FNSvalue

Blockchain Secure Authentication (BSA)

Passwordless Authentication
for
Digital Financial Services (DFS)

Secure. Fast. Convenient.

Table of Contents

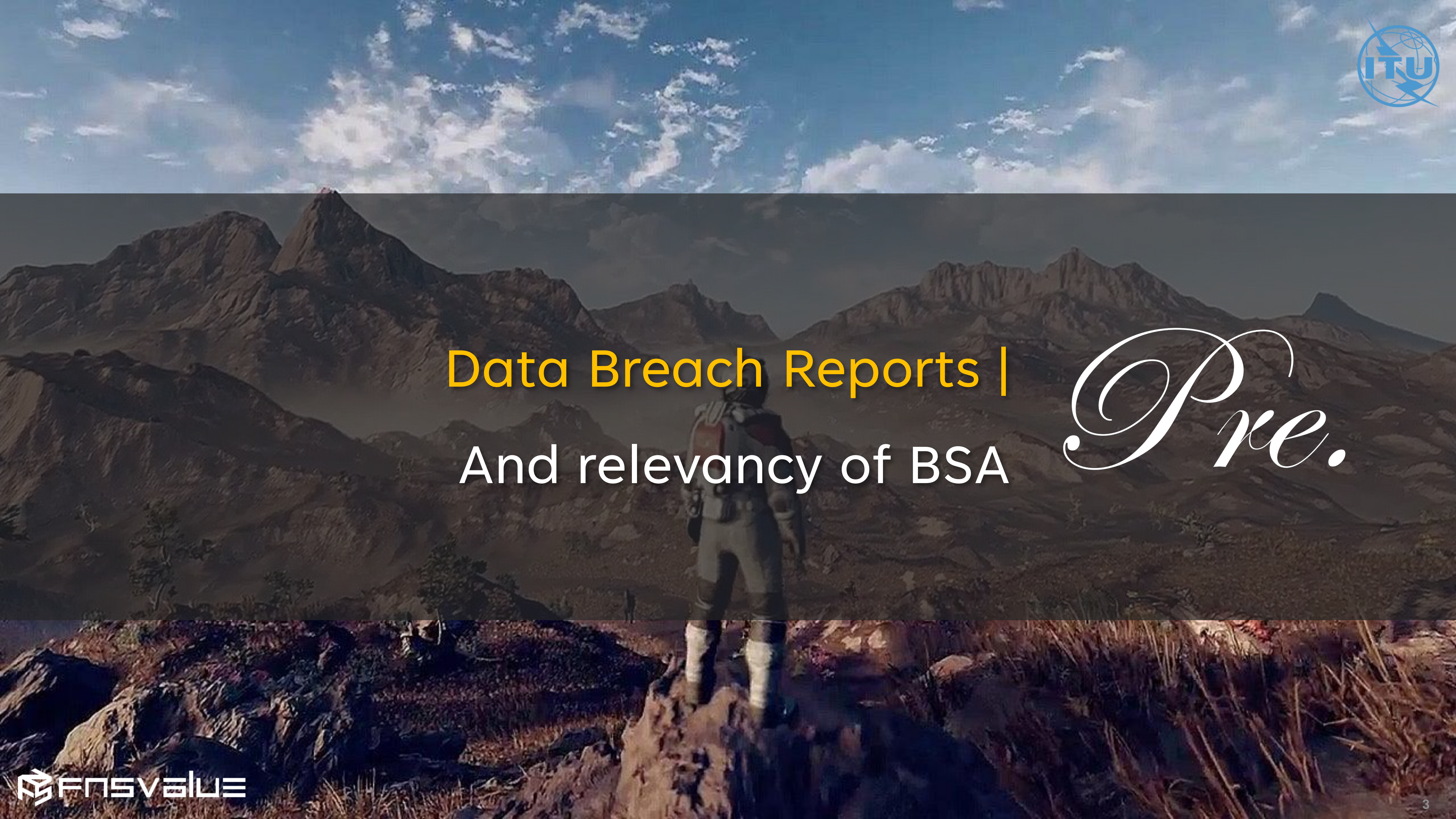
Preface | Data Breach Reports & Relevancy of BSA

Section 01 | How does BSA technology works & how does it enable Passwordless authentication for mobile payments

- User Experience Video
- BSA Authentication Process
- The Technology

Section 02 | ITU BSA Sandbox for DFS Regulators

- Enabling Use Cases
- Value Propositions



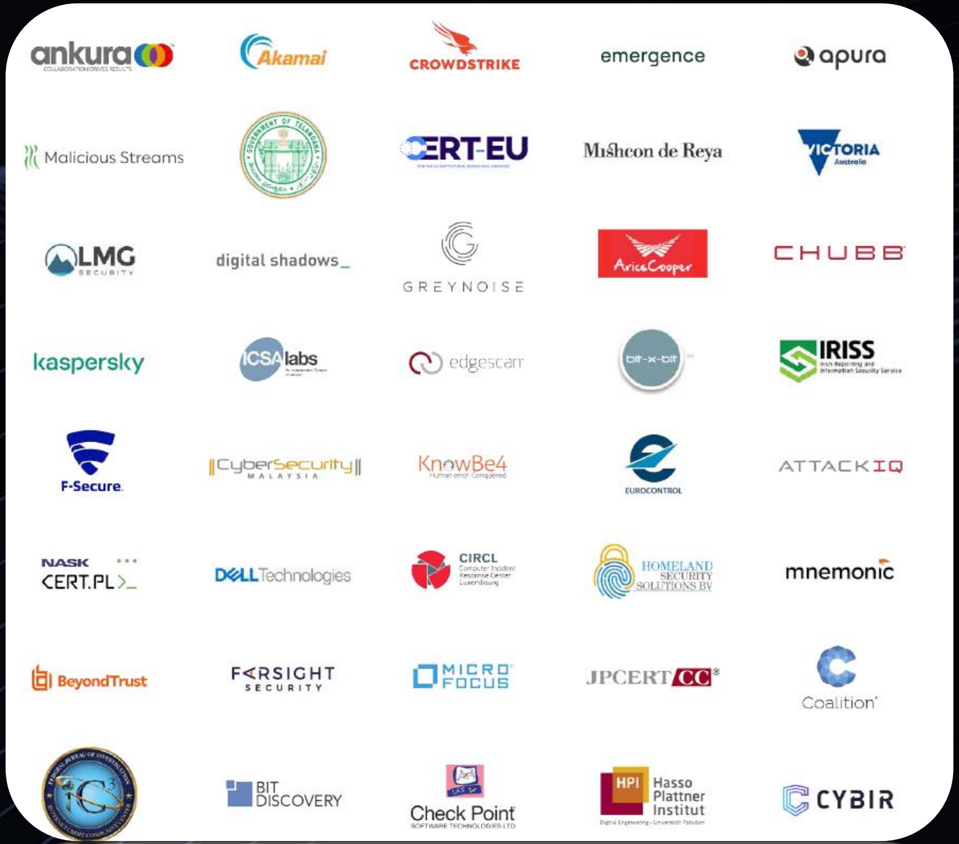
Data Breach Reports |

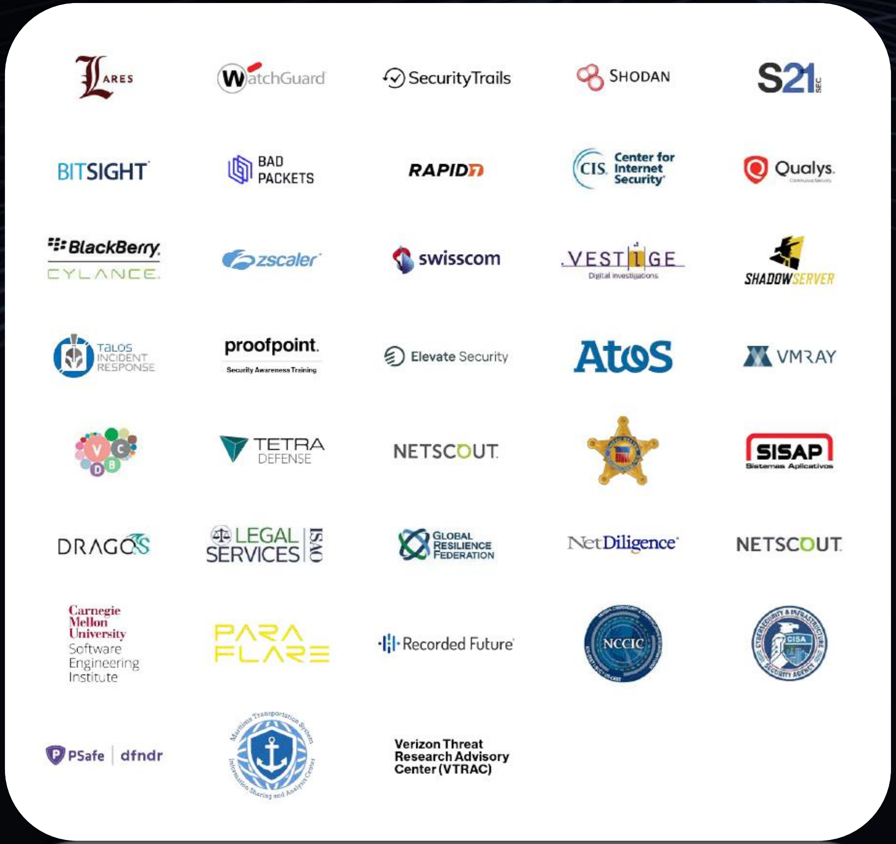
And relevancy of BSA

Pre.

Research, Study & Investigation

A snapshot of Data Breach Investigation Reports (DBIR) conducted by Verizon in 2021 and with known collaborating organizations involved for this report. They are namely:





Highlights of the Report

Some key highlights pointed out from the DBIR. There are:

1. Actor

2. Motives

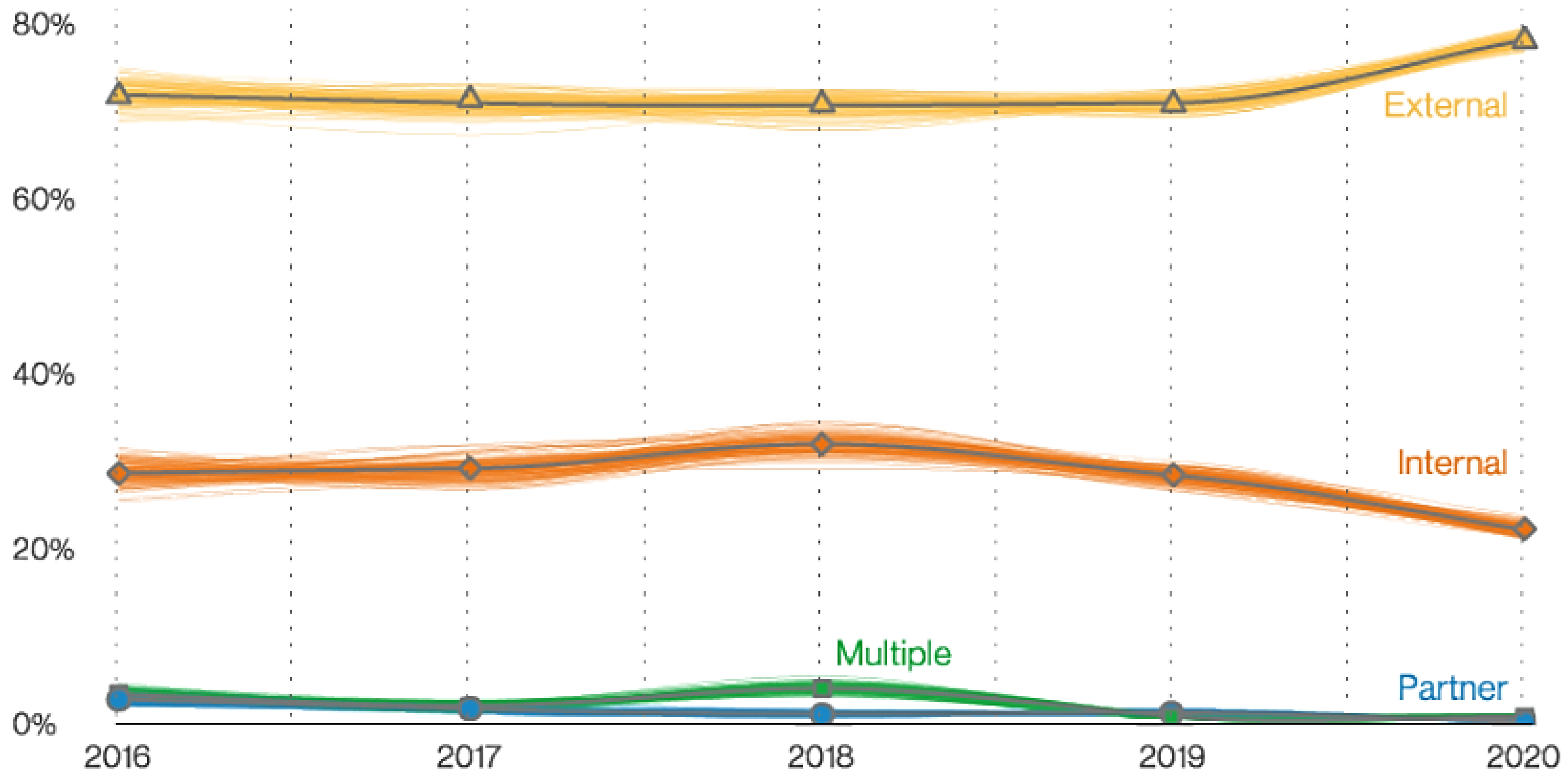
3. Actions

4. Where

5. Attributes

Highlights of the Report

Actors

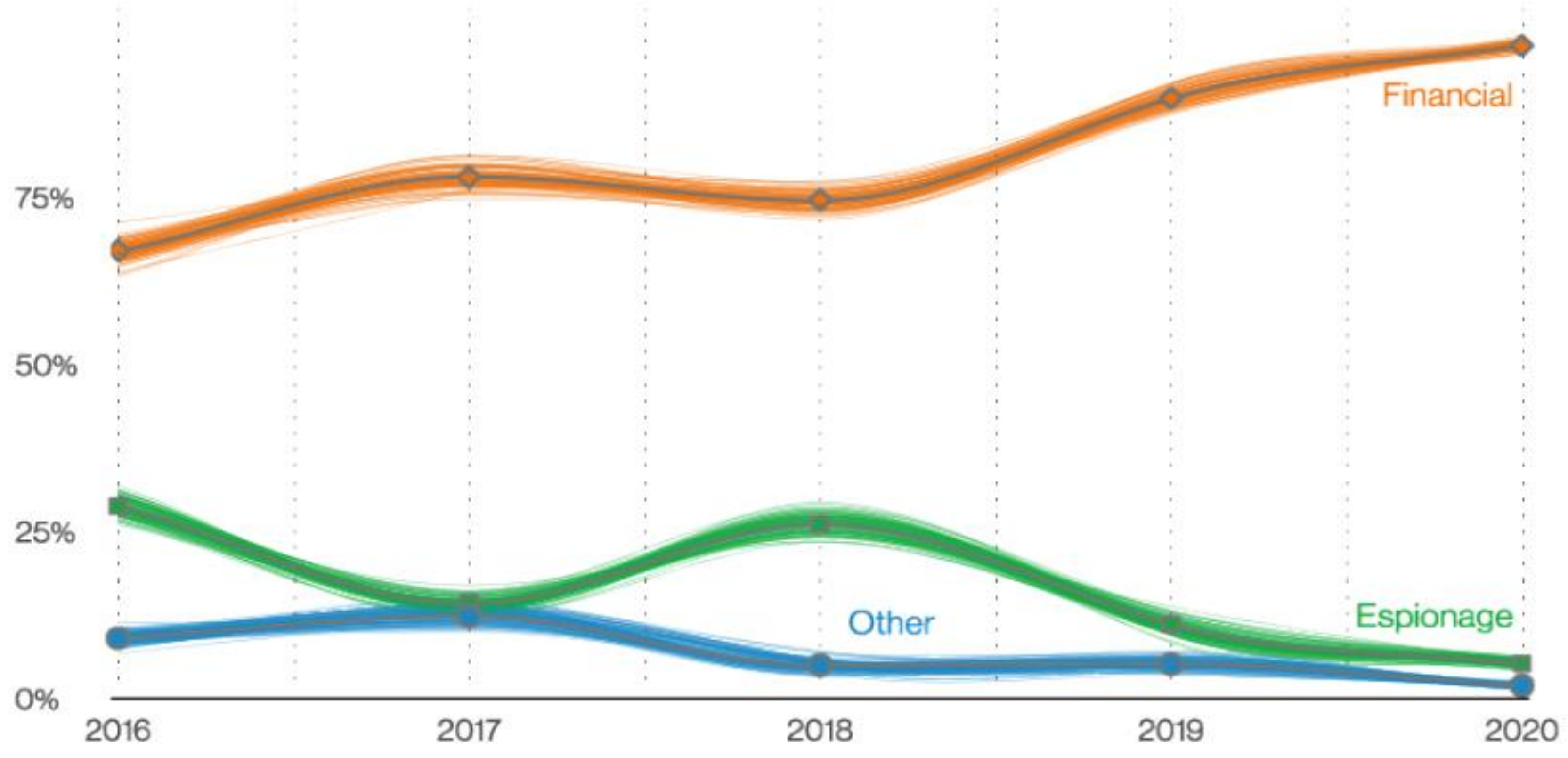


Threat actor over time in breaches

Source: Verizon |
Data Breach Investigation Report 2021

Highlights of the Report

Motives



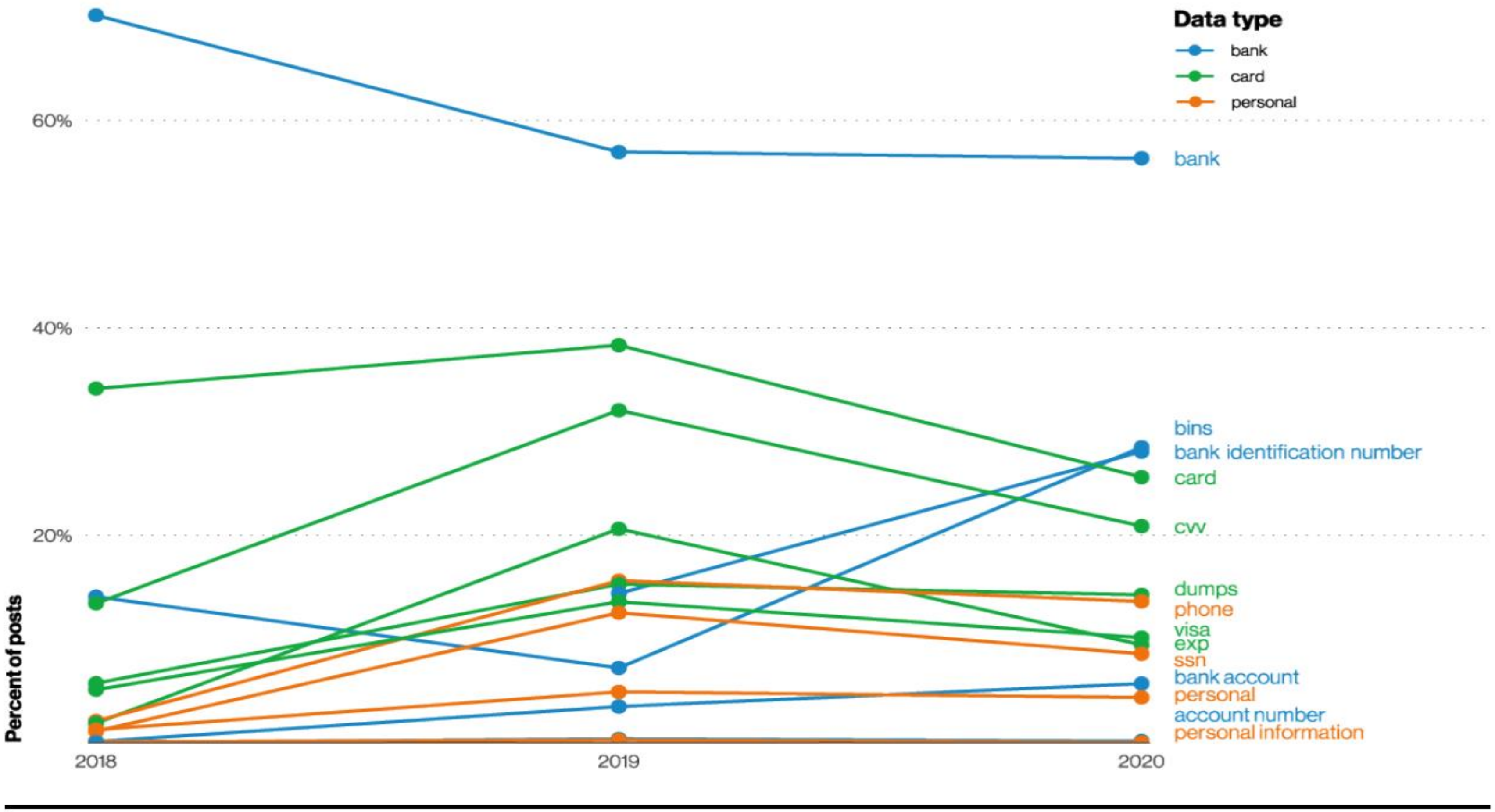
Top threat actor motive over time in breaches

Source: Verizon |
Data Breach Investigation Report 2021

Highlights of the Report

Motives

Details

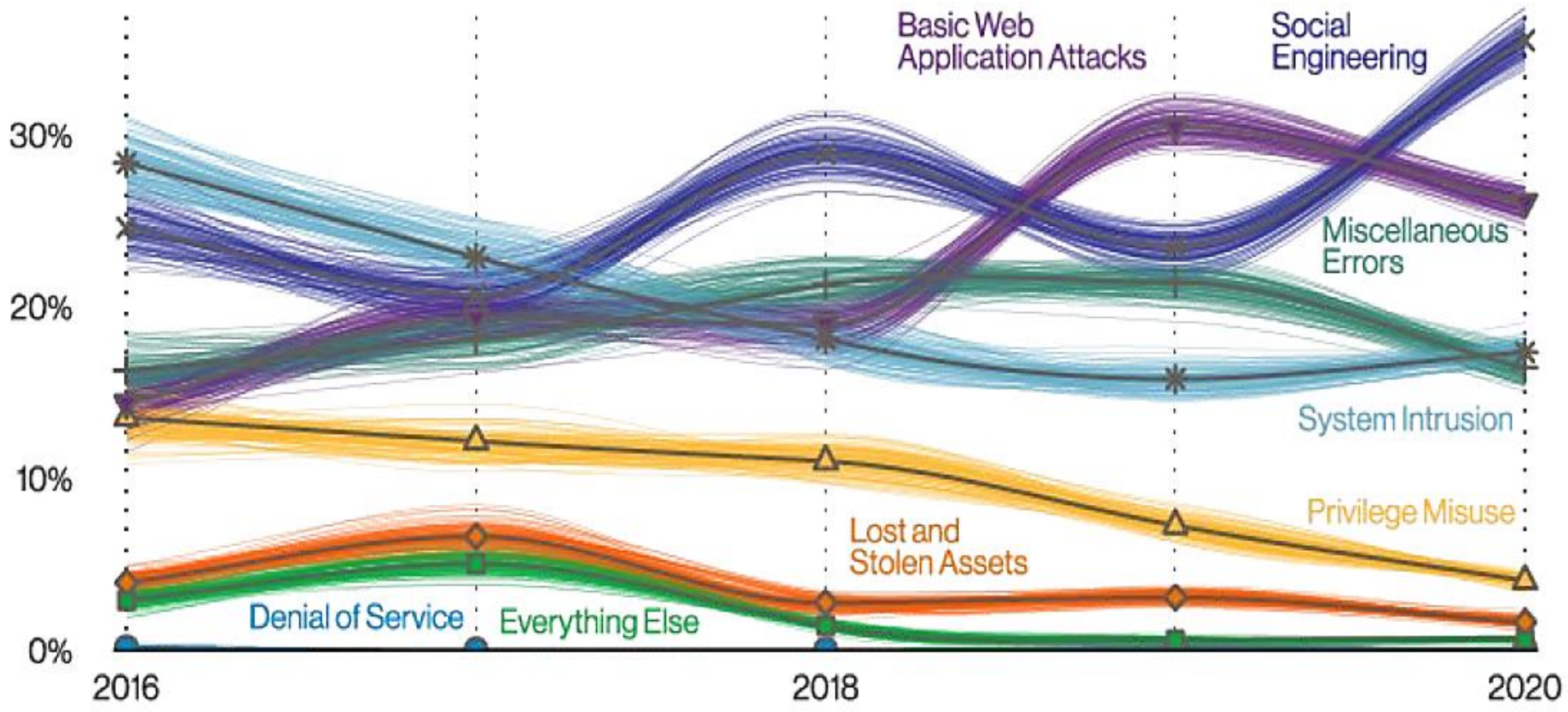


Terms over time in criminal forums and marketplaces

Source: Verizon |
Data Breach Investigation Report 2021

Highlights of the Report

Actions
~How?

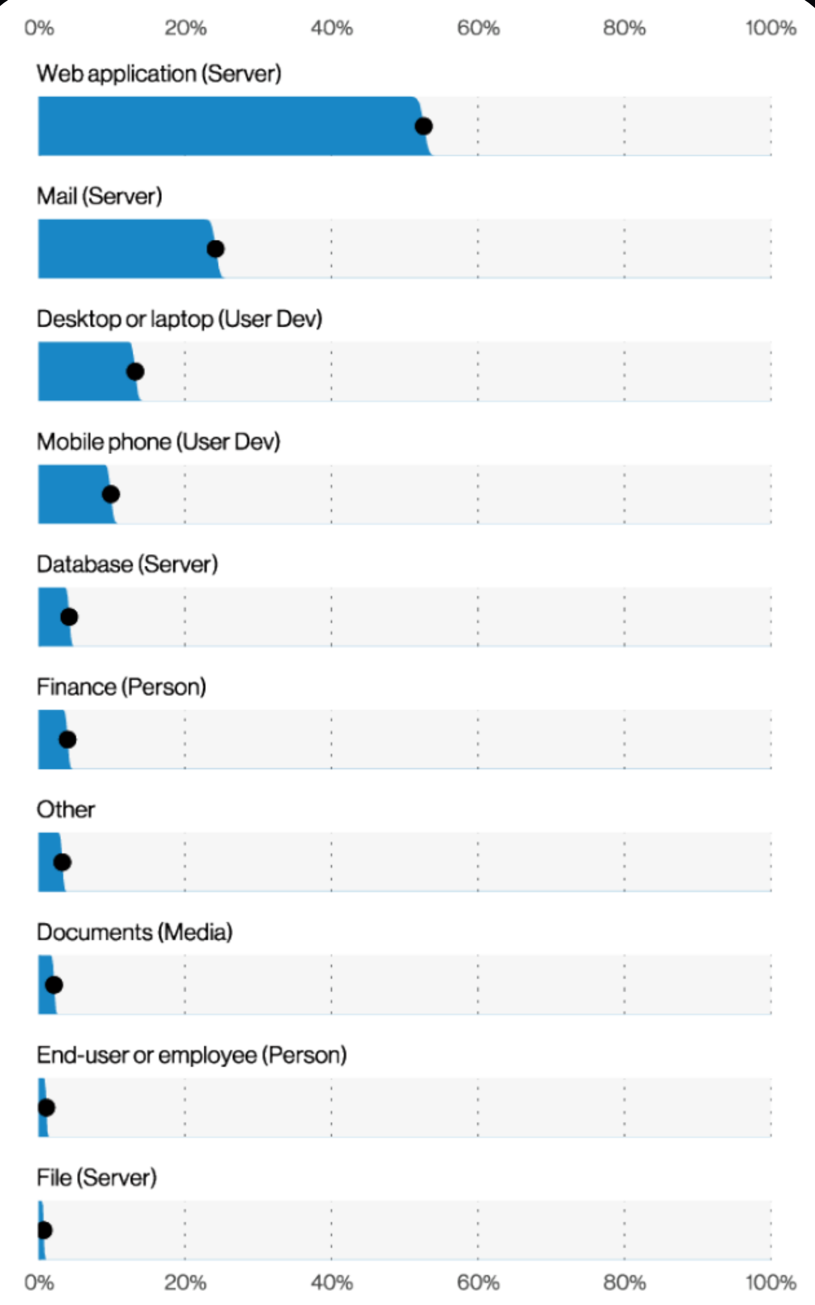


Patterns over time in breaches

Source: Verizon |
Data Breach Investigation Report 2021

Highlights of the Report

Where?



Top asset varieties in incidents (n= 9,188)

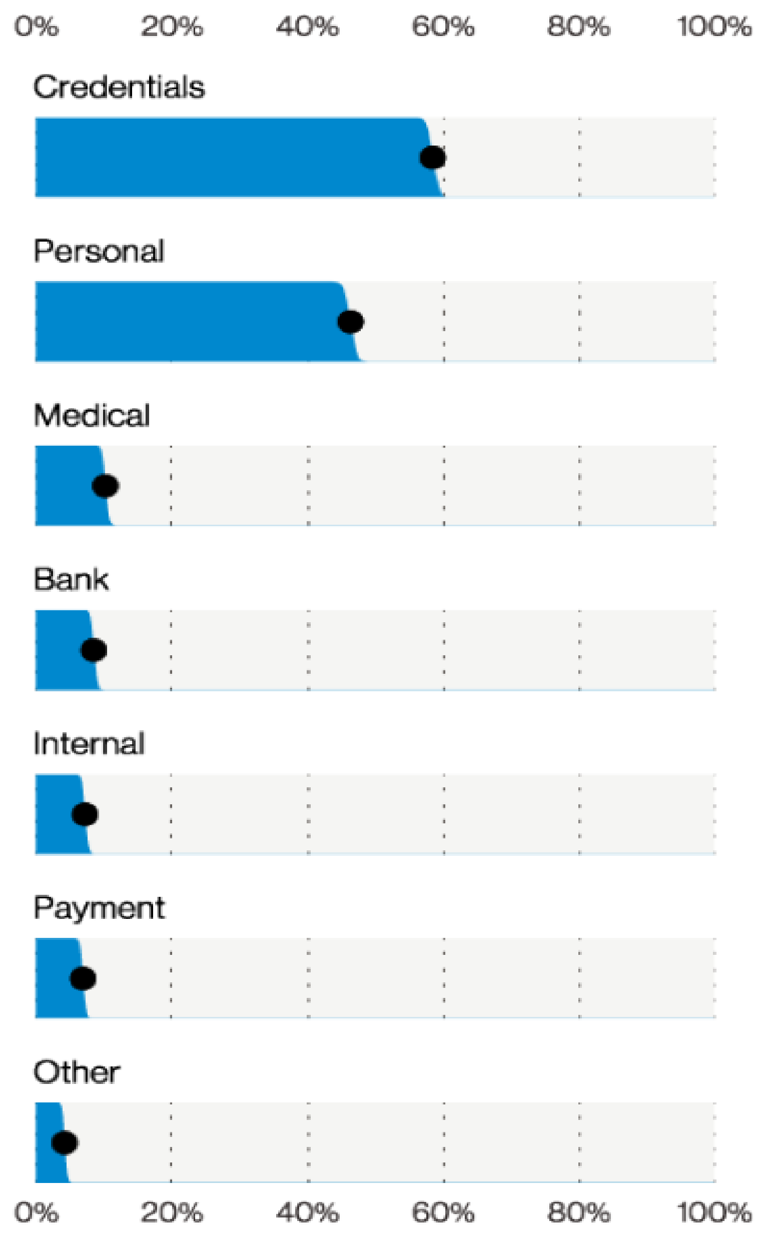
Source: Verizon |
Data Breach Investigation Report 2021

Highlights of the Report

Attributes

~ What?

Based on all pointed-out details, Credentials remain one of the most sought-after data types



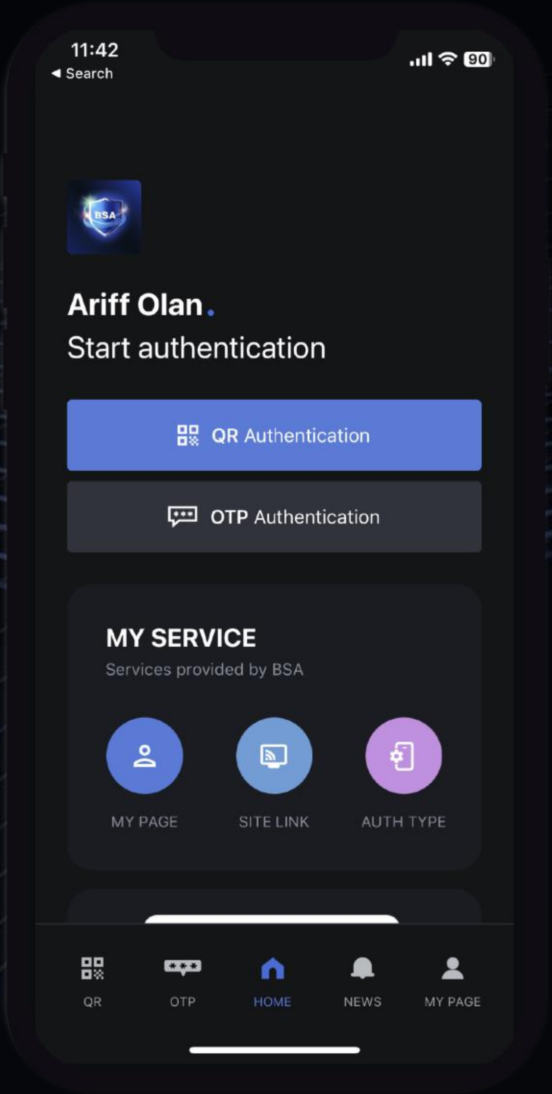
Top data varieties in breaches (n=4,552)

Source: Verizon |
Data Breach Investigation Report 2021

Relevancy of BSA

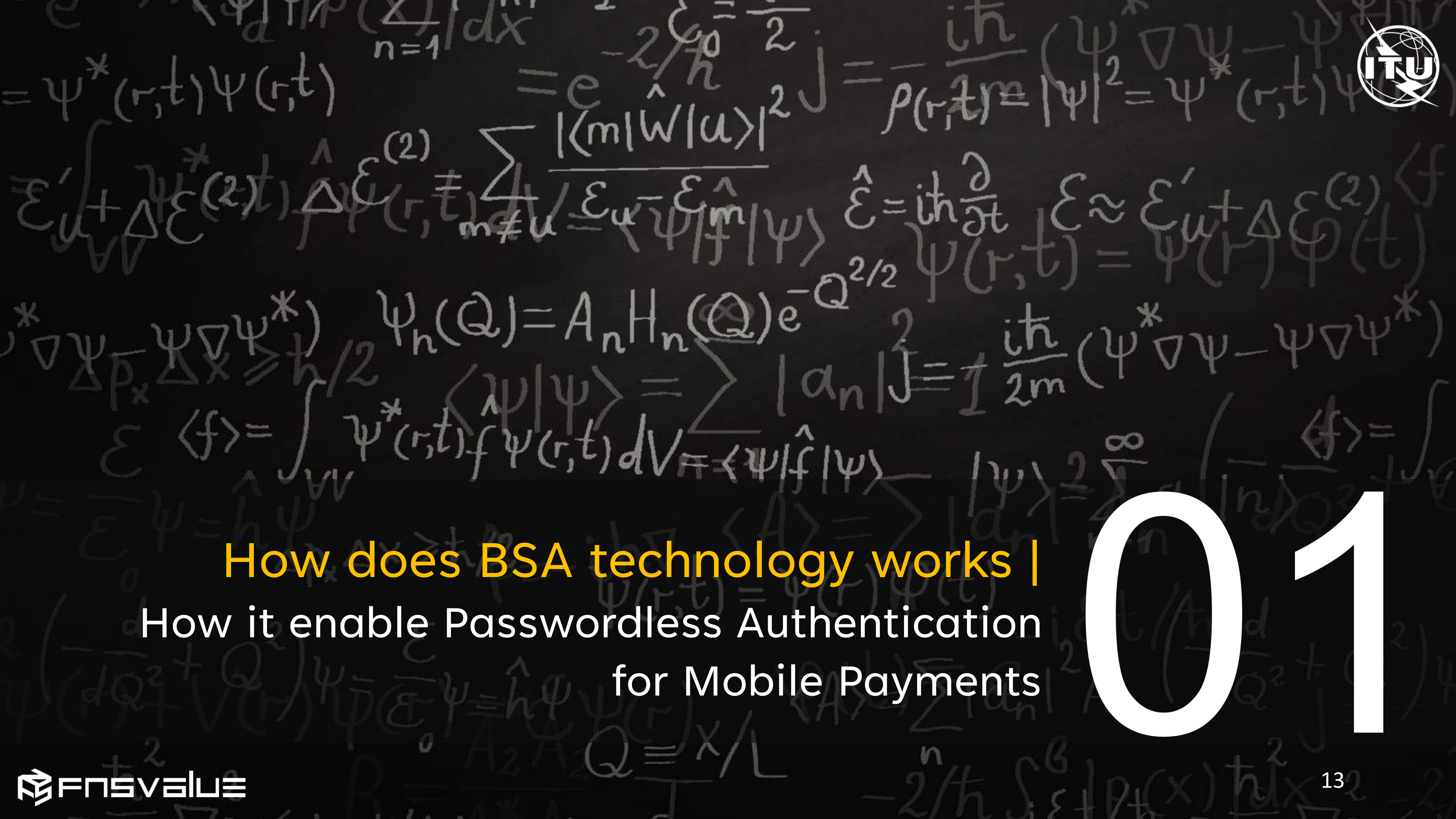
Blockchain Secure Authentication (BSA) is a True-Passwordless Multifactor Authentication (MFA) Solution.

Using Blockchain Technology for Verification and Authentication



Due to these common challenges

- Passwords / PINs, etc are easy to forget, steal, or hack.
- Multi-factor authentication (MFA) adds complexity and inconvenience for users, devices can be stolen.
- Biometrics alone can be spoofed or compromised.
- Centralized databases are vulnerable to breaches or attacks.



How does BSA technology works |

How it enable Passwordless Authentication for Mobile Payments

01

BSA Objectives

- **Empowering users with the choice of authentication methods**

  Enable organizations and users to choose from a range of supported authentication methods such as Username, QR Code, OTP and TOTP, allowing them to mitigate risks based on their specific use cases.

- **Enhance and standardise End-user Experience**

  Establish seamless, enjoyable, and consistent end-user experiences across all platforms.

How BSA Works

BSA works in 2 parts process

A. Onboarding
   1. Application – Web & Mobile
   2. User Device

B. Operational
   1. Username Login
   2. QR Code Login
   3. OTP Login
   4. TOTP Login

How BSA Works

BSA works in 2 parts process

A. Onboarding
   1. Application – Web & Mobile
   2. User Device

B. Operational
   1. Username Login
   2. QR Code Login
   3. OTP Login
   4. TOTP Login

The 4 BSA Technologies / protocol specifications

1. Multiple Identifier Random Combination
2. OTSK Verification
3. Distributed Node Verification
4. Hybrid Blockchain Network

BSA Technologies

Multiple Identifier Random Combination (MIRC)

Extracts Multiple Unique Identifiers from user's mobile device to create unhackable unique key.

One-Time Security Key (OTSK)

BSA uses a One-Time Security Key (OTSK) for blockchain channels, block, and instances to eliminate any point of forgery during authentication process. OTSK is 100% volatile and unhackable.

Multilateral Distributed Verification (MDV)

BSA implements Multilateral Distributed Verification (MDV) technology based on its Kernel Chain which is unique to maximize security levels.

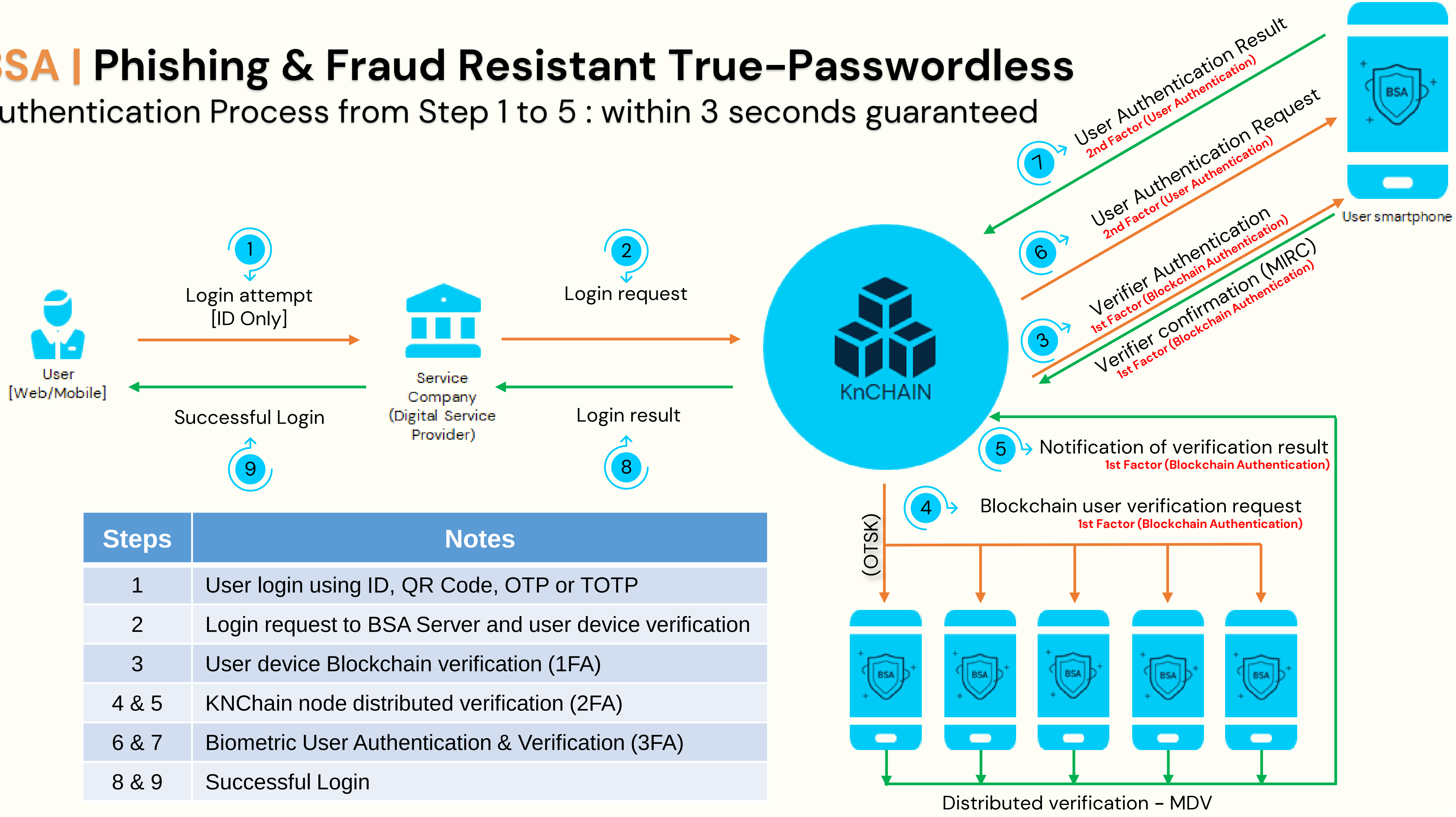
Kernel Chain Core (KNChain) Hybrid Blockchain

New global authentication ecosystem for individuals and corporations. Fast, easy, and robust security authentication service. Independent Hybrid Blockchain Service technology.

BSA Verification and Authentication Flow

BSA | Phishing & Fraud Resistant True-Passwordless

Authentication Process from Step 1 to 5 : within 3 seconds guaranteed



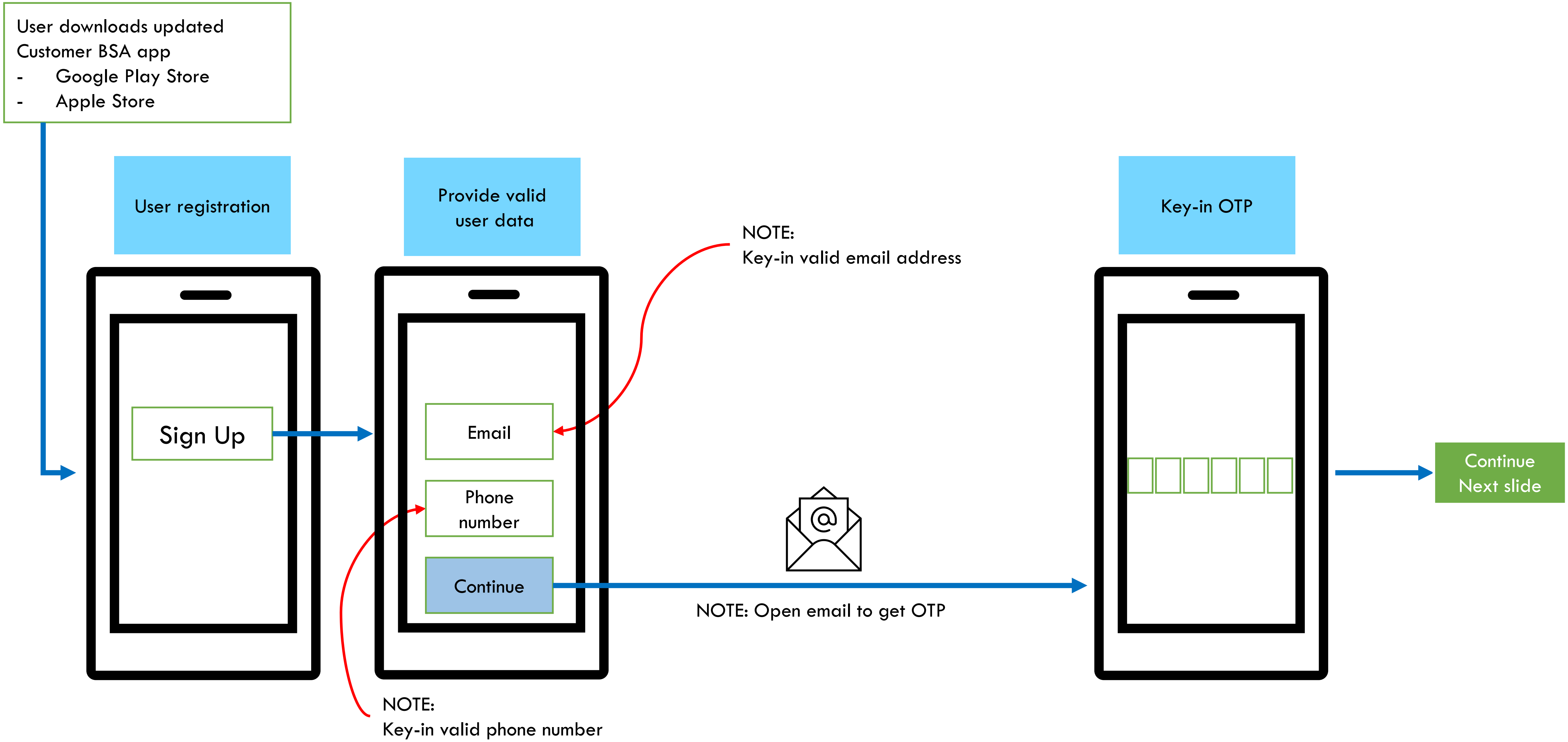
User
[Web/Mobile]
1
Login attempt
[ID Only]
Successful Login
9
Service
Company
(Digital Service
Provider)
2
Login request
Login result
8
KnCHAIN
7
User Authentication Result
2nd Factor (User Authentication)
6
User Authentication Request
2nd Factor (User Authentication)
3
Verifier Authentication
1st Factor (Blockchain Authentication)
Verifier confirmation (MIRC)
1st Factor (Blockchain Authentication)
User smartphone
BSA
5
Notification of verification result
1st Factor (Blockchain Authentication)
4
Blockchain user verification request
1st Factor (Blockchain Authentication)
(OTSK)
Distributed verification – MDV

Steps	Notes
1	User login using ID, QR Code, OTP or TOTP
2	Login request to BSA Server and user device verification
3	User device Blockchain verification (1FA)
4 & 5	KNChain node distributed verification (2FA)
6 & 7	Biometric User Authentication & Verification (3FA)
8 & 9	Successful Login

User On-Boarding Process

- The provided process flow is a generic user on-boarding process.
- On-boarding process can be customized to meet the customer requirements.
- The on-boarding process can be integrated with eKYC & digital certificate issuance for digital signing for a complete digital user on-boarding experience.
- The customer may enforce its own on-boarding process requirements & process flow including its preferred naming convention, terms & usage.

User On-Boarding: User Email & Phone Number Registration



User downloads updated Customer BSA app

- Google Play Store
- Apple Store

User registration

Provide valid user data

Key-in OTP

Sign Up

Email

Phone number

Continue

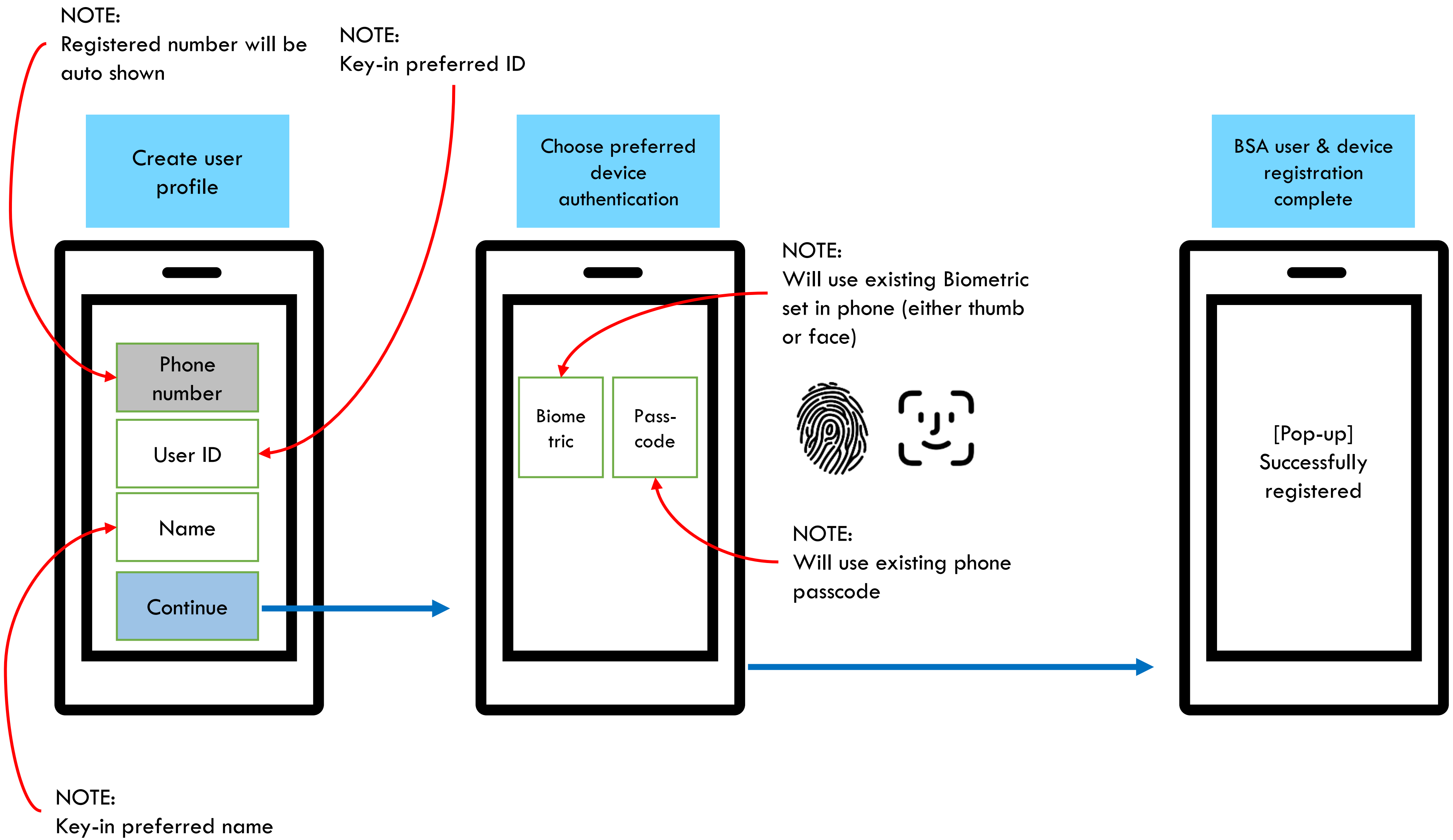
NOTE:
Key-in valid email address

NOTE:
Key-in valid phone number

NOTE: Open email to get OTP

Continue
Next slide

User On-Boarding: User ID & Name Registration



Create user profile
Phone number
User ID
Name
Continue
Choose preferred device authentication
Biometric
Pass-code
BSA user & device registration complete
[Pop-up] Successfully registered

NOTE:
Registered number will be auto shown

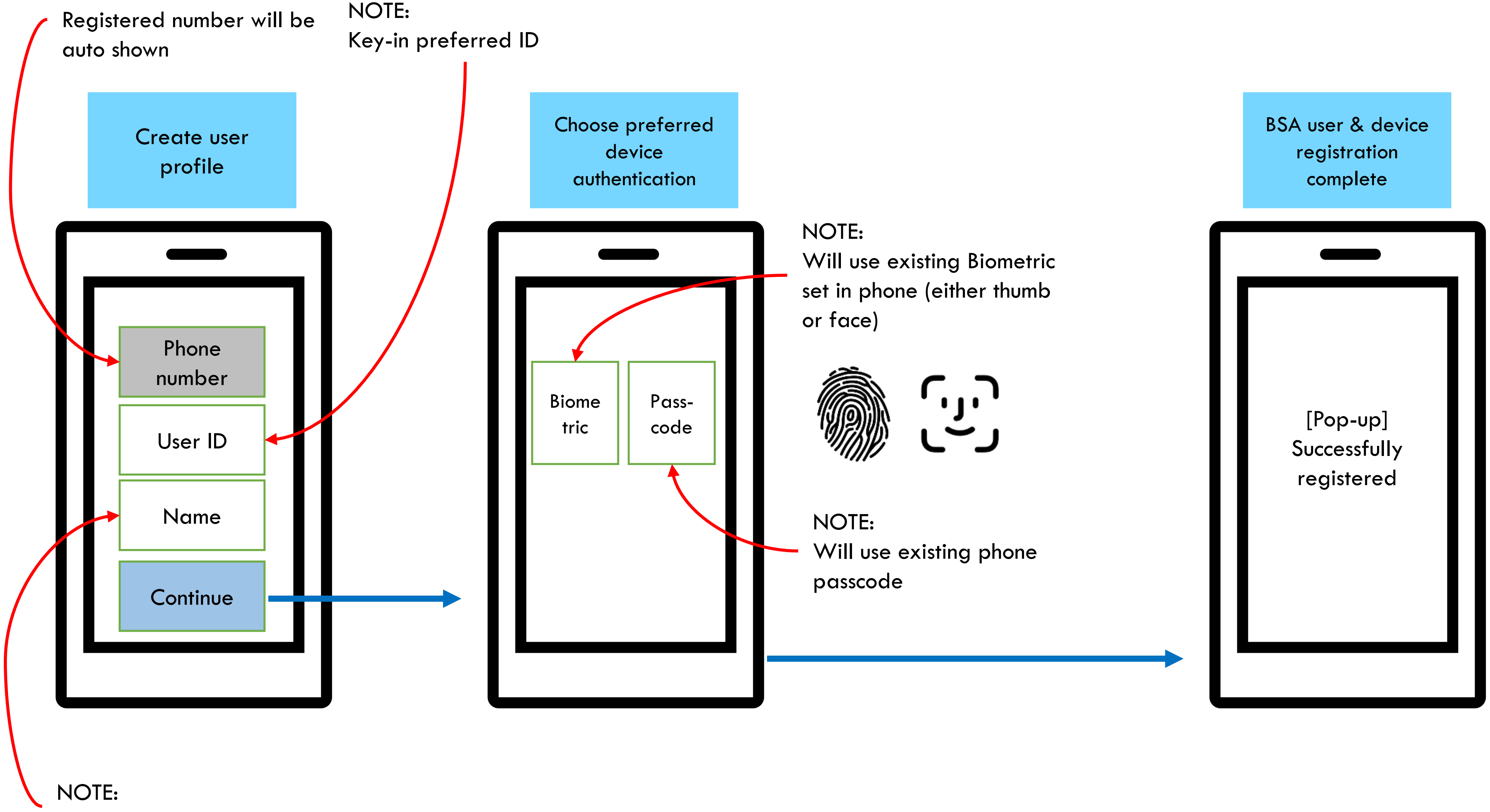
NOTE:
Key-in preferred ID

NOTE:
Will use existing Biometric set in phone (either thumb or face)

NOTE:
Will use existing phone passcode

NOTE:
Key-in preferred name

Existing user new device registration (lost/stolen/broken/new)



NOTE:
Registered number will be auto shown

NOTE:
Key-in preferred ID

Create user profile

Phone number

User ID

Name

Continue

Choose preferred device authentication

Biome tric

Pass- code

NOTE:
Will use existing Biometric set in phone (either thumb or face)

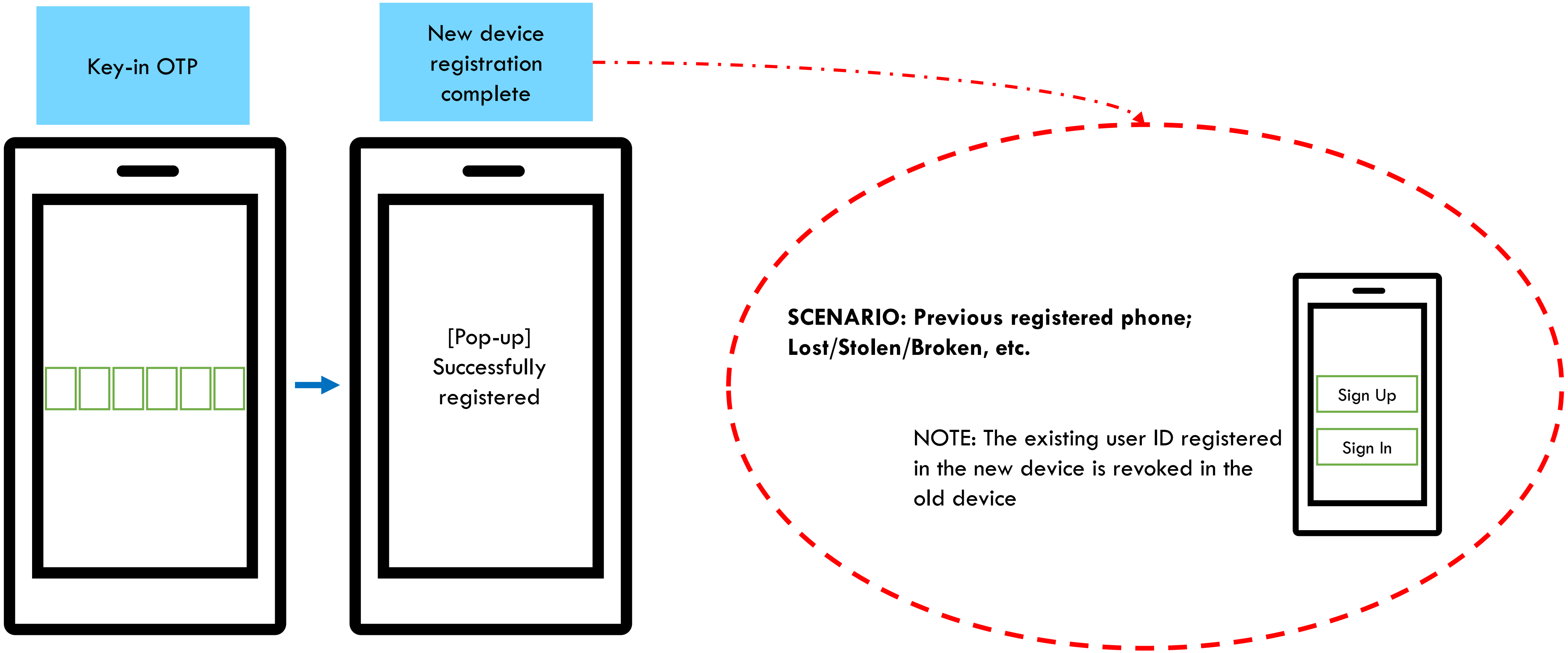
NOTE:
Will use existing phone passcode

BSA user & device registration complete

[Pop-up] Successfully registered

NOTE:
Key-in preferred name

Existing user new device registration (lost/stolen/broken/new)


Key-in OTP
New device registration complete
[Pop-up] Successfully registered
Sign Up
Sign In

SCENARIO: Previous registered phone; Lost/Stolen/Broken, etc.

NOTE: The existing user ID registered in the new device is revoked in the old device

02

ITU BSA Sandbox for DFS Regulators | Enabling Use Cases & Value Proposition

BSA Authentication Resources

For developers to implement BSA, there are two changes to make:

1. Setup a Cloud instance (ITU Cloud)
2. Web and mobile application enhancement
3. Integration (API, SDK, APK)

BSA ITU Developer Resources

- Visit https://developer.fnsbsa.com/ (ITU domain TBC)

1 - BSA Android SDK

BSA Android SDK for customer to develop their own Android Native Passwordless Authenticator with BSA SDK

2 - BSA iOS SDK

BSA iOS SDK for customer to develop their own iOS Native Passwordless Authenticator with BSA SDK

3 - BSA API for Web

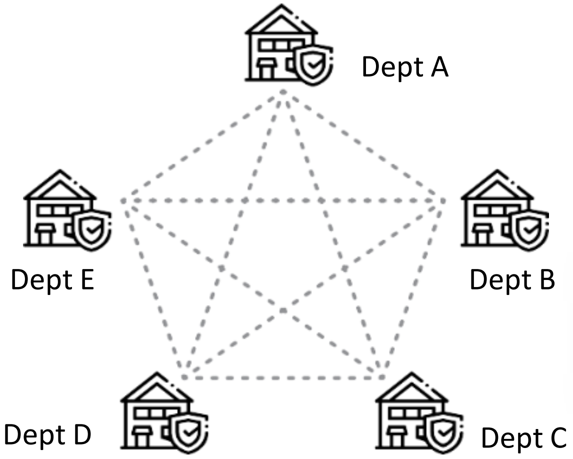
Provide Web API for Passwordless Login integration to any web application ecosystem and authenticate using BSA Sandbox app

4 - BSA App

Provide BSA demo app of FNSPay and BSA Sandbox app (iOS, Android) download

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

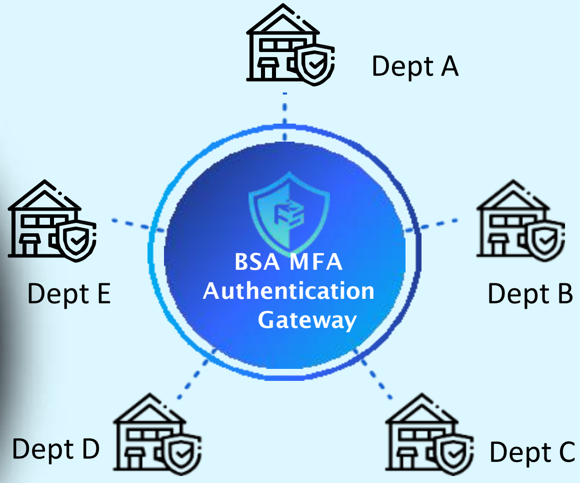
User Value

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



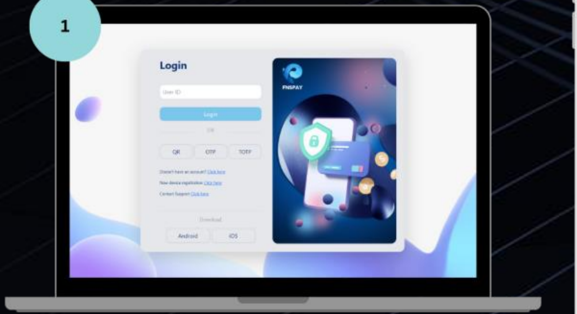
BSA MFA Authentication Services as the Secure Identity Authentication Gateway simplifies and unifies interoperability standardization of User Authentication security policy on user and device access.

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 BSA UI/UX:** Organization integrates BSA at their web portal landing page. Organizations are enabled with multiple options of logging into their web portals. 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: 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: BSA deployment managed to reduce time and cost to manage organization resources, e.g., lost, stolen or forgotten password, etc.

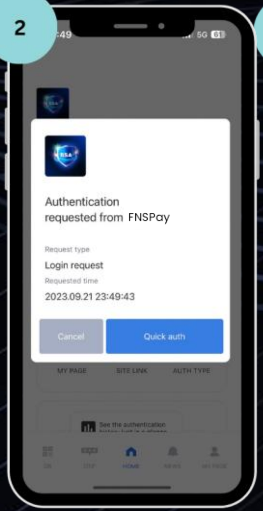
Use Case 2: Application Login

1



BSA Web Admin Portal
(Browser)

2

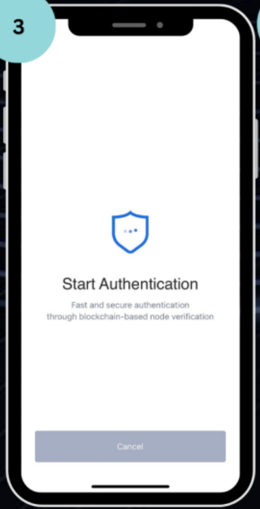

Authentication
requested from FNSPay

Request type
Login request

Requested time
2023.09.21 23:49:43

Authentication Request
Notification

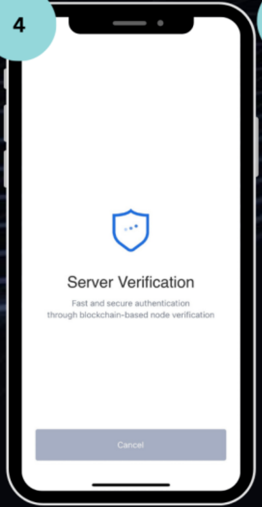
3


Start Authentication

Fast and secure authentication
through blockchain-based node verification

Start Authentication

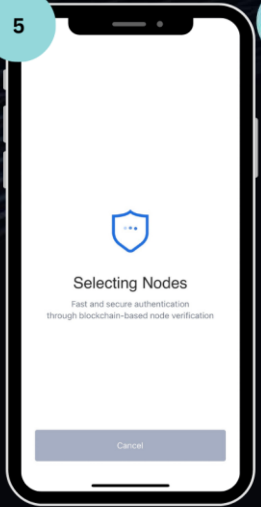
4


Server Verification

Fast and secure authentication
through blockchain-based node verification

Server Verification

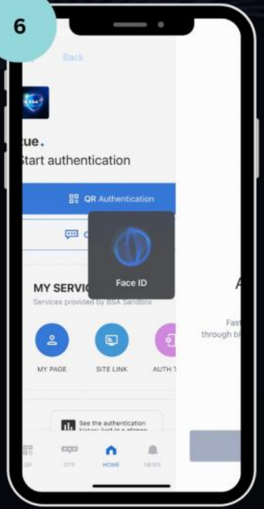
5


Selecting Nodes

Fast and secure authentication
through blockchain-based node verification

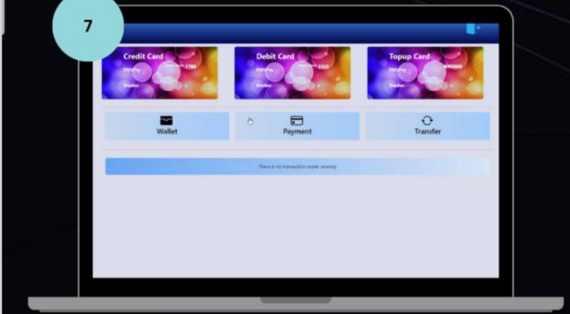
Selecting Nodes
(Node Verification)

6



Face Recognition
(Biometrics Authentication)

7

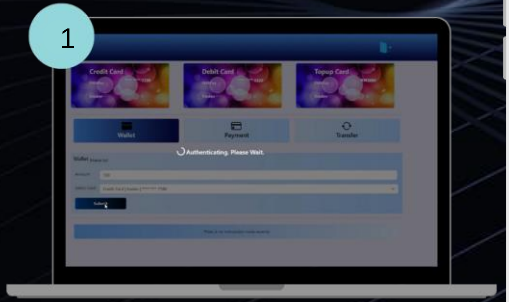


BSA Web Admin Portal Dashboard
(Browser)

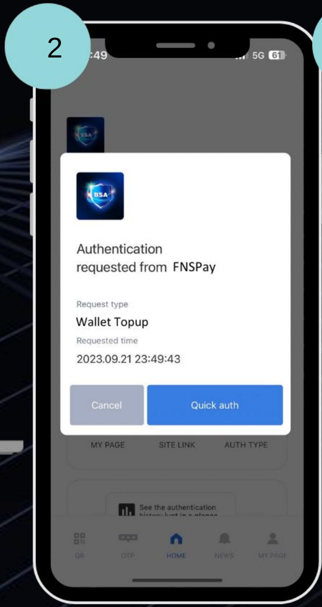
Enabling Use Case 3 | Secured Payment Approval

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 BSA UI/UX:** Organization integrates BSA at their payment web/mobile app portal. SMS OTP and tokens are replaced with One-Time Authentication 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: BSA deployment managed to reduce time and cost for managing organization resources, such as lost, stolen, or forgotten password, etc.

Use Case 3: Payment Authorization



Wallet Topup Transaction request (Browser)

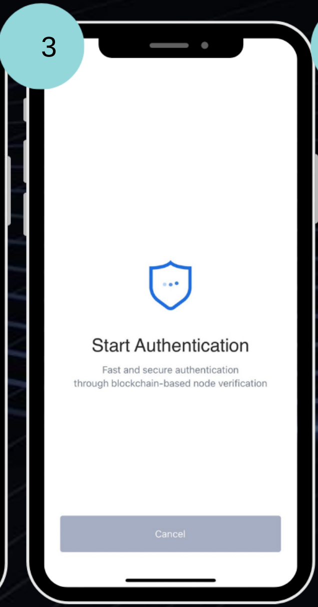


Authentication requested from FNSPay

Request type
Wallet Topup

Requested time
2023.09.21 23:49:43

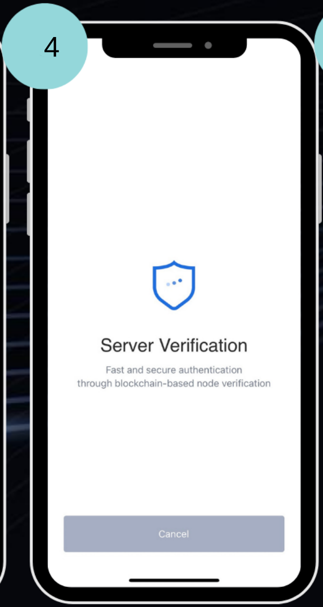
Transaction Authorization Request



Start Authentication

Fast and secure authentication through blockchain-based node verification

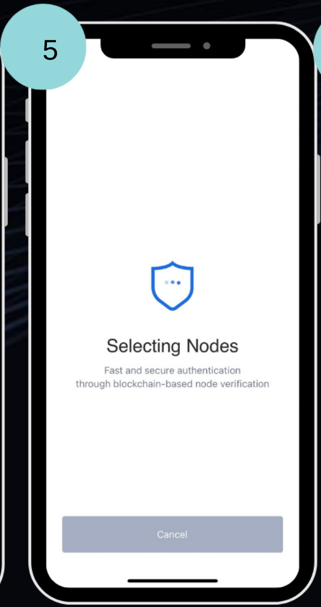
Start Authentication



Server Verification

Fast and secure authentication through blockchain-based node verification

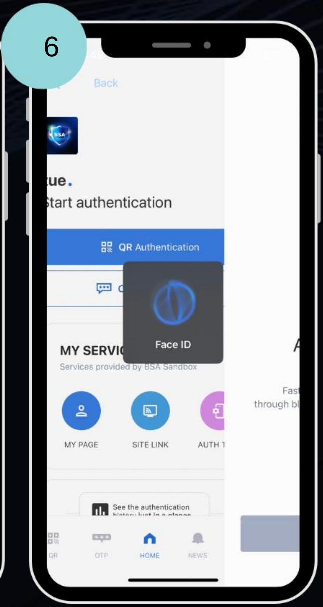
Server Verification



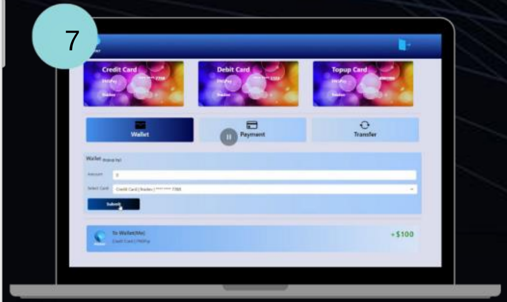
Selecting Nodes

Fast and secure authentication through blockchain-based node verification

Selecting Nodes (Node Verification)



Face Recognition (Biometrics Authentication)

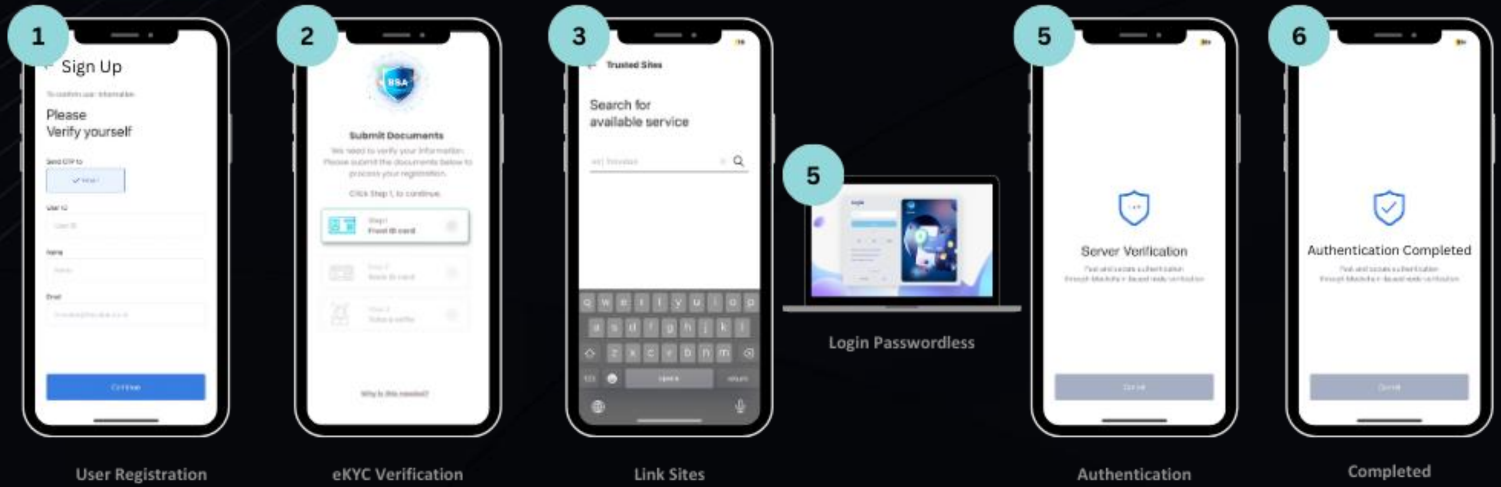


Wallet Topup Transaction Successful (Browser)

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



FNSVALUE

Thank You