

TEST SCHEDULE & TEST PROCEDURE –v01

**TEST SCHEDULE & TEST PROCEDURE
For
App Provider Certification**

Released on: 14-Dec-2021

**CENTRE FOR DEVELOPMENT OF TELEMATICS
MANDI ROAD, MEHRAULI, NEW DELHI 110030, INDIA
ELECTRONICS CITY (PHASE I), HOSUR ROAD, BANGALORE 560100, INDIA**



Revision Chart

This document replaces: None

Document code : PMWANI-AppProvider-TSTP-PLAN-v01

Document name : TSTP for App Provider

Version/ Draft no.	Submitted on	Summary of changes	Reference Sections	Reason of change
v01d01	03-Sep-2021	None, first	All	None
v01	14-Sept02021	As per the review feedback received	Section 1.3, 2.3	As per the review feedback received

Preface

This document is intended to be used for the Certification of User App Provider against the certification criteria mentioned in WANI Architecture 2.0 on Public Open Wi-Fi Framework (Architecture & Specification).

TABLE OF CONTENTS

1. Introduction.....	5
1.1 Objective and background	5
1.2 Scope of TSTP plan.....	5
1.3 References:	5
1.4 Definitions, Acronyms and Terminology	6
1.4.1 Definitions.....	6
1.4.2 Acronyms.....	6
2. TESTING STRATEGY FOR USER APP PROVIDER.....	8
2.1 List of deliverables for TSTP	8
2.2 Pre-requisites and acceptance criteria for Certification.....	8
2.2.1 Pre-requisites for Certification	8
2.2.2 Acceptance criteria	8
2.3 Environment for Testing for Certification	9
2.4 Certification Testing methods and tools	9
3.1 Introduction.....	10
3.2 Certification Test Cases for App Provider	10
4. Summary of Test Results	13
<i>End of Document</i>	<i>13</i>

1. Introduction

1.1 Objective and background

PM-WANI framework enables proliferation of broadband in the country under distributed architecture and unbundling of infrastructure to improve performance by different players in the PM-WANI ecosystem.

There are total four players in the WANI architecture PDO, PDOA, App Provider and Central Registry. The Central Registry maintains the complete data of all the other three entities. The CR will not only maintain the data but also update in real time the XML file of PDO details with mobile App providers and PDO aggregators.

The App server and its back-end has the function of user mKYC in this framework who are going to manage all the user creation data and maintaining the mKYC Part.

1.2 Scope of TSTP plan

The test cases described in this document are for validation of App Server and its front end. It's user interface and user experience(UI/UX)and user mangement validation as well as it's data and security related transaction between UI and back-end server.

The main scope of this document to check functional requirment of WANI frame work based on Public Open Wi-Fi framework Architecture & Specification Version 2.0.

1.3 References:

1. Public Open Wi-Fi framework Architecture & Specification Version 2.0, Released by DoT, Govt. Of India
2. Wi-Fi Access Network Interface(WANI) and Framework and Guidelines for Registration, Released by Goverment of India, Ministry of Communications, Department of Telecommunications (Data Service Cell)

1.4 Definitions, Acronyms and Terminology

1.4.1 Definitions

802.11	IEEE Standards for Information Technology -- Telecommunications and Information Exchange between Systems -- Local and Metropolitan Area Network -- Specific Requirements (ISO/IEC 8802-11: 1999)
802.11a	54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
802.11b	Enhancements to 802.11 to support 5.5 Mbit/s and 11 Mbit/s (1999)
802.11i	MAC Enhancements for Enhanced Security - Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2004)
802.1X	Port based Network Access Control
802.11e	IEEE 802.11e-2005 or 802.11e is an Approved amendment to the IEEE 802.11 standard that defines a set of Quality-of-Service enhancements for wireless LAN
802.11n	High Throughput (HT) features
802.11ac	Very High Throughput (VHT) features
802.11d	Specifications for operation in additional regulatory domains
802.11h	Transmit Power Management extensions in the 5 GHz band

1.4.2 Acronyms

Table 1-2: Acronyms Used in this Document

Acronyms	Explanation
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FETP	File Transfer Protocol
GE	Gigabit Ethernet
GMK	Group Master Key
GPL	General Public License
GUI	Graphical User Interface
HTTP	Hyper Text Transfer Protocol
IP	Internet Protocol

NAT	Network Address Translation
MAC	Medium Access Control
NTP	Network Time Protocol
RF	Radio Frequency
SSID	Service Set Identification
VLAN	Virtual Local Area Network
VSA	Vendor Specific Attribute
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WFA	Wi-Fi Alliance
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup
WLAN	Wireless Local Area Network
WMM	Wireless Multimedia
WSS	WLAN Switching Solution
WSS-AP	WLAN Switching Solution for Access Point
WAC	WLAN Switching Solution for Access Controller
FET	Front End Test
BET	Back End Test
User App	PM WANI Compliant App to connect to PMWANI network
TSTP	TEST SCHEDULE & TEST PROCEDURE

2. TESTING STRATEGY FOR USER APP PROVIDER

2.1 List of deliverables for TSTP

After the validation of the User App Provider against the certification criteria mentioned in PM-WANI document on Public Open Wi-Fi Framework (Architecture & Specification version 2.0), a provisional certificate with compliance or partial compliance will be issued to the Applicant.

2.2 Pre-requisites and acceptance criteria for Certification

2.2.1 Pre-requisites for Certification

#	Deliverable	Pre-requisites for starting Testing for Certification
1.	Compliance Certificate to Applicant	Security Certificates, User App, Access to App Backend server

2.2.2 Acceptance criteria

Compliance to test cases listed in section 3.

2.3 Environment for Testing for Certification

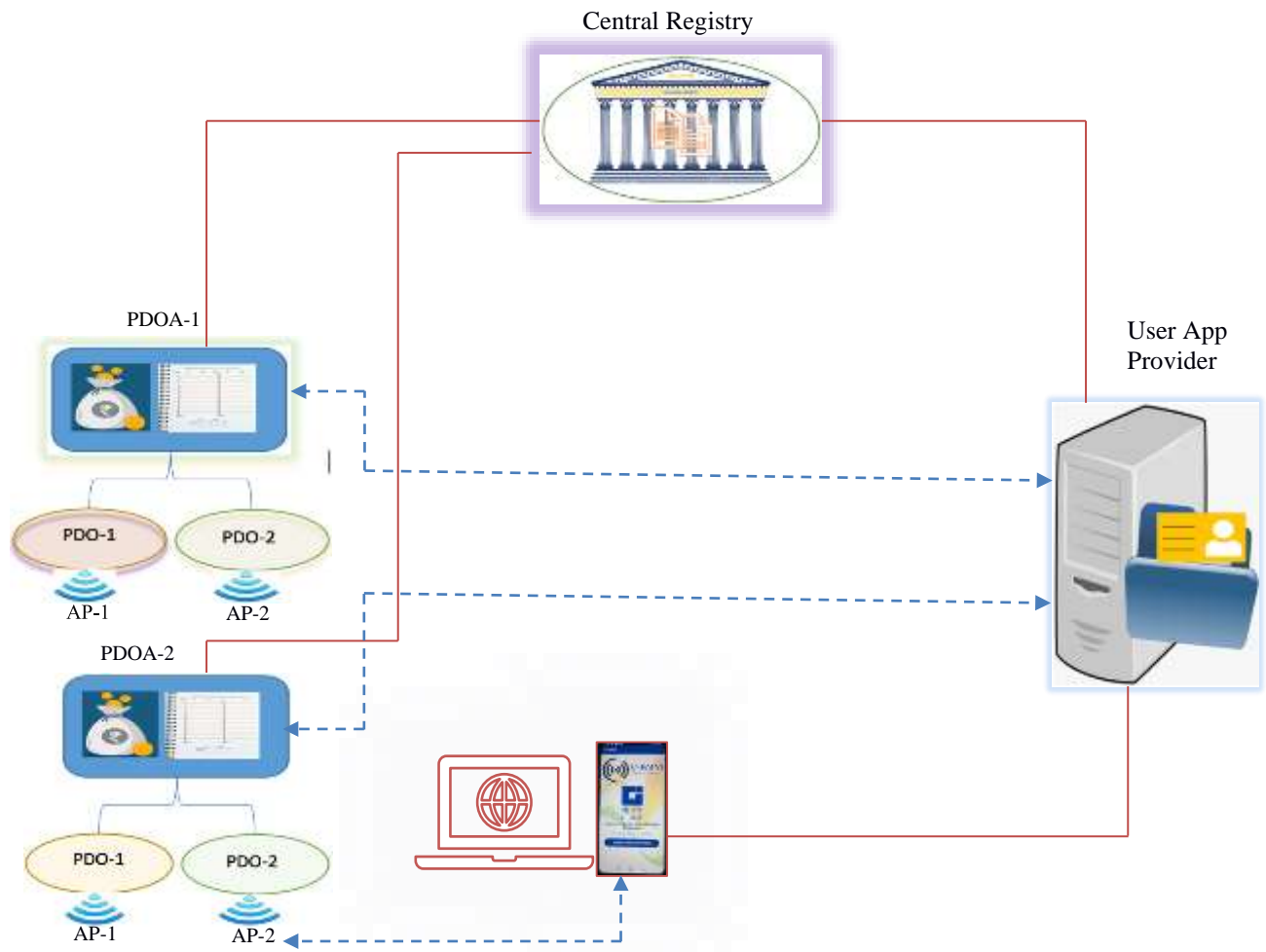


Figure 1: User App Provider Certification Testing Setup

Above Figure-1 depicts the setup for the Certification testing environment and it will be referred for the execution of the test cases.

2.4 Certification Testing methods and tools

Artifact to be Tested	Type of test	Details of tools/equipment needed
WANI_APP-Server, User App	Certification test cases based on Public Open Wi-Fi Framework (Architecture & Specification v.2.0), Functional testing as well as security testing	Linux, Penetration testing tools, smart phone(s).

3. Certification Test Cases

3.1 Introduction

This certification of the User App and App Backend Server is basic requirement of the PM-WANI frame work. In this plan mKYC functionality will also be checked.

3.2 Certification Test Cases for App Provider

Pre-requisite: Name of the User App should be provided by App Provider Server should be installed and configured and URL should be available.

Test procedure:

Test Clause No.	Clause	Mode of Test	Action to be taken
1.0	This document specifies the certification requirement of APP Provider to provide Public Wi-Fi to users under the Prime Minister's Wi-Fi Access Network Interface (PM-WANI) scheme.	General Information	
2.0	Prerequisite information from APP Provider		
2.1	Network Diagram indicating APP and its backend server network and IP address of each network node in PMWANI framework	APP Provider shall submit the network diagram	To verify if the system software of App Provider can be tested in C-DOT PMWANI Certification setup.
2.2	Details for uploading on the Central Registry for Certification testing Authentication URL (https based) Public keys to validate the signature of the APP Provider. This element will contain the base-64 encoded certificate in X509 V3 format. Currently SHA256withRSA (2048 bit key) is the supported signing algorithm.	APP Provider shall submit the details	Adding the provided details in the Certification Lab. Central Registry
2.3	APP downloadable from Play store or in the form of APK	APP Provider shall submit the details	Snapshot of successful download
3.0	Verification of APP Installation		
3.1	APP Installation from Play store on Smartphone (Android/iOS)	Test shall be conducted in Certification Lab	Snapshot of successful installation

TSTP for App Provider Certification

3.2	APP installation on latest version of Android/iOS operating system	Test shall be conducted in Certification Lab	Snapshot of successful installation
3.3	APP installation on different make and model of smart phones	Test shall be conducted in Certification Lab	APP installation will be tried on at least two make and models.
3.4	Permission such as Wi-Fi, GPS, Camera, reading SMS etc. required by APP during installation	Test shall be conducted in Certification Lab	Snapshot of the permissions sought by APP.
3.5	In case of an APP update available, verification of the update information to the end user	Declaration	
4.0	Verification of Compliance to WANI Standard V2.0		
4.2	KYC of the User using Mobile OTP	Test shall be conducted in Certification Lab	SIM for testing Snapshot of OTP received and successful authentication
4.3	Creation, view and update of User profile with “username” and “password” as mandatory fields	Test shall be conducted in Certification Lab	Snapshot of successful username creation.
4.4	Discovery of WANI compliant Reference Access points	Test shall be conducted in Certification Lab	To be tried for the following scenarios: With one WANI compliant access point With two WANI compliant access points By shutting down one WANI compliant access point
5.0	Verification of Internet Access		
5.1	Flow of waniapptoken from the APP to reference PDOA network after selecting the WANI SSID on the APP Interface. When Cellular data is OFF When Cellular data is ON	Test shall be conducted in Certification Lab	Snapshot of log at PDOA for receipt of waniapptoken
5.2	Viewing plan page of reference PDOA	Test shall be conducted in Certification Lab	Snapshot of log providing the transmission of waniapptoken response by App Provider backend
5.3	Selecting plan page of reference PDOA	Test shall be conducted in Certification Lab	Snapshot providing the Plan page of PDOA

TSTP for App Provider Certification

5.4	Purchasing the Data plan of reference PDOA	Test shall be conducted in Certification Lab	Snapshot providing the purchase of data plan.
5.5	User accessing the internet on the smartphone	Test shall be conducted in Certification Lab	Snapshot providing internet access to the user on browser and other popular apps such as Whatsapp, Youtube and Facebook
5.6	User accessing the internet on the laptop by using the “username” & “password” created during user profile.	Test shall be conducted in Certification Lab	Snapshot providing internet access to the user on browser for popular sites such as Google and Facebook
6.0	Verification of User Interface (UI) of APP		
6.1	Verification of crashing of APP on different Android/iOS version and models of smartphone	Test shall be conducted in Certification Lab	Snapshot of any crash if faced
6.2	Verification of notifications sent to the User on the APP	Test shall be conducted in Certification Lab	Snapshot of notifications received on the App.
7.0	Verification of User log		
7.1	User KYC Log indicating Mobile number used for KYC, date and time of KYC process, KYC status (success or fail)	Test shall be conducted in Certification Lab	Verification of User KYC log for the following: Mobile number used for KYC, date and time of KYC process, KYC status (success or fail)
7.2	User profile indicating username and date and time of creation.	Test shall be conducted in Certification Lab	Snapshot of log on App backend providing username and date and time of creation
7.2	User connection to PDOA network indicating PDOA ID, Username and date and time of connection.	Test shall be conducted in Certification Lab	Snapshot of log on App backend providing PDOA ID, Username and date and time of connection.
8.0	Ticket management, Phone/email for user grievances		
8.1	APP Provider shall provide a ticket management portal to users to raise complaints.	Test shall be conducted in Certification Lab	Snapshot of portal provided for raising complaints.
8.2	APP Provider shall provide Customer Care Phone number and email id on the captive portal page shown to the user	Test shall be conducted in Certification Lab	Snapshot of Customer care phone number and email ID on the captive portal page.
9.0	Interoperability with Different PDOAs		

9.1	App shall be able to access internet by connecting to different Access Points of different PDOAs present at the same location	Test shall be conducted in Certification Lab	Add the access point to different PDOA and try internet access via both the PDOs.
9.2	App shall be able to access internet by connecting to two different Access Points of different PDOAs present at the different locations	Test shall be conducted in Certification Lab	Same as above
10.0	Subscriber periodic authentication		
10.1	The App Provider shall authenticate each subscriber periodically based on some predefined algorithm.	Test shall be conducted in Certification Lab	Verify re-authentication as per the APP provider defined logic.

4. Summary of Test Results

Saral Sanchar Registration No. _____

User App Provider Name _____

App Type (Pl. Tick): **Android** _____ **iOS** _____

<i>Test Clause No.</i>	<i>Compliance</i> (Complied /Not Complied / Submitted/Not Submitted / Not Applicable)	<i>Remarks /</i> <i>Test Report Annexure</i> <i>No./Snapshot</i>

[Add as per requirement]

Date:

Place:

Signature of Applicant / Authorized Signatory

Signature & Name of C-DOT testing Officer

End of Document