ITU Digital Financial Services Blockchain Secure Authentication Application Challenge

Participation guidelines

Table of Contents

1 Introduction

The ITU BSA Application Challenge (hereinafter the "Challenge") aims to promote the utilization of Blockchain Secure Authentication (BSA) in digital financial services applications to address existing insecurities in authentication processes within DFS. The Challenge motivates developers to cultivate skills necessary for deploying BSA authentication, advocating the replacement of conventional passwords with more robust authentication protocols grounded in blockchain technology.

Reach: The first edition of the Challenge will focus on attracting developers and regulators on strong authentication DFS applications using Blockchain Secure Authentication.

- **Timeframe:** The Challenge consists of the following stages:
  A. Launching of Application and ITU Circular: 1st week of April
  B. Registration for application challenge starts: First week of April – 30 April 2024
  C. Induction Bootcamps: Weeks of 13 May, and 20 May, and 24 June 2024
     - 14 – 15 May 2024 08:00–11:30 CEST
     - 16 – 17 May 2024 14:30–17:00 CEST
     - 24 June 2024 08:00–09:30 CEST (Q&A session)
     - 24 June 2024 14:00–15:30 CEST (Q&A session)
  D. Competition: 13 May 2024 – 1 August 2024
  E. Evaluation:
     - Preliminary evaluation: Second week of August
     - Jury Evaluation: September 2024
  F. Results:
     - Awards: 13 October 2024
     - Showcase: 14 – 24 October 2024
- **Teams** comprising 1 to 5 members solve the problem statement with 4 Tasks on Blockchain Secure Authentication.
- **Problem statement:** In today's digital landscape, where safeguarding data is paramount, the reliance on passwords as the primary authentication method poses a significant challenge. Despite their widespread use, passwords often represent a weak point in cybersecurity, vulnerable to various attacks such as phishing, brute force, and credential stuffing. Many individuals opt for simplistic passwords, reuse them across different platforms, or neglect to update them regularly due to the complexity of managing multiple credentials. This behavior heightens the susceptibility of digital financial services (DFS) accounts and systems to unauthorized access and breaches. Hence, it is essential to explore, develop, and embrace innovative authentication technologies and strategies like multi-factor authentication (MFA), biometrics, and blockchain secure authentication (BSA) to fortify cybersecurity defenses, elevate user experience and trust in digital platforms, and address the global password dilemma.
- **Motivation of participants**: Participants will compete for prizes, ITU certificates and global recognition. Participants will also gain value from the opportunities to learn about implementation of BSA. The solutions from the top three participants will be showcased during World Telecommunications Standard Assembly (WTSA) and winners will be announced at the ITU Global Standards Symposium (GSS) on 14 October 2024.
- **Bootcamps**: ITU will organize a series of online bootcamps webinars to explain the problem statements and provide an online discussion forum to assist participants during the Competition Phase.
- **Prizes:** The Challenge offers a first prize of USD 5,000, a second prize of USD 3,000, and a third prize of USD 2,000, all sponsored by FNSV Co. Ltd (hereinafter "FNSV").
- All events will take place **online**.
- Participants are encouraged to submit **open-source solutions**.
- **Open source:** The Challenge encourages the submission of open-source implementations to enable a broad range of stakeholders to access the outcomes of the Challenge and continue collaborating with relevant Challenge participants.

2 Terms and Conditions of Participation

2.1. The Challenge will be open to natural persons, groups of no more than 5 natural persons, and legal persons from all ITU Member States (hereinafter "Participants")

2.2. The following persons shall not be eligible for participation in the Challenge:

a. ITU personnel;

b. members of family or household of ITU personnel;

c. individuals holding an offer for future employment with ITU;

d. individuals employed by or related to members of the Challenge Management Board;

e. individuals employed by or related to members of the Jury Panel;

f. FNSV personnel;

g. members of family or household of FNSV personnel; and

h. individuals holding an offer for future employment with FNSV.

2.3. By entering the Challenge, Participants consisting of groups (of no more than 5 natural persons) shall sign an undertaking confirming their agreement to designate and authorize one individual from among each group to accept the disbursement of a prize on its behalf in the event such a prize is awarded to that group.

2.4. By registering for participation in the Challenge, Participants accept the Participation Guidelines, including these terms and conditions.

2.5. ITU reserves the right to verify the eligibility of all Participants as well as the accuracy of their submitted information. ITU also reserves the right to disqualify Participants if it reasonably considers that the information they have provided and/or their Submissions do not comply with the terms, instructions and guidelines provided in the Challenge website (https://zindi.africa/competitions/itu-digital-financial-services-blockchain-secure-authentication-application-challenge), the Challenge online registration form, as well as the present terms and conditions.

2.6. By entering the Challenge, Participants warrant that all information submitted by them is true, complete, and up-to-date and that they are authorized to participate on behalf of their institutions/organizations (as the case may be).

2.7. Participants acknowledge and agree that their participation in the Challenge is free of charge, but does not entail any right to compensation of any kind or to reimbursement of any expenses incurred.

2.8. ITU will not provide any equipment or technical/communication infrastructure necessary to participate in the Challenge.

2.9. The Challenge will be organized and administered by ITU. Participants will follow relevant instructions available at: https://zindi.africa/competitions/itu-digital-financial-services-blockchain-secure-authentication-application-challenge

2.10. Participants' submissions must be provided in English.

2.11. Participants' submissions must not: (a) violate the intellectual property rights of third parties; (b) be illegal under applicable national laws and international law; and (c) depict or incite hatred, defame, abuse, harass, stalk, threaten a specific person or social group, incite violence or conflict or otherwise violate the legal rights of third parties (including those of privacy and publicity).

2.12. Participants' submissions must be original unpublished works that are not currently under review by under another challenge/competition or journal and must be solely owned by participants. Participants may only take credit for their own original work. Where required, Participants shall add citations and give credits to others. Plagiarism will result in immediate disqualification from the Challenge.

2.13. ITU shall not be responsible for any lost, late, corrupted, mutilated or misdirected Submissions, or Submissions not received within the established deadlines.

2.14. All participants will retain the intellectual property rights on the contents of their submissions. However, by entering the Challenge, each participant grants ITU a limited, non-exclusive, global, royalty-free right and license to use, reproduce, communicate, demonstrate, make available for public, display and distribute the content of the submissions for ITU's marketing, promotional, informational and educational or awareness purposes, via printed,

digital or online media, including ITU's website. Participants shall represent that they have the legal right to grant such license to ITU. Participants also permit ITU to use their names, likeness, video(s) and/or photograph(s) in connection with the Challenge, in any media, worldwide, at no remuneration. Participants understand and agree that the Organizers may also create content based on their updates, such as success stories, blog posts, photos or social media postings which may be published on ITU's websites, the Challenge website, as well as other communication channels and made available to the public, at ITU's discretion.

2.15. Participants may not use the ITU's name, emblems or the logos of any its events in any online or offline communication, without its prior written permission.

2.16. In addition to the terms of the general privacy notice of ITU's website, the following terms shall apply with respect to the collection and processing of Participants' personal information by ITU and its subcontractors for the Challenge:

a. Participants hereby provide their consent for the processing and storage by ITU of all contact information submitted by them to ITU (hereinafter, the "Participant Data"), for the purpose of managing their participation requests and enabling and facilitating their participation in the Challenge. Participants acknowledge that, to the extent that it is necessary, ITU may pass such Participant Data to third parties who assist ITU in the organization and management of the Challenge or provide Challenge-related services on behalf of ITU. Prior to sharing Participant Data with third parties, ITU will satisfy itself that such third parties afford appropriate protection with respect to the processing of personal information.

b. In the event the Challenge is hosted on a third-party platform, access and/or use of the respective platform may be subject to additional terms and conditions as set out by that third party, including such third party's privacy policy. Participants are encouraged to review these terms and conditions prior to deciding to participate in the Challenge.

c. ITU may also use the Participant Data to provide Participants with additional information in relation to other upcoming ITU events which ITU reasonably believes could be of interest to Participants, and to carry out surveys in relation to ITU events. Each participant may choose not to receive information related to ITU events by unsubscribing from such communications, using the "unsubscribe" link.

2.17. By entering the Challenge, Participants agree to release and hold ITU harmless from and against any and all claims, expenses, and liability, including but not limited to negligence and damages of any kind to persons and property, infringement of trademark, copyright or other intellectual property rights arising out of or relating to their participation in the Challenge and the contents of their submissions.

2.18. You acknowledge and agree that the Organizers are entitled to modify the content of the Challenge website and/or the present terms and conditions and to abbreviate, modify, suspend, cancel or terminate the Challenge (partially or in its entirety) without any obligation (present or future), by notifying you via an announcement at the Challenge website (https://zindi.africa/competitions/itu-digital-financial-services-blockchain-secure-authentication-application-challenge).

2.19. ITU reserves the right to make all final decisions regarding the Challenge.

2.20. Nothing herein shall be considered to be a limitation or a waiver of the privileges and immunities of ITU, which are specifically reserved.

3 Problem Statement

The problem statement for the Challenge is as follows:

Bank A is embarking on a transformative journey in digital banking with the introduction of the Digital Wallet Application (DWA) to be developed. This initiative prioritizes strong authentication methods to enhance customer experience and ensure secure, seamless passwordless authentication using BSA across web and mobile platforms. The DWA will facilitate convenient access to customer profiles and digital wallet services. Bank A is dedicated to providing a secure and user-friendly digital onboarding process, enabling customers to access their accounts anytime, anywhere.

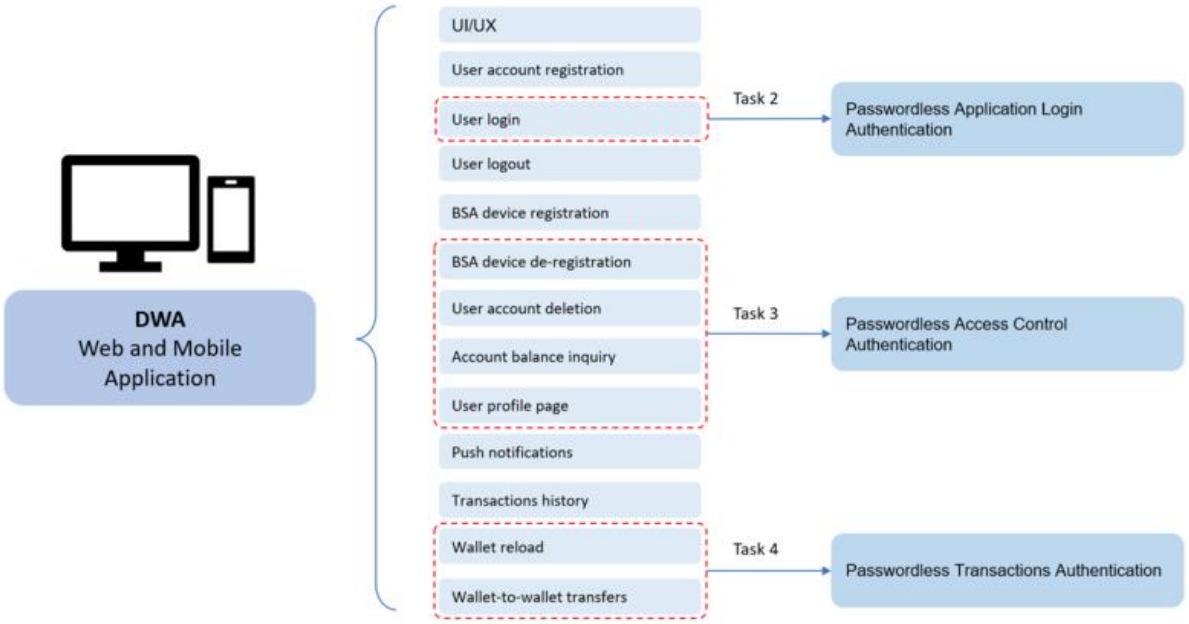
Objective:

To develop or submit an existing fully functional digital wallet application that is compatible **with both web and mobile platforms**, utilizing Passwordless BSA as the sole authentication method. Additionally, the same **mobile application will serve as the application's authenticator for Passwordless BSA.**

Key DWA Requirements:

1. **Basic Functionalities:**
    a. UI/UX (including but not limited to home page, splash screen, intuitiveness of the application flow, branding, functioning menus/buttons, overall visuals and aesthetics)
    b. User account registration and account deletion
    c. User account login and logout
    d. Push notifications
2. **Digital Wallet features:**
    a. Implement balance inquiry functionality allowing users to check their wallet balance.
    b. Include a transaction history feature enabling users to view their past transactions.
    c. Enable wallet-to-wallet transfers allowing users to send funds to other users' wallets.
    d. Implement wallet reloading functionality enabling users to add funds to their wallets.
3. **Passwordless Blockchain Secure Authentication (BSA) Authentication**
    a. Implement Passwordless BSA for 3 key components:
        i. **Login:** Users must authenticate using BSA to access the digital wallet application.
        ii. **Access Control:** Users must further authenticate to access restricted sections such as the user profile and Account Balances page.
        iii. **Payment Transactions:** BSA authentication is required before executing any wallet-to-wallet transfers or wallet reloading actions.
    b. Device Registration/Deregistration for BSA
    c. Mobile application component to function as authenticator for BSA authentication.

Here is the outline of Digital Wallet Application (DWA)'s minimum expected functionalities, including but not limited to the list below:



Participants have the freedom to exercise creativity and incorporate additional features into the DWA, as long as they meet the minimum expected functionalities.

The following items will be provided to each participant:

i. BSA Web SDK and documentation
ii. BSA Mobile SDK and documentation
iii. BSA Documentation (APK Manuals, User Onboarding Manuals, Server Provision guidelines)
iv. FNSPay Demo application and documentation (for reference)

Notes for participants:

- For mobile application development, participants shall develop on **Android platforms only.**
- The BSA-integrated mobile application will serve as the application's authenticator for Passwordless BSA.
- For the web and mobile application, participants can choose to either develop or utilize their own existing DWA.
- Participants without infrastructure for the development of the DWA may request for server provision after creating/joining a team.

3.1 Tasks for Participants

The problem statement comprises of four tasks, all participants are expected to complete all tasks. The tasks are as follows:

1. **Task 1:** Develop or utilize their own existing DWA
2. **Task 2:** Integrate Passwordless Login Authentication for user login
3. **Task 3:** Integrate Passwordless Access Control Authentication for sections including but not limited to:
    a. User profile page
    b. Account balances page
    c. Transactions history page
    d. User account deletion
    e. Device de-registration
4. **Task 4:** Integrate Passwordless Transactions Authentication into wallet reload and wallet-to-wallet transfers.

3.2 Implementation Guidelines

3.2.1 Task 1: Develop or utilize their own existing DWA

Objective

To develop or submit an existing a functional digital wallet application that is compatible with both web and mobile platforms.

Criteria:

1. **Web/Mobile Application**
    a. Develop or utilize a web and mobile DWA that includes but not limited to the following functionalities:
        i. Intuitive and seamless UI/UX
        ii. User account registration and deletion
        iii. User login and logout
        iv. BSA device registration and de-registration
        v. Account balance inquiry
        vi. User profile page
        vii. Push notifications
        viii. Transactions history
        ix. Wallet reloads
        x. Wallet-to-wallet transfers and receive
    b. Display the participant's organization logo and branding; if not applicable, use a placeholder logo/branding. Ensure the branding is consistent throughout the application.
    c. Include guides or hints for first time users to help users navigate the application.
    d. Establish a successful connection to the BSA-integrated mobile application through site linking (for the web component of the application).

Note: Participants who submit existing applications must ensure that the application includes the listed functions. While additional functions are acceptable, the application must not lack any of the required features (functionalities i-x).

3.2.2 Task 2: Integrate Passwordless Login Authentication for user login

Objective

To achieve successful integration of passwordless BSA for the login process. Participants must build and develop the DWA in web and mobile platforms, where BSA passwordless authentication is the exclusive method for user login.

Criteria:

1. **Passwordless Login Authentication**
    a. Include a login page with four methods of BSA authentication:
        i. Username
        ii. QR Code
        iii. OTP
        iv. TOTP

        Ensure all authentication methods are working as expected.
    b. The application should not use any passwords.
    c. The application's access must be restricted both prior to and during the authentication process, allowing access only upon successful completion of authentication.
    d. Implement passwordless BSA integration for web component using Web Software Development Kit (SDK).
    e. Implement passwordless BSA integration for mobile component using BSA SDK and Firebase Cloud Messaging (FCM)
    f. Complete the authentication process in under 10 seconds.
    g. Clearly display success and failure messages upon authentication

3.2.3 Task 3: Passwordless Authentication for Access Control

Objective

To successfully integrate passwordless BSA for access control within the application, and to implement BSA authentication as a mandatory requirement for accessing specific functions.

Criteria:

1. **Access Control Authentication**
    a. Incorporate passwordless BSA authentication (via biometrics or passcode) for accessing the following functions, including but not limited to:
        i. User profile page
        ii. Account balance inquiry
        iii. BSA device de-registration
        iv. User account deletion
    b. Restrict access to the specific functions until the authentication process is successfully completed.
    c. Upon successful authentication, enable access to the designated functions.
    d. Complete the authentication process in under 20 seconds, including application processing time.
    e. Clearly display success and failure messages upon authentication.

Note: Participants are permitted to integrate passwordless access control authentication into additional functions of the application; however, adherence to the above list of functions is mandatory.

3.2.4 Task 4: Passwordless Authentication for Payment Transactions

Objective

To successfully integrate passwordless BSA for payment transactions, the application is required to initiate an authentication process before executing any transactions.

Criteria:

1. **Payment Transaction Authentication**
    a. Implement passwordless BSA authentication (biometrics or passcode) for the execution of payment transactions, such as:
        i. Wallet reloads
        ii. Wallet-to-wallet transfers
    b. Restrict the reloading or transferring of wallet credits until the authentication process is successfully completed.
    c. Upon successful authentication, proceed with the complete execution of transactions.
    d. Complete the authentication process in under 20 seconds, including application processing time.
    e. Clearly display success and failure messages upon authentication.

Note: Participants are prohibited from utilizing real money or authentic payment gateways within the application. Instead, they are required to solely employ virtual numbers resembling currency for all transactions.

4 Phases of the Challenge

4.1 A: Launch and Registration

The details for the Challenge are collated on the ITU DFS BSA Application Challenge website: https://zindi.africa/competitions/itu-digital-financial-services-blockchain-secure-authentication-application-challenge

Participants can register for the Challenge at: https://zindi.africa/competitions/itu-digital-financial-services-blockchain-secure-authentication-application-challenge

- Participants will register by providing their name, email address, country, and organisation.
- Participants will receive a confirmation of their registration.
- Once registration is validated, participants will receive a confirmation email and further instructions.
- Participants will be expected to share an FCM JSON file*.
- Participants will also receive a client key by email after registration has been validated.
- Participants should start developing their application upon receipt of the confirmation email and the client key.

***Attention Participants:** Please be aware that the Firebase Cloud Messaging (FCM) SDK creates a unique registration token for each client app instance. It is crucial that this token is included in your JSON submission and shared with ITU to facilitate integration with the BSA. See instructions on how to generate the key here

4.2 B: Induction Bootcamps

Participants attend online bootcamps, organised by ITU in collaboration with FNSV, to learn about using the BSA APIs and the development requirements. FNSV may provide baseline code/SDKs as a starting point for participants. The objectives of the bootcamps are to help participants advance smoothly and submit their solutions.

The bootcamps will guide participants on the following:

a) Challenge guidelines

b) BSA Technology brief

c) Sandbox environment for trial and testing.

d) BSA architecture

e) Pre evaluation requirements

f) Evaluation criteria

g) User access to Virtual Machine – Provided on request from participants

h) Documentation on the Web APIs and Mobile SDK

i) Manual Guide BSA/FNSPay APP (for reference)

j) A discussion forum for peer and expert interaction

The Bootcamp will be conducted through a series of webinars and the schedule can be viewed on https://itu.int/en/ITU-T/dfs/seclab/Pages/challenge.aspx

4.3 C: Competition

During this phase, participants will concentrate on developing the solutions outlined in the problem statement.

Upon completion, teams must submit their applications/solutions as per the problem statement requirements, along with the following additional materials:

a. The DWA mobile APK
b. The DWA web URL
c. Provide a comprehensive report in PDF format consisting of the following:
    i. System Architecture
    ii. Process Flows
    iii. Application Manual or Guidelines
    iv. Test Scripts with results
d. Provide a 5-10 minute video demonstrating the application functionalities and authentication flow
e. Source Code to be submitted to a centralized GitHub repository.

ITU will also host a midterm bootcamp to gather feedback from teams and provide updates on their solutions to the problem statement.

4.4 D: Evaluation

4.4.1 Preliminary Evaluation

ITU conducts an initial review to verify that each submission is complete. FNSV to conduct preliminary evaluation to shortlist finalists for the final round. Preliminary evaluation will be assessed based on Sections A and B only.

4.4.2 Jury Evaluation

The Jury Panel will meet to evaluate the submissions based on the following criteria, categorized into three sections: Section A, Section B, and Section C. Section B is further segmented into four subsections, B1 to B4.

The maximum total points achievable in this Challenge is 130 points, distributed as follows:

Section	Subsection	Maximum Points
Section A: Web and Mobile Application (35 points)	No subsections	35
Section B: BSA Integration (75 points)	Section B1: Task 2 - Integrate Passwordless Login Authentication for user login	20
	Section B2: Task 3 - Integrate Passwordless Access Control Authentication	18
	Section B3: Task 4 - Integrate Passwordless Transactions Authentication	15

	Section B4: BSA Backend Integration	22
Section C: Documentation and Presentation (20 points)	No subsections	20
	Total Points	**130**

Example: To calculate the final score, let's consider Participant A who received the following scores:

a) Section A: 25 points
b) Section B1: 15 points
c) Section B2: 12 points
d) Section B3: 10 points
e) Section B4: 20 points
f) Section C: 14 points

Participant A's final score is determined by adding up the individual scores as follows: 25 + 15 + 12 + 10 + 20 + 14 = 96 out of 130 points. This translates to a percentage of 73%.

4.4.3 Evaluation Criteria

Below are the evaluation criteria, crafted to assess the effectiveness, user experience, and overall quality of the BSA integration. This evaluation criteria are divided into sections: Section A, Section B, and Section C; Sections B includes 4 subsections.

Section A: Task 1 - Develop or utilize an existing DWA

No.	Item	Aim		Sub-Item
1	Web and Mobile Application (35 Points)	Encompasses the overall design and functionality of the DWA. It evaluates the user interface (UI) and user experience (UX) aspects, including the intuitiveness of the UI, the seamless flow of the application, and the overall functionality as a digital wallet application.	1.1	Login Page
			1.2	Home Page
			1.3	Logo
			1.4	Branding
			1.5	Visuals & Aesthetics
			1.6	Navigation
			1.7	User account registration
			1.8	User login
			1.9	User logout
			1.10	User Deletion
			1.11	BSA Device Registration
			1.12	BSA Device De-Registration
			1.13	Account Balance Inquiry
			1.14	User profile page
			1.15	Push notifications
			1.16	Transactions history
			1.17	Wallet reloads
			1.18	Wallet-to-wallet Transfers
			1.19	Wallet-to-wallet Receiving
			1.20	Responsiveness
			1.21	Loading Time
			1.22	Consistency

Section B: BSA Integration

This section is divided into 4:

- Section B1 – assesses the functionality of Passwordless Login Authentication in the application
- Section B2 - assesses the functionality of Passwordless Access Control Authentication in the application
- Section B3 - assesses the functionality of Passwordless Transactions Authentication in the application

- Section B4 - assesses the integration aspect of the application

Section B1: Task 2 - Integrate Passwordless Login Authentication for user login

2	Passwordless Login Authentication (20 Points)	To assess the integration of passwordless login authentication within the application. It reviews the successful or unsuccessful integration of login authentication within the application.	2.1	Functionality of Username Authentication
			2.2	Functionality of QR Authentication
			2.3	Functionality of OTP Authentication
			2.4	Functionality of QR Authentication
			2.5	Functionality of TOTP Authentication
			2.6	No Passwords
			2.7	Authentication Speed
			2.8	Inaccessibility before login Authentication
			2.9	Inaccessibility during login Authentication

Section B2: Task 3 - Integrate Passwordless Access Control Authentication

No	Item	Aim		Sub-Item
3	Passwordless Access Control Authentication (18 Points)	To evaluate the integration of Passwordless Access Control Authentication within the application, ensuring that authentication is required before accessing specific sections within the application.	3.1	Presence of access control authentication at User Profile page
			3.2	Functionality of access control authentication at User Profile page
			3.3	Presence of access control authentication at Account Balance page
			3.4	Functionality of access control authentication at Account Balance page
			3.5	Presence of access control authentication during BSA device de-registration
			3.6	Functionality of access control authentication during BSA device de-registration
			3.7	Presence of access control authentication during User Account deletion
			3.8	Functionality of access control authentication during User Account deletion
			3.9	Error Display Message
			3.10	Authentication Speed
			3.11	Inaccessibility before Access Control Authentication
			3.12	Inaccessibility during Access Control Authentication

Section B3: Task 4 - Integrate Passwordless Transactions Authentication

No	Item	Aim		Sub-Item
4	Passwordless Transactions Authentication (15 Points)	To evaluate the integration of Passwordless	4.1	Presence of transaction authentication when attempting to reload wallet
			4.2	Functionality of transaction authentication when attempting to reload wallet

		Transactions Authentication within the application, ensuring that authentication is required before any payment transactions are made.	4.3	Presence of transaction authentication when attempting to transfer credits
			4.4	Functionality of transaction authentication when attempting to transfer credits
			4.5	Error Display Message
			4.6	Authentication Speed
			4.7	Inaccessibility before Transactions Authentication
			4.8	Inaccessibility during Transactions Authentication

Section B4: BSA Backend Integration

No	Item	Aim		Sub-Item
	Backend Integration (22 points)	To evaluate the backend integration of passwordless authentication within the application, consider factors such as the speed of authentication and the effectiveness of error handling.	1.1	Application Site Link
			1.2	Web SDK (Web component)
			1.3	BSA SDK (Mobile component)
			1.4	FCM
			1.5	Mobile application as BSA Authenticator

Section C: Documentation and Presentation

No	Item	Aim		Sub-Item
	Documentation and Presentation (20 Points)	This criterion assesses the clarity and comprehensiveness of participant submissions regarding documentation and presentations.	1.1	System Architecture
			1.2	Process Flows
			1.3	Application Manual or Guidelines
			1.4	Test Scripts with Results
			1.5	Video Documentation
			1.6	Source code

a) The Jury Panel prepares a shortlist of the top 6 participants based on the above criteria.

b) Final Presentations:

- The top 6 teams will be notified by ITU two weeks before the presentation to the Jury Panel.
- Each team will need to prepare a PowerPoint presentation of 20 minutes duration to showcase their work to the Jury Panel.

c) Finalization of Rankings:

- The Jury Panel finalize the results of the Challenge after the final presentations.

4.5 E: Showcase and Award

Solutions from the top three participants will be showcased during the World Telecommunications Standard Assembly (WTSA), and winners will be announced at the ITU Global Standards Symposium (GSS) on 14 October 2024.

4.5.1 Promotion:

- Promotion of the challenge results and winning applications follows the announcement.

4.5.2 Awards and Certificates:

- The winner and runners up of the Challenge will receive prizes as follows:
    - First prize: USD 5,000
    - Second prize: USD 3,000
    - Third prize: USD 2,000
- Certificates will also be issued for other participants that submitted a valid solution but did not rank among the top 3 teams)

5 Resources for participants

ITU with the support of FNSV, has put together the following resources provided free-of charge to registered participants of the challenge.

i. aOS SDK Guide: https://resourceaz.fnsbsa.com/itu-ac/resources/02-AC-aOS-SDK.pdf
ii. web SDK Guide: https://resourceaz.fnsbsa.com/itu-ac/resources/03-AC-Web-SDK.pdf
iii. Server Provision Guide: https://resourceaz.fnsbsa.com/itu-ac/resources/04-AC-Provision-Server-Guide.pdf
iv. FNSPay APK: https://resourceaz.fnsbsa.com/fnspay/resources/01-FNSPay.apk
v. FNSPay Manual: https://resourceaz.fnsbsa.com/fnspay/resources/02-FNSPay-Manual-Guide.pdf
vi. FNSPay Demo Slide: https://resourceaz.fnsbsa.com/fnspay/resources/03-FNSPay-Demo-Manual.pptx
vii. FCM Setting Guide: https://resourceaz.fnsbsa.com/itu-ac/resources/08-AC-FCM-Setting-Guide.pdf

6 Governance Structure

6.1 Challenge Management Board

The Challenge Management Board comprises of technical experts to advise on technical and evaluation aspects of the Challenge.

NAME	**AFFILIATION**
Norkhadra Nawawi	Marketing Senior Executive, FNS Malaysia
Radhilufti Madehi	Marketing Senior Manager, FNS Malaysia
Jay Hyung Lee	Director, Solution Business Department, FNSV Korea
SECRETARIAT	
Venkatesen Mauree	Programme Coordinator, ITU
Arnold Kibuuka	Project Officer, ITU

6.2 Jury Panel

The Jury Panel comprises individual experts who will evaluate the progress and merit of the applications proposed by participants. The Jury Panel will be set up by ITU and will finalise the evaluation criteria for the challenge. All decisions of the Jury Panel will be final.

7 Open Source

The Challenge encourages the submission of open-source implementations, based on (ITU) standards. Open-source code will enable a broad range of stakeholders to access the outcomes of the Challenge and continue collaborating with relevant participants.

8 Code of Conduct

All participants must adhere to the Code of Conduct To Prevent Harassment, Including Sexual Harassment, at UN System Events (available at https://www.un.org/management/sites/www.un.org.management/files/un-system-model-code-conduct.pdf).

9 Benefits

9.1 Benefits for participants

- Realize your dreams: Receive expert support to implement use cases and technology ideas using software and access to platforms.
- Shape the future: Opportunity to define, provide inputs and shape the technologies related to DFS authentication.
- Create your network: Network with ITU experts and peers.
- Be practical: Platform to gain hands-on experience related to BSA authentication and concepts related to future networks.

9.2 Special Benefits for certain sponsor categories

- Brand visibility
- Program opportunities
- Media opportunities

10 Contact Information

Email: dfsappchallenge@itu.int

Website: https://itu.int/en/ITU-T/dfs/seclab/Pages/challenge.aspx

Discussion board: ITU Digital Financial Services Blockchain Secure Authentication Application Challenge - Zindi