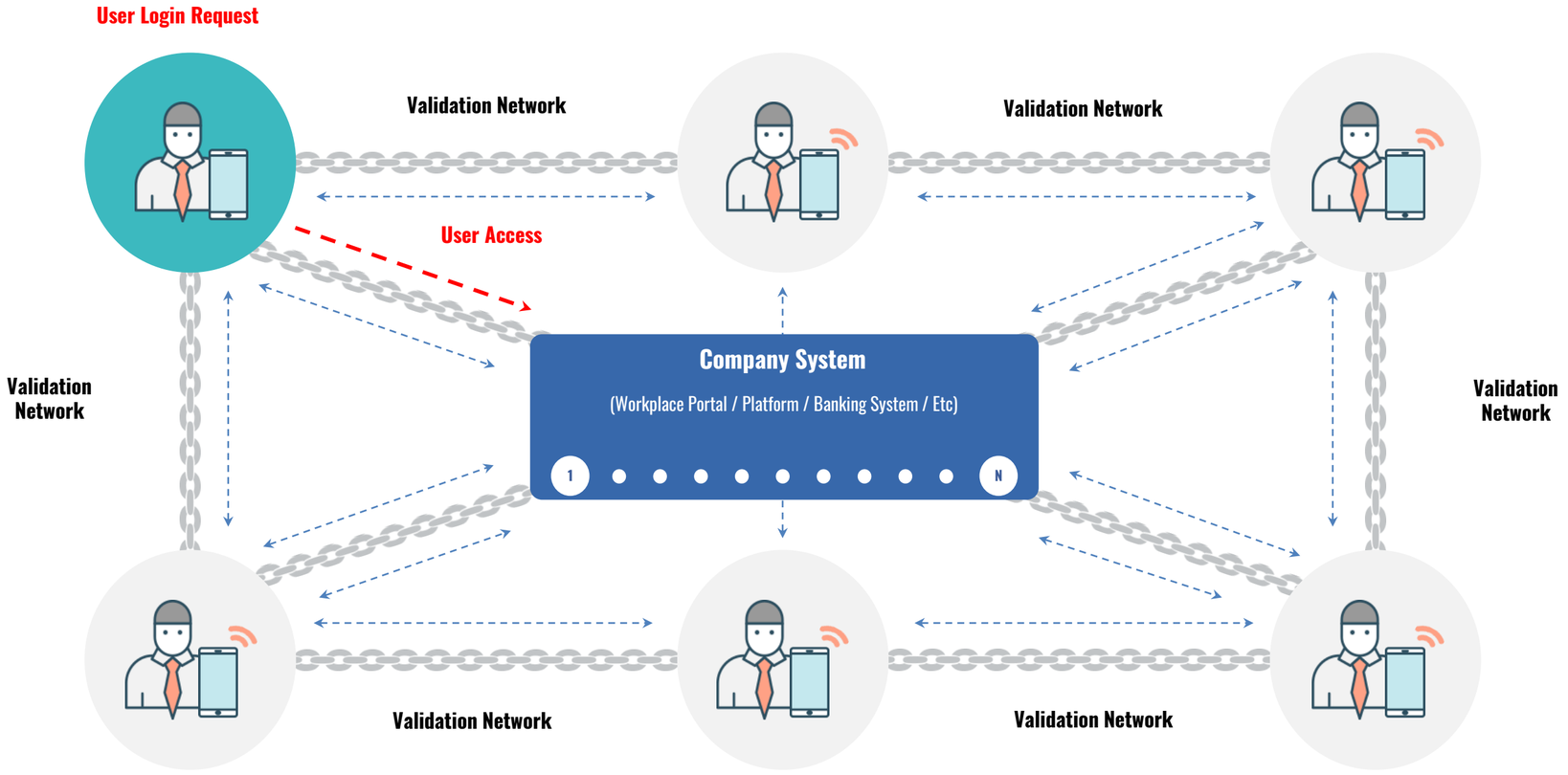
Re-encryption of the security key merged at STEP 05

BSA Technology - MDV

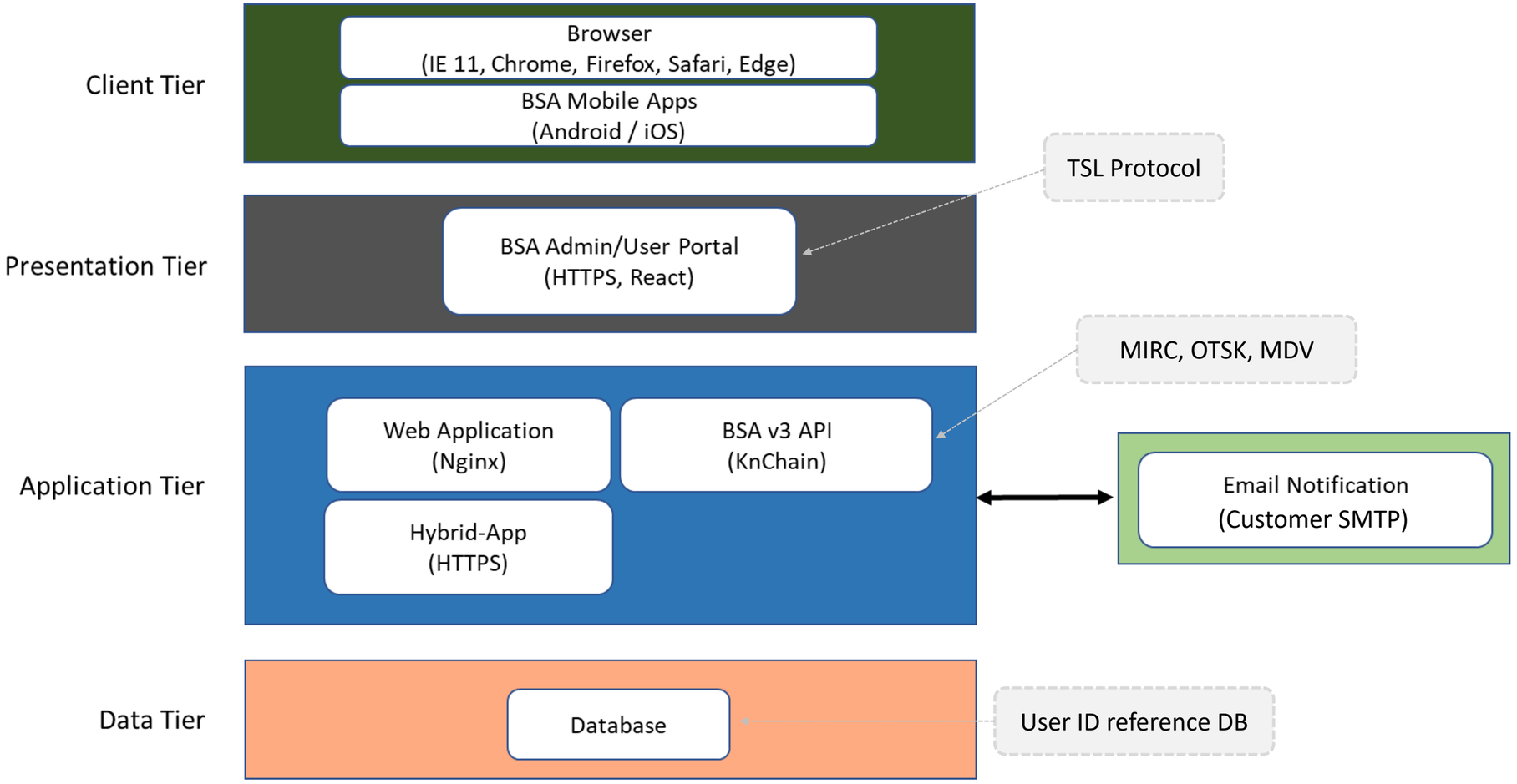
KNChain | MIRC | OTSK | MDV



Multilateral Distributed Verification (MDV)



BSA Architecture for On-Premise / On-Cloud

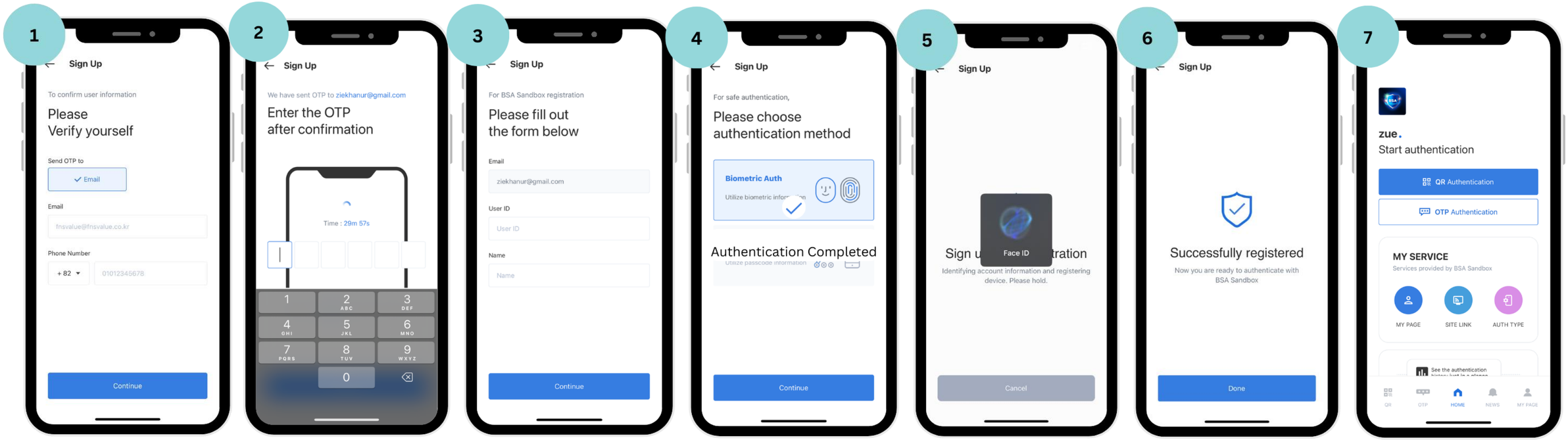


BSA Entities

- **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


Anytime ·

BSA Demo : User Registration/Onboarding (Sign Up)



Key-in email and phone number

Email OTP verification (only registration)

Key-in user name and name

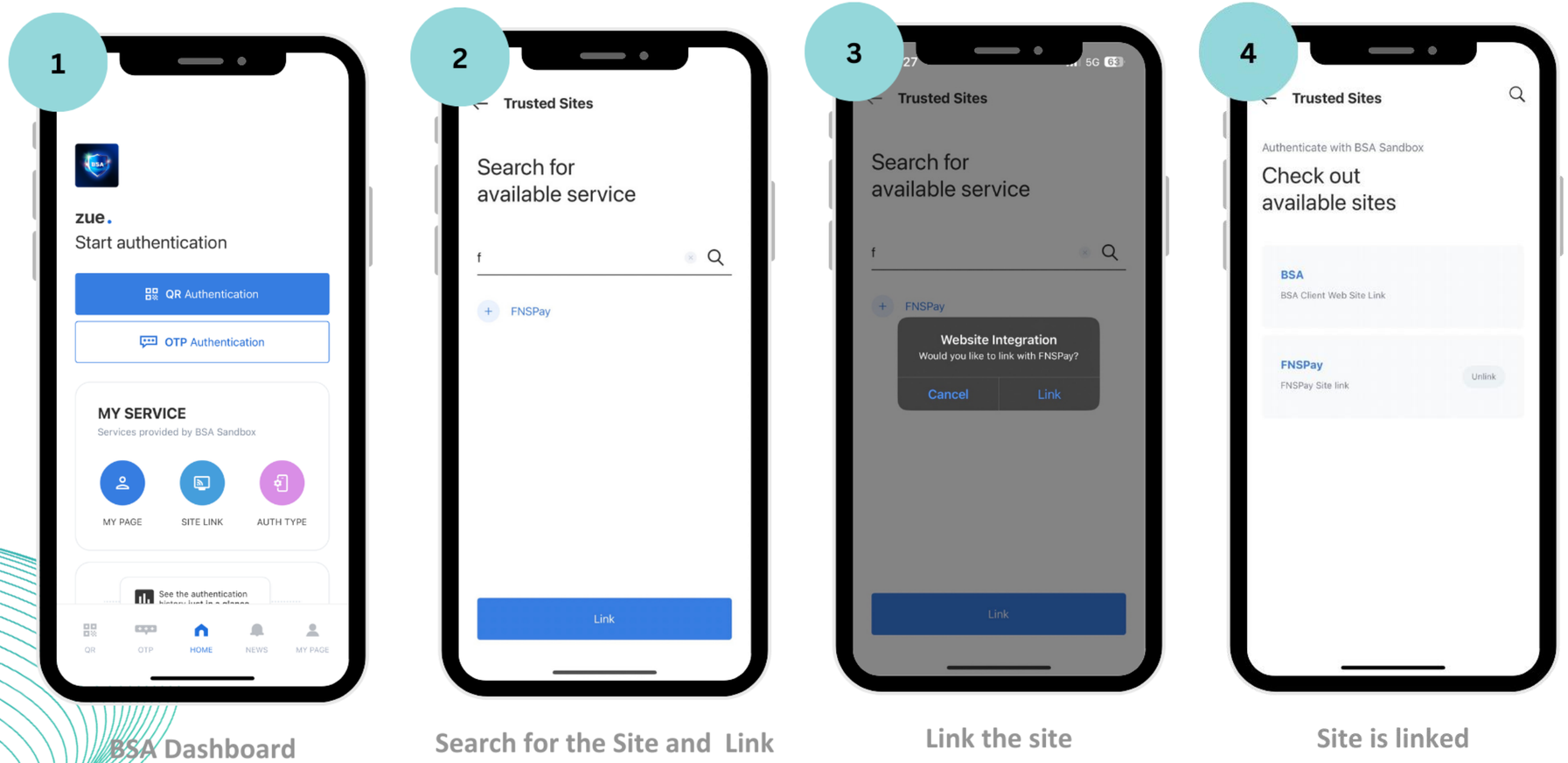
Choose authentication method

Register chosen authentication method

Completed

BSA Dashboard

BSA Demo : Authorized BSA Application (Site Link)



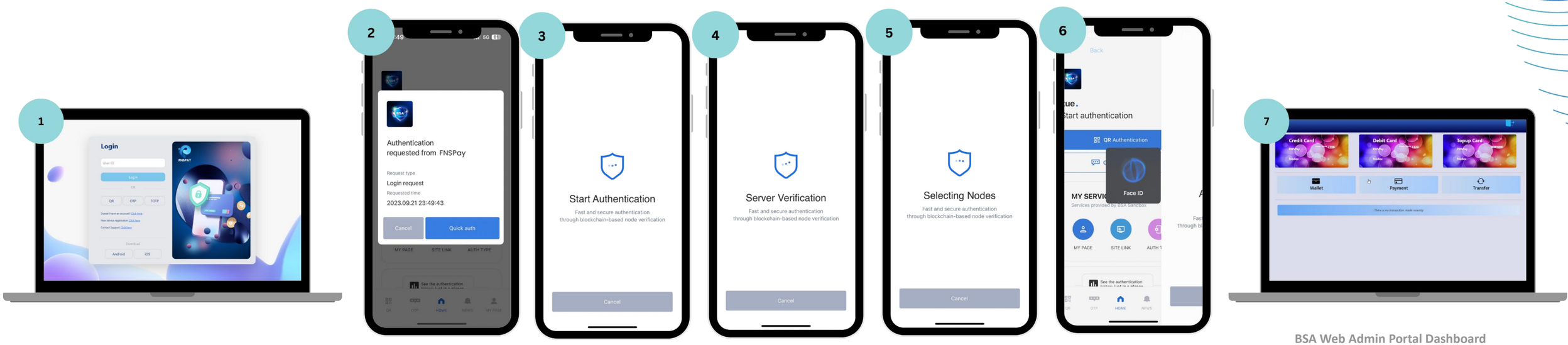
BSA Dashboard

Search for the Site and Link

Link the site

Site is linked

BSA Demo : Login Authentication (Web Banking App)



BSA Web Admin Portal (Browser)

Authentication Request Notification

Start Authentication

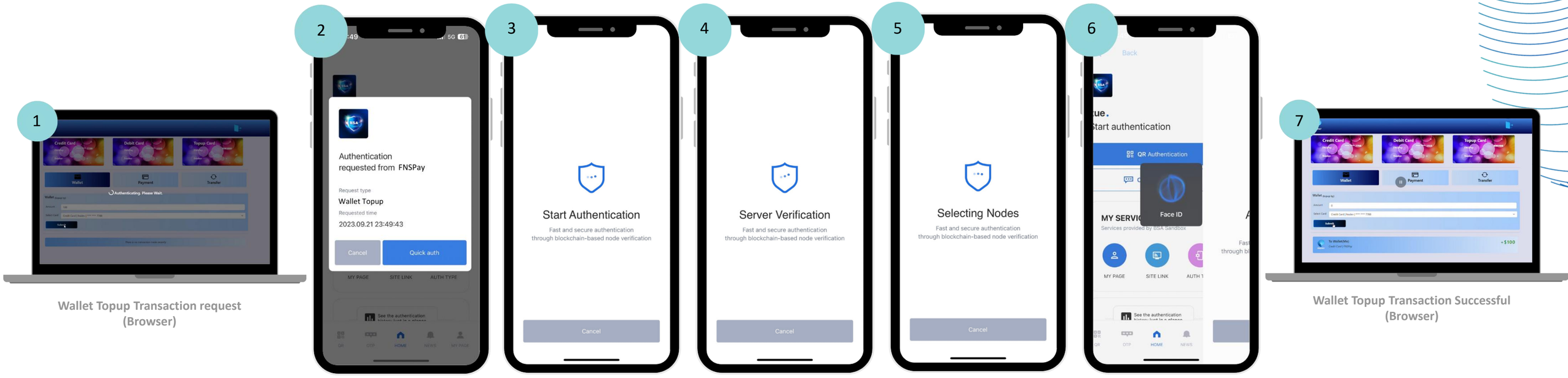
Server Verification

Selecting Nodes (Node Verification)

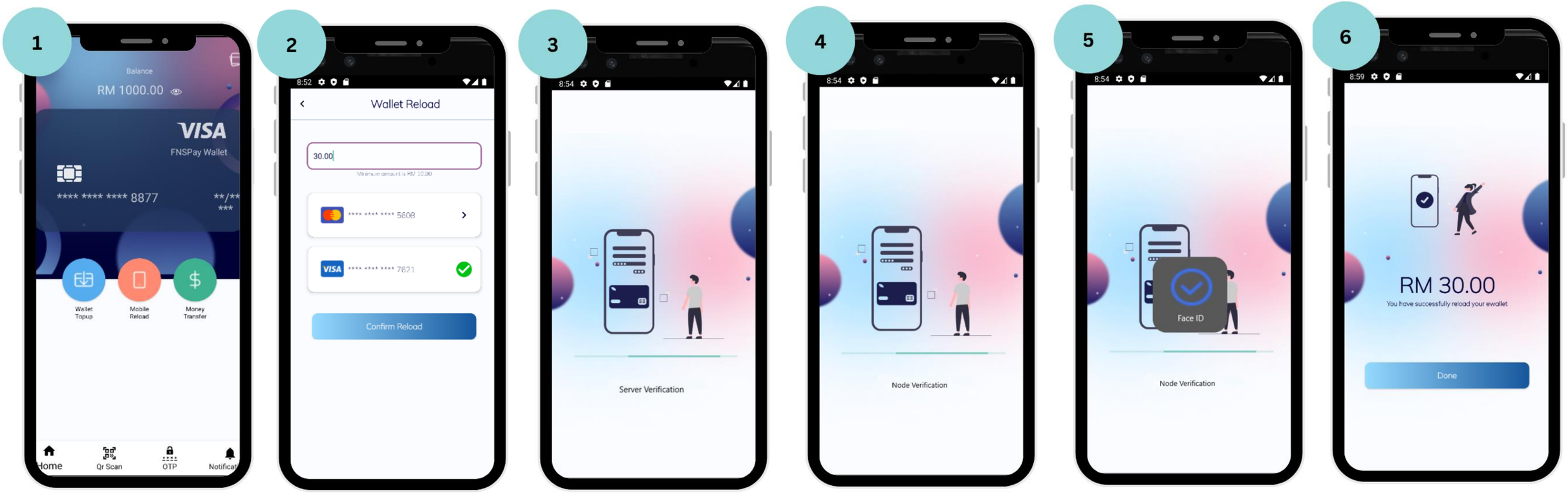
Face Recognition (Biometrics Authentication)

BSA Web Admin Portal Dashboard (Browser)

BSA Demo : Transaction Authorization (Web Banking App)

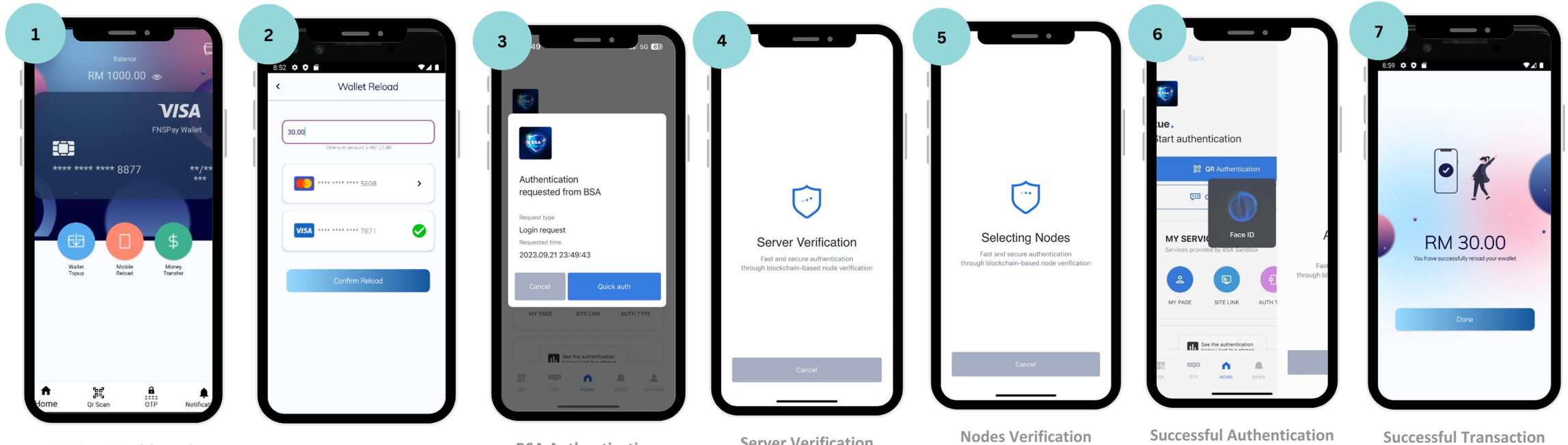


BSA Demo : Transaction Authorization (Mobile Banking App – One Mobile Native App)



FNSPay Dashboard | Wallet Reload | Server Verification | Node Verification | Biometric verification | Successful Transaction

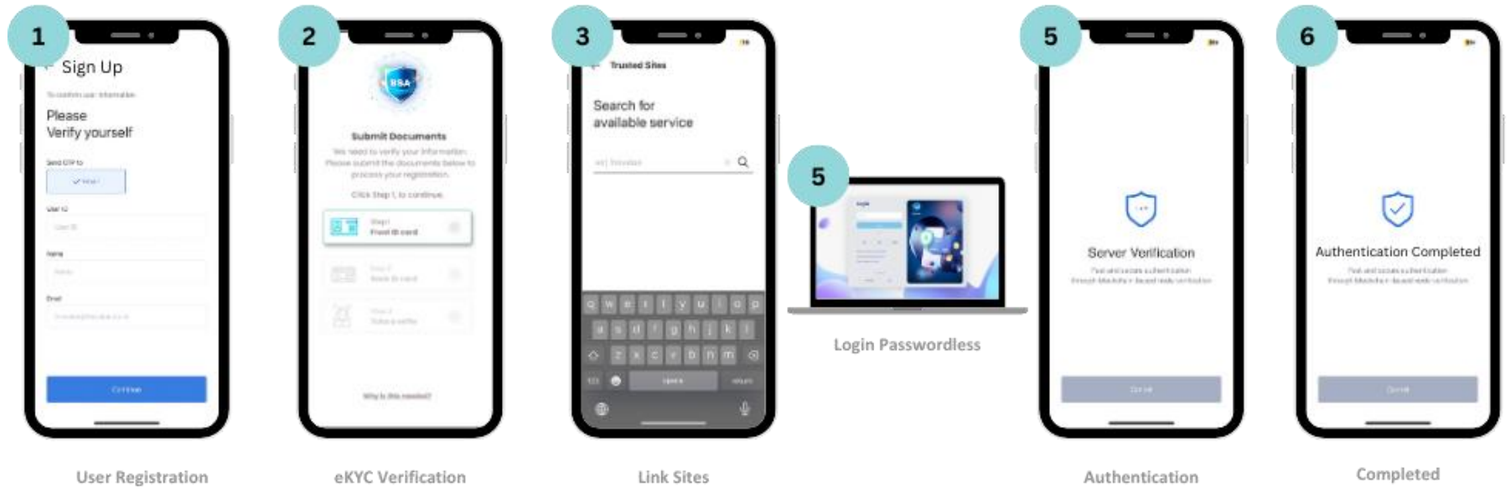
BSA Demo : Transaction Authorization (Mobile Banking App – Multiple Mobile Native App)



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



ITU and FNSV Collaboration

- ✓ FNSV is committed to support ITU to develop security best practices and technical guidelines for regulators in emerging economies to implement strong passwordless authentication technologies based on Blockchain Secure Authentication (BSA) to address the vulnerabilities associated with passwords in DFS.
- ✓ FNSV has signed a Collaboration Agreement (CA) with ITU on the 29th August 2023 for the establishment and promotion of ITU DFS BSA Sandbox. ITU DFS BSA Sandbox provides a platform for developers to test passwordless authentication based on passwordless Blockchain Secure Authentication (BSA).
- ✓ FNSV will participate in ITU DFS Security Lab and ITU DFS Security Clinic to provide guidance to DFS providers and regulators in emerging economies for the adoption of ITU security recommendations in DFS.

ITU DFS BSA Sandbox & Application Challenges

- ✓ ITU and FNSV are developing a sandbox/testbed environment for testing passwordless authentication solutions based on blockchain for mobile payments & DFS applications.
- ✓ Technical guidelines/APIs will be made available for deployment of passwordless authentication solutions based on blockchain which can be provided to developers for the activities of the sandbox and for testing the security of the authentication solutions.
- ✓ ITU will organize application challenges in 2024 using the sandbox environment.
- ✓ ITU DFS BSA Sandbox will also be available for DFS providers and regulators to assess passwordless blockchain secure authentication and verify compliance against regulations such as data protection and privacy.
- ✓ Information on how to implement the blockchain passwordless authentication solution will be included in future DFS Security Clinics organized by ITU

BSA standardization in SG 17

- ✓ SG17 has approved FNSV new standard development recommendation at Q10 for X.accsadlt: Access security authentication based on DLT and X.afotak: Authentication framework based on One-Time Authentication Key using Distributed Ledger Technology.
- ✓ On figure 1, shows Access Security Authentication based on DLT (X.accsadlt) diagram where it defines BSA architecture and how it provides a strong authentication with the elements.
- ✓ Figure 2 enumerate high level implementation of Authentication Framework One-Time Authentication Key using DLT (X.afotak)

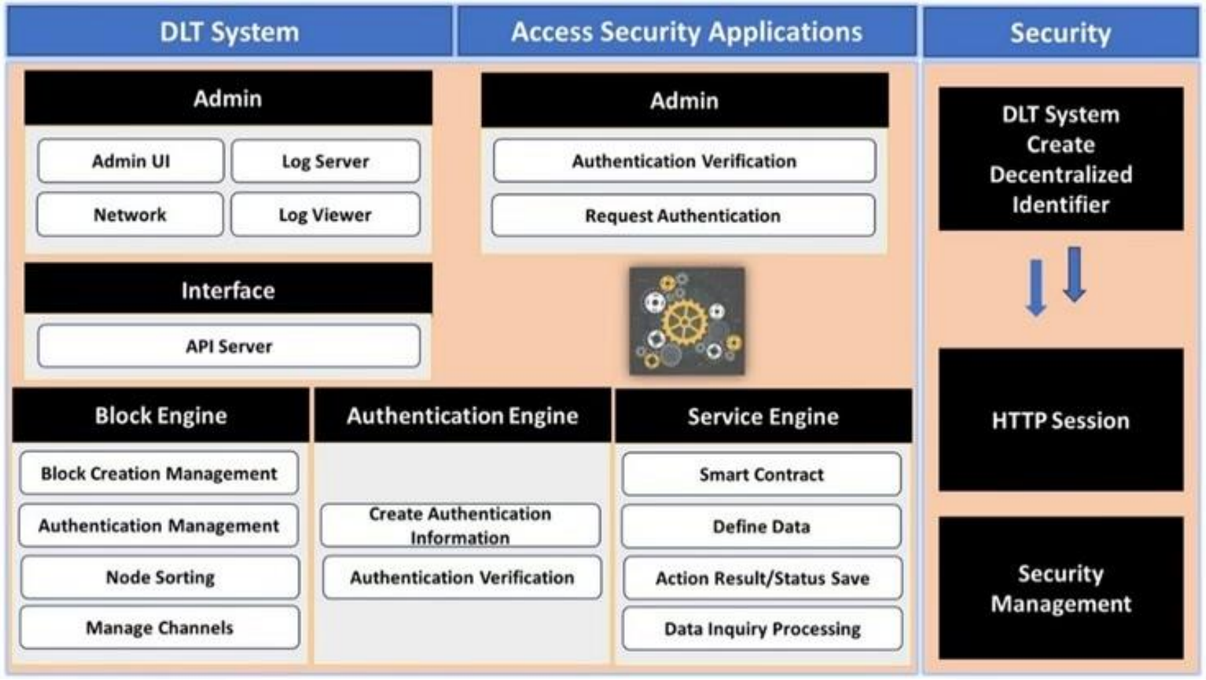


Figure 1: Access Security Authentication based on DLT

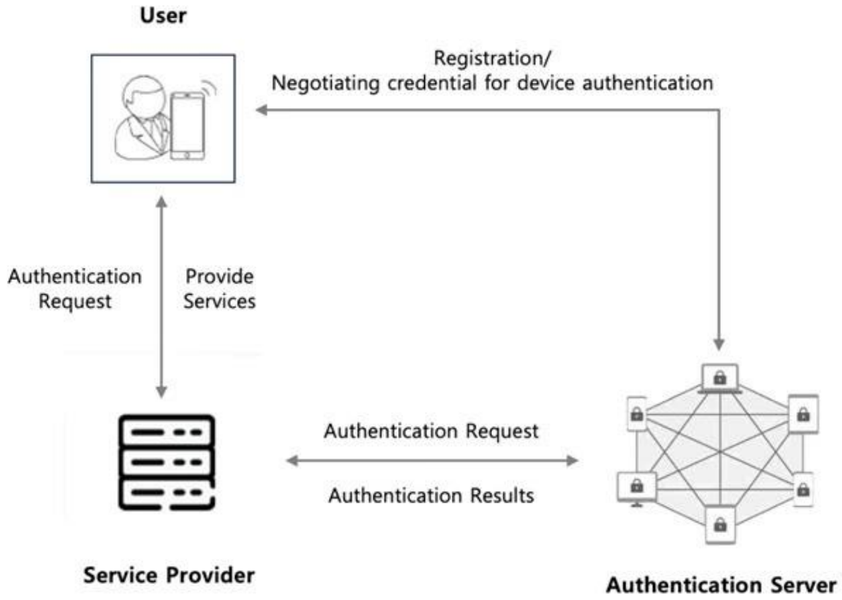


Figure 2: Authentication Framework One-Time Authentication Key using DLT

THANK YOU!

Scan here to access

www.fnsbsa.com