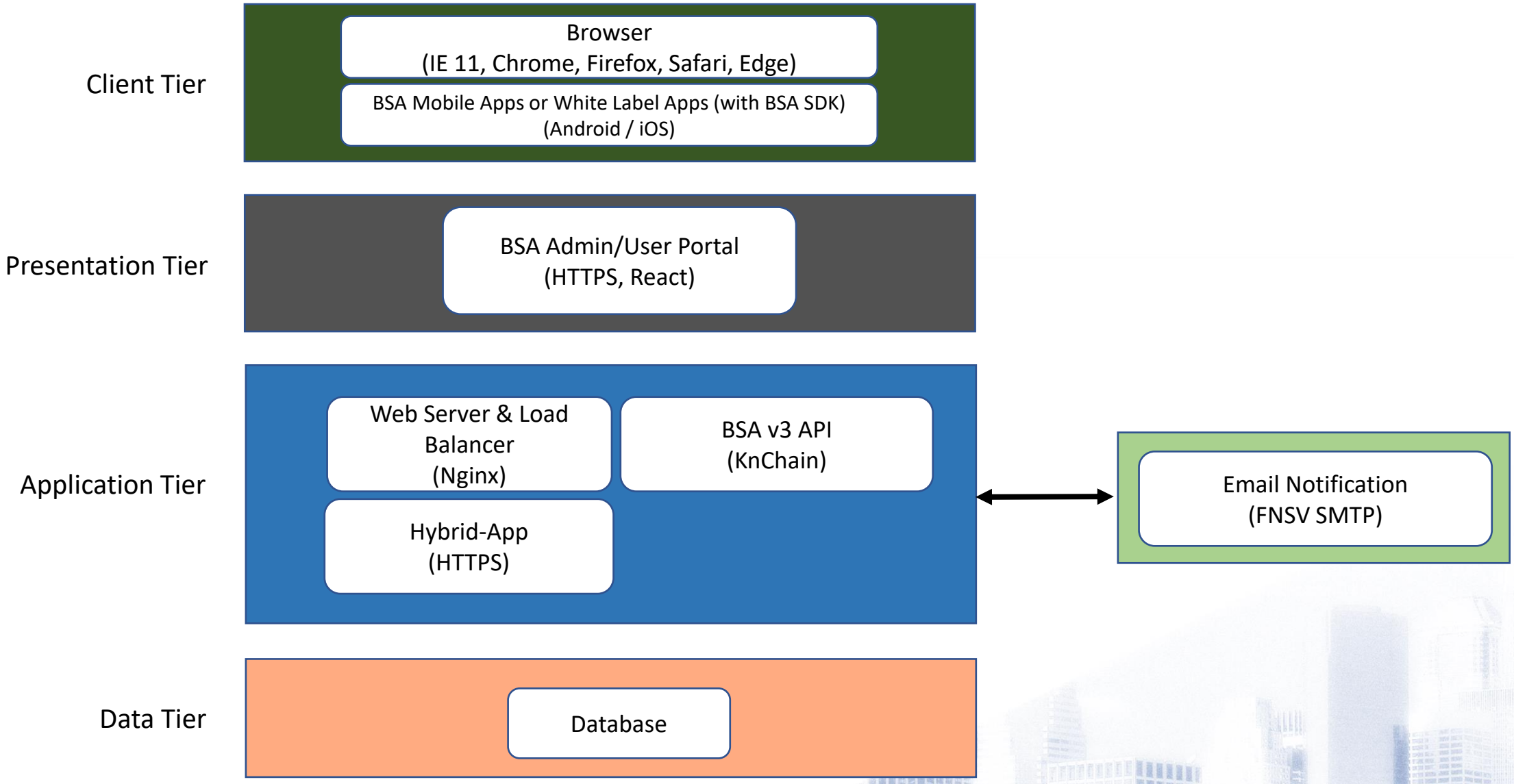
FNS (M) SDN.BHD.
FEASIBLE NETWORK SYSTEM

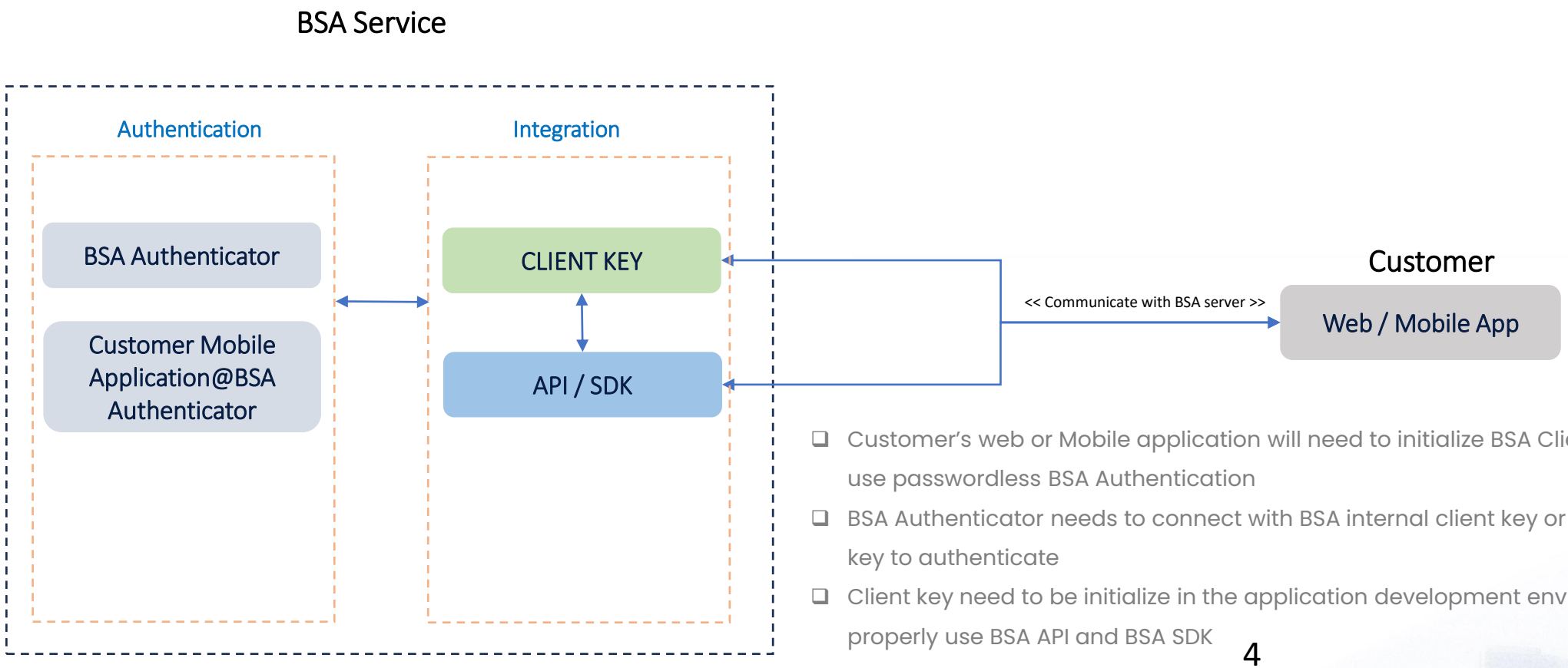
BSA Technical Presentation

Technical presentation for CI/CD


Client Tier
Browser
(IE 11, Chrome, Firefox, Safari, Edge)
BSA Mobile Apps or White Label Apps (with BSA SDK)
(Android / iOS)
Presentation Tier
BSA Admin/User Portal
(HTTPS, React)
Application Tier
Web Server & Load Balancer
(Nginx)
BSA v3 API
(KnChain)
Hybrid-App
(HTTPS)
Email Notification
(FNSV SMTP)
Data Tier
Database

The general components for BSA Passwordless Integration

1. Customer's Application – Web or/and Mobile
2. BSA Authenticator – BSA App or Customer White Label with BSA service
3. Integration development – BSA Web SDK or/and BSA Mobile SDK
4. User Onboarding – Register User, Register Device and Site Link on Mobile App (BSA App or White Label with BSA Service)



- Customer's web or Mobile 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 customer's client key to authenticate
- Client key need to be initialize in the application development environment to properly use BSA API and BSA SDK

1. USER ONBOARDING

Register New User for BSA:

1. User to download BSA App or Customer Mobile App(@BSA Auth) for User and Device information registration.
2. Users to Site Link Web Applications in Authenticator App - BSA App or Customer Mobile App(@BSA Auth)

- (User to approve Login request when prompted in User Mobile Device)

2. SYSTEM ONBOARDING

System Integration

1. Customer Web Application – development to integrate with BSA Web SDK for Passwordless login.
2. Customer Mobile Application – development to integration with BSA Mobile SDK for BSA Onboarding, Passwordless Login, Authentication Approval / Reject)

1. For Web Application Only:

Digital Banking X

(Web Application with BSA Web SDK)

+

Authenticator Application for BSA

BSA Authenticator

2. For Web Application and Mobile Application:

Digital Banking X

(Web Application with BSA Web SDK and

Mobile Application with BSA Mobile SDK)

Mobile Application

(Integrate with BSA Mobile SDK)

3. For Mobile Application Only:

Digital Banking X

(Mobile Application with BSA Mobile SDK)

A. Pre-requisites:

1. **Client Key:** Key to be used for integration between Customer Web Application and BSA Web SDK
2. **BSA Web SDK:** To implement BSA by using JavaScript based BSA Web SDK into CI/CD environment

B. BSA Integration with Customer application

1. Customer Web Application needs to integrate with BSA Web SDK **for Passwordless Login**
2. The integration with BSA Web SDK (libraries, API, services) plus the Client Key assigned; will enable the Customer Web Application(s) to use BSA passwordless Authentication Service.
3. **User registration:** User require to download and register with **BSA Authentication App**, Site Link to Customer Web Application integrated with BSA for passwordless login

C. Authentication Methods:

1. **Passwordless login:**
   a. **Normal Authentication :** Username authentication by keying in username only and then authenticate using BSA Authenticator App
   b. **QR Authentication:** BSA QR code authentication by scanning the QR using BSA Authenticator
   c. **OTP Authentication:** BSA in-app OTP authentication
   d. **TOTP Authentication:** Offline authentication in a case where mobile phone does not have any internet connectivity

A. Pre-requisites:

1. **Client Key:** Key to be used for integration between Customer Web Application and BSA Web SDK
2. **BSA Web SDK:** To implement BSA by using JavaScript based BSA Web SDK into Customer Web Application
3. BSA Mobile SDK : To implement BSA by using iOS and aOS SDK into Customer Mobile App

B. BSA Integration with Customer application

1. Customer Web Application needs to integrate with BSA Web SDK for **Passwordless Login**
2. Customer Mobile Application need to integrate with BSA Mobile SDK for **BSA Onboarding and Passwordless Login**
3. The integration with BSA Web SDK and Mobile SDK (libraries, API, services) plus the Client Key assigned; will enable the Customer Web and Mobile Application to use BSA passwordless Authentication Service.
4. **User registration:** Customer is required to upload the Customer Mobile App (@BSA Authenticator) to respective App Store Providers. Users are required to download and register with Customer Mobile App (@BSA Authenticator) to onboard BSA Services. (Site Link can be optional in this case)

C. es

D. Authentication Methods:

1. **Web Application and Mobile Application Passwordless login:**
   a) **Normal Authentication :** Username authentication by keying in username only and then authenticate using Customer Mobile App(@BSA Authenticator)
   b) **QR Authentication:** BSA QR code authentication by scanning the QR using BSA Authenticator
   c) **OTP Authentication:** BSA in-app OTP authentication
   d) **TOTP Authentication:** Offline authentication in a case where mobile phone does not have any internet connectivity

A. Pre-requisites:

1. **Client Key:** Key to be used for integration between Customer Web Application and BSA Web SDK
2. BSA Mobile SDK : To implement BSA by using iOS and aOS SDK into Customer Mobile App

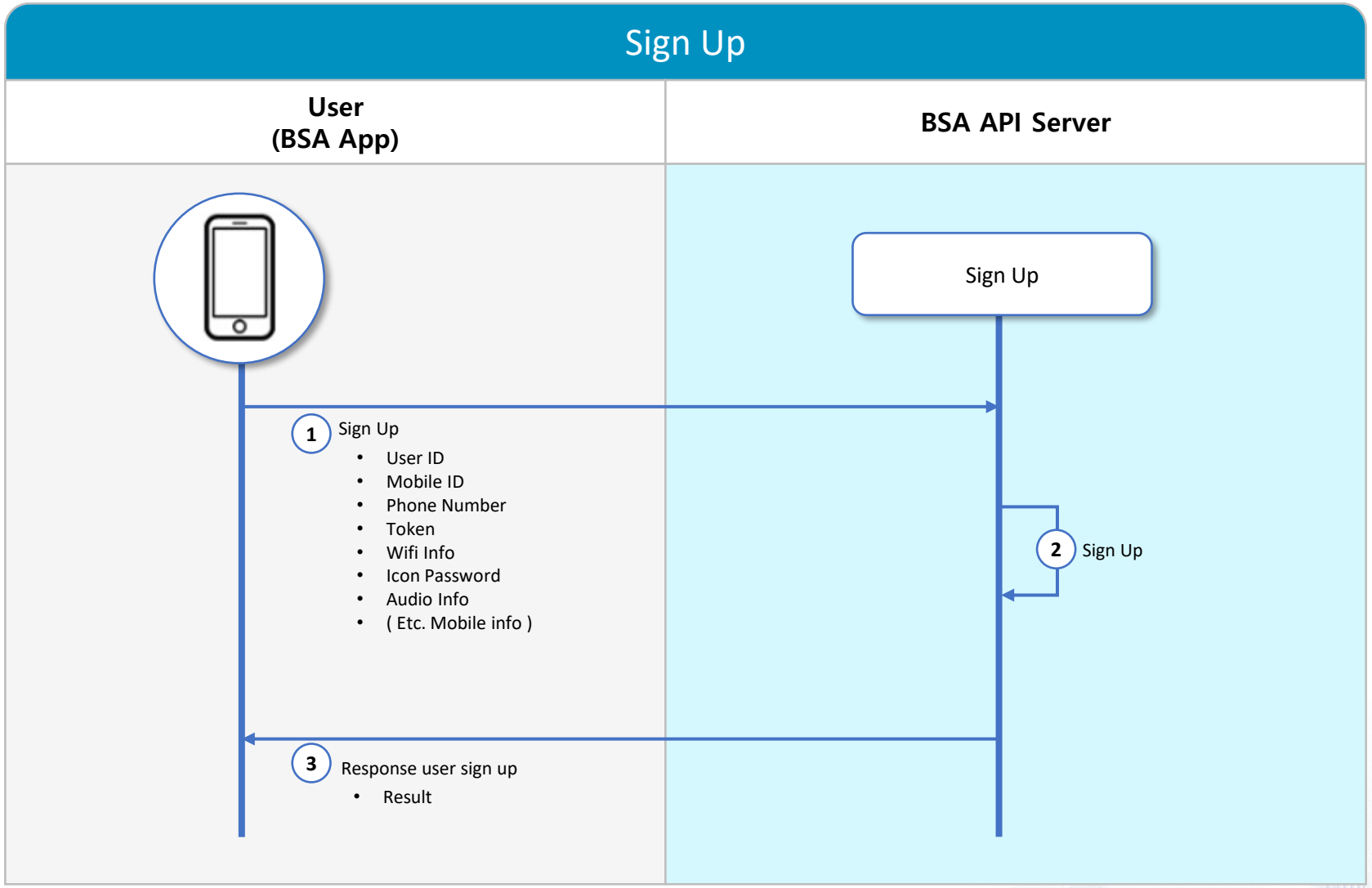
B. BSA Integration with Customer application

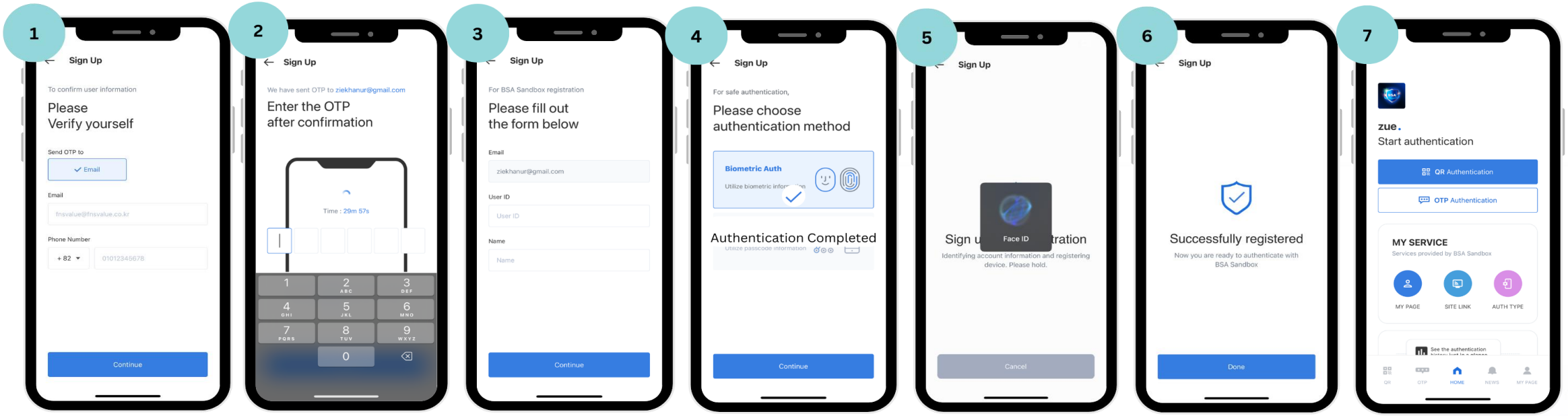
1. Customer Mobile Application need to integrate with BSA Mobile SDK for **BSA Onboarding and Passwordless Login**
2. The integration with BSA Mobile SDK (libraries, API, services) plus the Client Key assigned; will enable the Customer Mobile Application to use BSA passwordless Authentication Service.
3. **User registration:** Customer is required to upload the Customer Mobile App (@BSA Authenticator) to respective App Store Providers. Users are required to download and register with Customer Mobile App (@BSA Authenticator) to onboard BSA Services. (No Site Link for Mobile Application only installation)

C. es

D. Authentication Methods:

1. **Mobile Application Passwordless login:**
   a) **Normal Authentication :** Username authentication by keying in username only and then authenticate using Customer Mobile App(@BSA Authenticator)


Sign Up
User
(BSA App)
BSA API Server
Sign Up
1
Sign Up
User ID
Mobile ID
Phone Number
Token
Wifi Info
Icon Password
Audio Info
(Etc. Mobile info)
2
Sign Up
3
Response user sign up
Result



Key-in email and phone number

Email OTP verification (only registration)

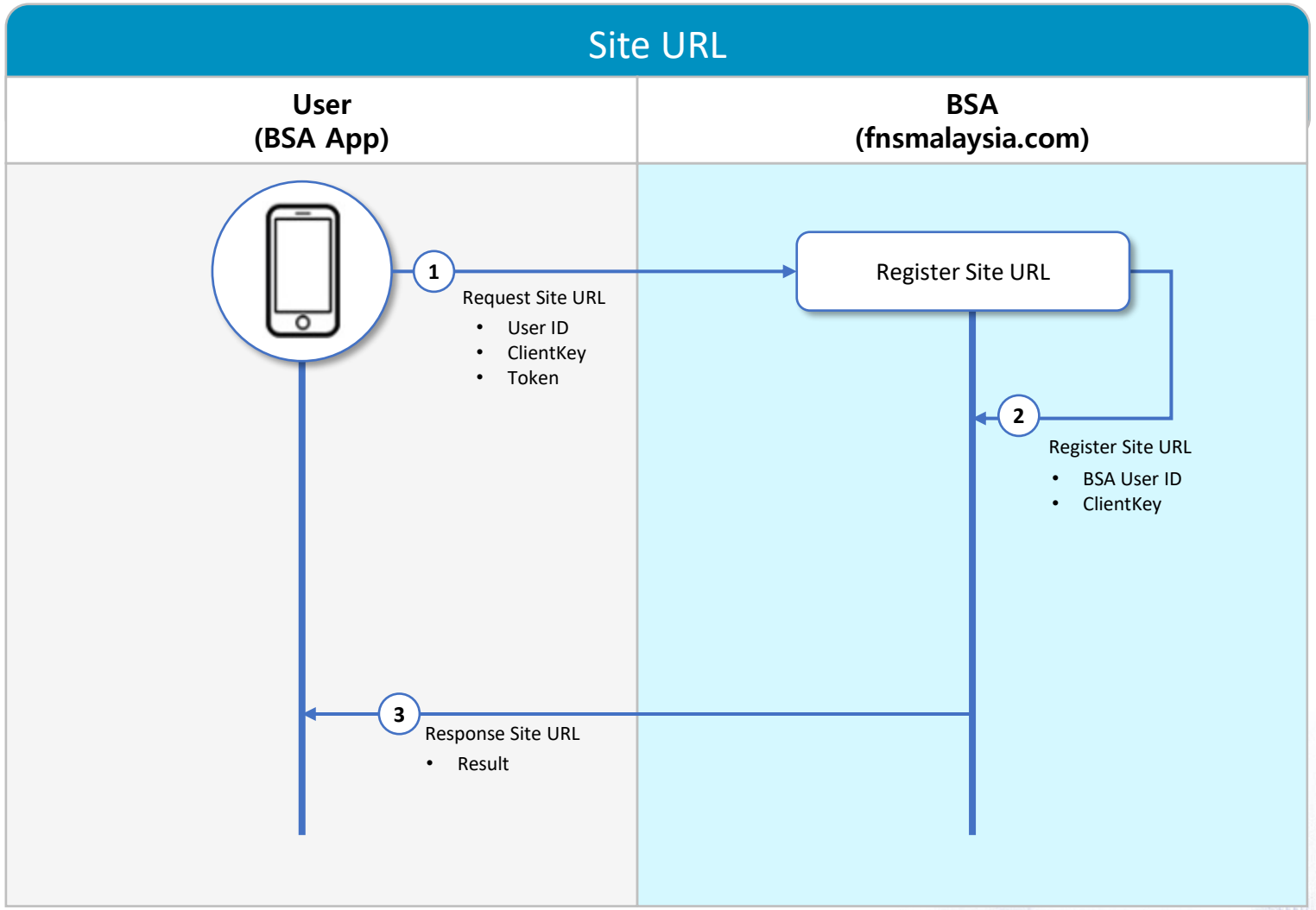
Key-in user name and name

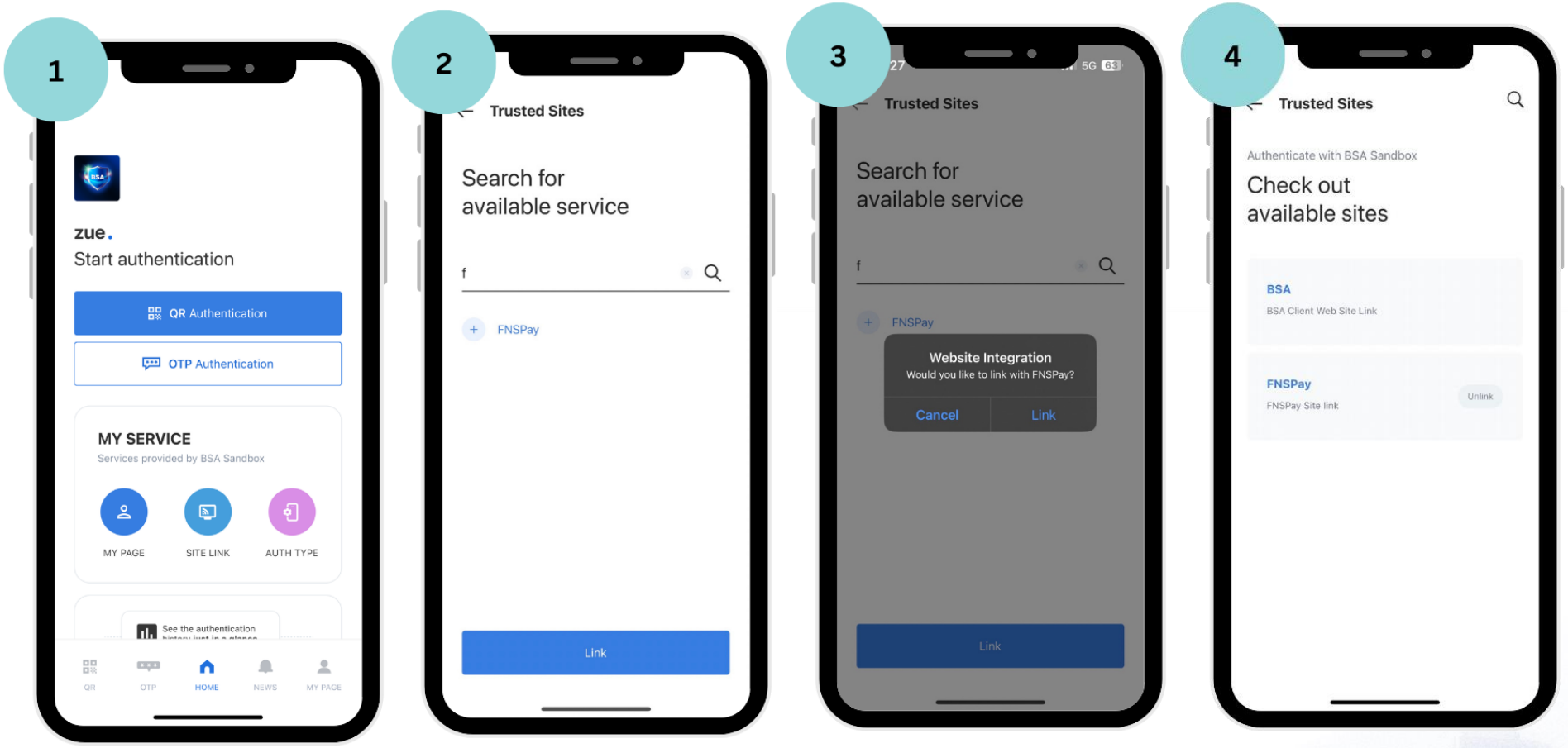
Choose authentication method

Register chosen authentication method

Completed

BSA Dashboard


Site URL
User
(BSA App)
BSA
(fnsmalaysia.com)
Register Site URL
1
Request Site URL
• User ID
• ClientKey
• Token
2
Register Site URL
• BSA User ID
• ClientKey
3
Response Site URL
• Result

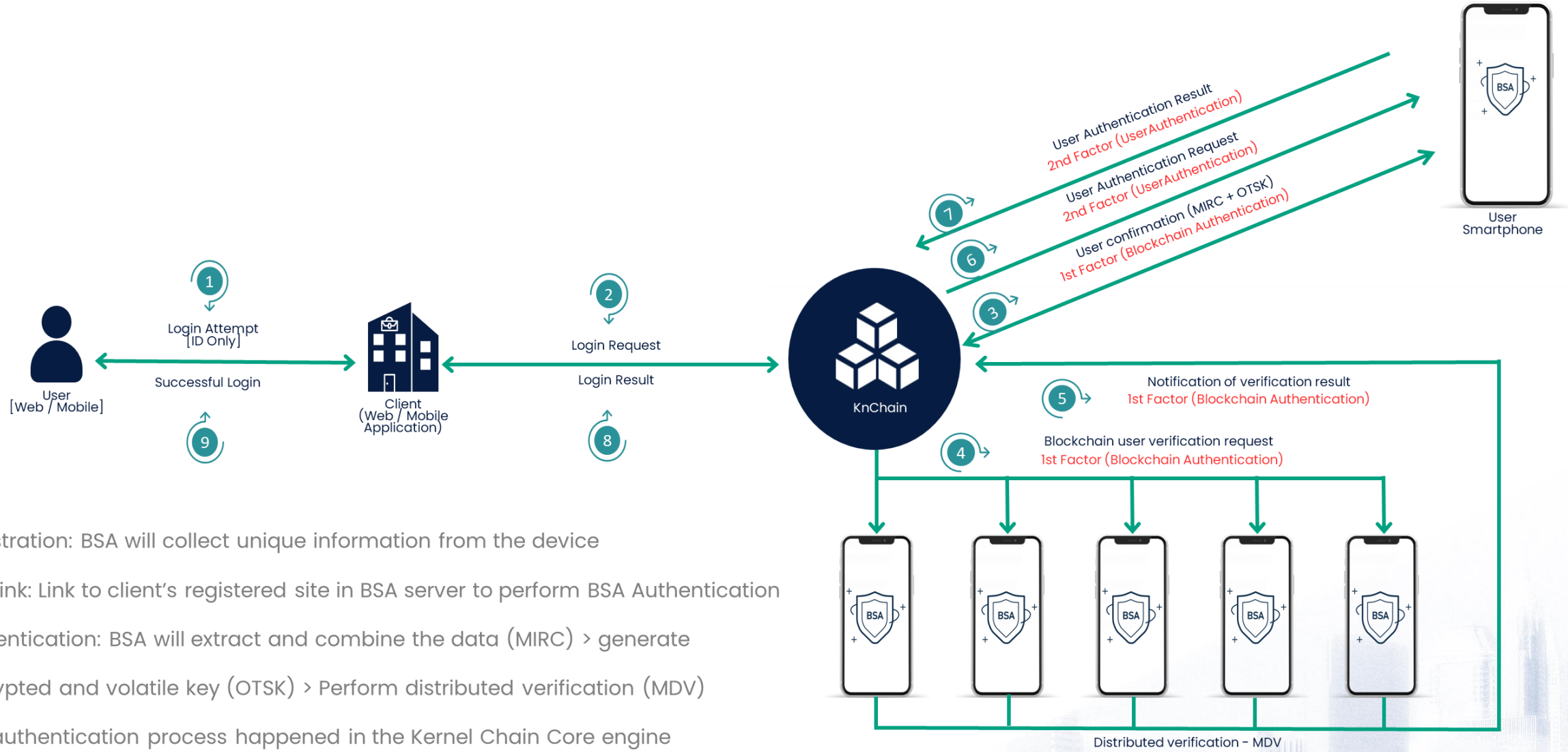


BSA Dashboard

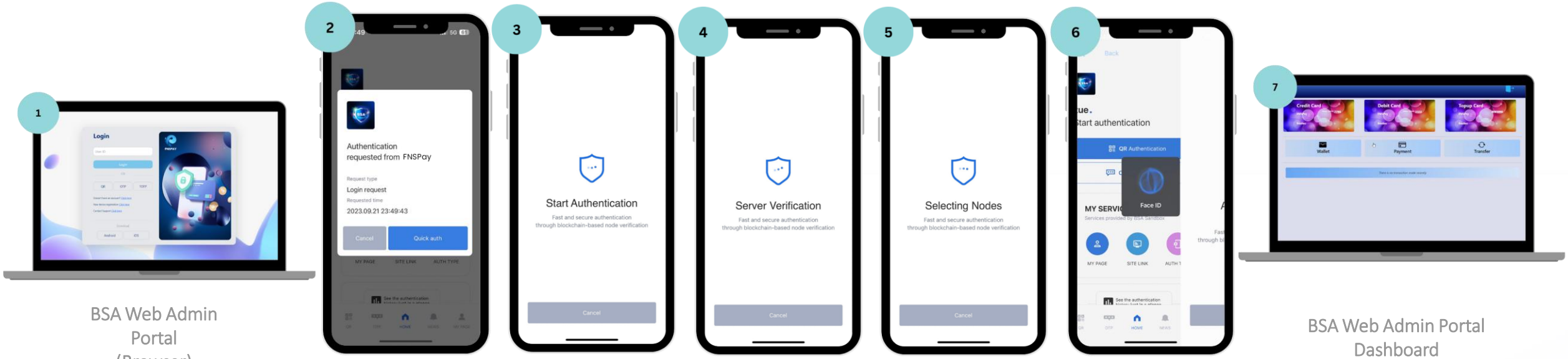
Search for the Site and Link

Link the site

Site is linked



- 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 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)

1. BSA Web Admin Portal: https://web.fnsmalaysia.com/login
2. BSA aOS Mobile App (Authenticator): https://play.google.com/store/apps/details?id=com.fnsm.bsa&pli=1
3. BSA iOS Mobile App (Authenticator): https://apps.apple.com/gy/app/bsa-authenticator/id6462007090
4. BSA Web SDK Guide: https://resource.fnsbsa.com/resource/BSA-Web-SDK.pdf
5. BSA aOS SDK Guide: https://resource.fnsbsa.com/resource/BSA-aOS-SDK-Guide.pdf
6. BSA iOS SDK Guide: https://resource.fnsbsa.com/resource/BSA-iOS-SDK-Guide.pdf

CI/CD		
No	**Description**	**Info**
1	System and/or application Custodian	
2	List of IP addresses with hostname	
3	Current user use CI/CD service	
4	Potential number of users for the Pilot test	
5	Web application technology used	
6	List of OS	
7	List of API and/or system integration	
8	DB type and version	
9	System hosted (Location)	
10	API Gateway	
11	Directory Services Authentication (LDAP/ADFS)	
12	Current Deployment Environment	
13	Network Port	
14	Web Server	

FNS (M) SDN.BHD.
FEASIBLE NETWORK SYSTEM

Thank you!