

TEST SCHEDULE & TEST PROCEDURE –v01

**TEST SCHEDULE & TEST PROCEDURE
For
PDO Aggregator**

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-PDOA-TSTP-PLAN-v01

Document name : TSTP for PDOA

Version/ Dra FET no.	Submitted on	Summary of changes	Reference Sections	Reason of change
v01d01	2-Sep-2021	None	All sections	None
v01	14-Sep-2021	As per the review feedback received	As per the review feedback received respected sections updated.	As per the review feedback received

Preface

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

TABLE OF CONTENTS

Table of Contents

Table of Contents	4
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 PDO AGGREGATOR.....	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 Certification	9
2.4 Certification methods and tools	9
3.1 Introduction.....	10
3.2 Certification Test Cases for PDOA server.....	10
4. Summary of Test Results	14
Signature & Name of C-DOT testing Officer	14

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 PDOA is main part in this framework who are going to manage all the last mile premises like PDO and have all the functionality to manage the customer and provide the service to them and perform the functions relating to Authorization and Accounting. Necessary provisions shall be made by PDOA for storage of user data for one year to ensure compliance with legal provisions, as required.

The user data privacy will be ensured by App Providers and PDOAs. Complete user data and usage logs will be stored within India.

1.2 Scope of TSTP plan

The test cases described in this document are for testing of PDOA and its front end. It's user interface and user experience(UI/UX) and user mangement testing 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

The definitions for the terms used in this document are listed in the Table 1-1.

Table 1-1: Definitions Used in this Document

Definition	Explanation
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 PDO AGGREGATOR

2.1 List of deliverables for TSTP

After the validation of the PDO Aggregator server 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

S. No.	Deliverable	Pre-requisites for starting validation
1.	Compliance certificate	PDOA URL, Access of PDOA

2.2.2 Acceptance criteria

Compliance to test cases listed in section 3.0

2.3 Environment for Certification

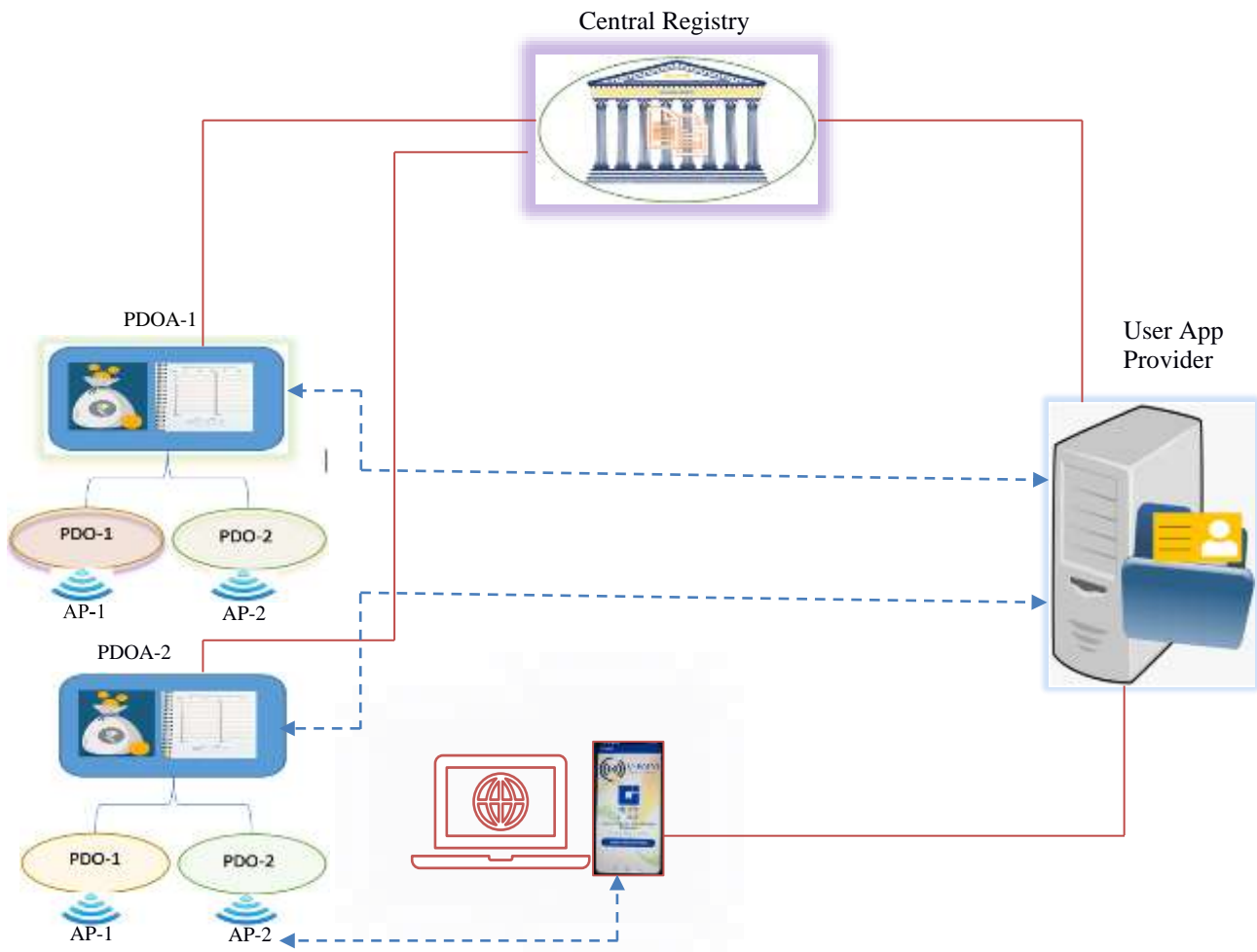


Figure 1: PDO Aggregator Testing Setup

Above Figure-1 depicts the setup for the Certification testing environment and it will be refer for the execution of the test cases. Under test PDOA should work with C-WANI App.

2.4 Certification methods and tools

Deliverable/ artifact to be Tested	Type of test	Details of tools/equipment needed
WANI PDOA Server	Certification test based on PM-WANI document on Public Open Wi-Fi Framework (Architecture & Specification), Functional testing as well as security testing	Penetration testing tools, smart phone(s).

3. Certification test cases

3.1 Introduction

This certification of the PDOA server and its Captive Portal is basic requirement of the PM-WANI frame work.

3.2 Certification Test Cases for PDOA server

Pre-requisite: Server should be installed and configured and URL should be available. PDOA Data to be configured with Central Registry for Certification.
User should be registered with C-WANI APP

Test procedure

Test Clause No.	Clause	Mode of Test	Action to be taken
1.0	This document specifies the certification requirement of Public Data Office Aggregator (PDOA) to provide Public Wi-Fi to users under the Prime Minister's Wi-Fi Access Network Interface (PM-WANI) scheme.	General Information	None
2.0 Prerequisite information from PDOA			
2.1	Network Diagram indicating Access point/router/controller connectivity to PDOA network and IP address of each network node in PM-WANI framework	PDOA shall submit the network diagram	To verify if the system software of PDOA can be tested in C-DOT PM-WANI Certification setup.
2.2	Details for uploading on the Central Registry for Certification testing Access point details (MAC ID of Wi-Fi Radio(s), SSID, CPURL, State, District, Geo Location). Public keys to validate the signature of the PDOA. This element will contain the base-64 encoded certificate in X509 V3 format. Currently SHA256withRSA (2048 bit key) is the supported signing algorithm.	PDOA shall submit the details	Adding the access point details in the Certification Lab. Central Registry
2.3	Access Point	PDOA shall bring the 2 No. of Access point to C-DOT	Verify if the access point supports Ethernet/optical backhaul. Accordingly arrange for the converter. Ensuring internet access on the access point without any proxy.
3.0 Verification of Compliance to WANI Standard V2.0			
3.1	The user shall be able to access the internet through C-DOT Reference APP installed on smartphone after clicking the SSID broadcasted by Wi-Fi Access point of PDOA and selecting a free/paid plan.	Test shall be conducted in Certification Lab	Receipt of <i>wanipdoatoken</i> on C-DOT App Backend to be verified. Verification of internet availability through

			browser and on apps such as Whatsapp, YouTube and Facebook. Procedure for the verification of token
3.2	The user shall be able to access internet on laptop after clicking on SSID broadcasted by Wi-Fi Access point of PDOA and entering “username” and “password” created in C-DOT Reference APP user profile.	Test shall be conducted in Certification Lab	Verification of most popularly used internet sites such as Google and Facebook.
3.3	PDOA software shall not directly issue “username”/ “password” to the user in the form of SMS/Email/OTP as done in conventional Wi-Fi networks.	Declaration from PDOA	
4.0	Verification of display of Captive Portal Page on WANI compliant APP		
4.1	The captive portal shall have a responsive User Interface so that it can be easily used on devices of different sizes, make/models and OS versions.	Test shall be conducted in Certification Lab	To be tried on at least two different make and models.
4.2	The captive portal shall have proper error handling and present appropriate user-friendly error messages, especially for common issues such as viewing, selecting and purchasing data plans, viewing status of data plan active or expired, data remaining in active plan, network issues, no valid plan, authentication failure etc.	Test shall be conducted in Certification Lab	Screen capture for following to be verified: Viewing Plan Selecting Plan Purchasing Plan Viewing status of active plan When app backend is not reachable No valid plan Wrong password entered
4.3	The captive portal screen shall provide user the option to view his data consumption history including session duration, devices connected, data consumed, data remaining, validity etc	Test shall be conducted in Certification Lab	Screen capture with following information to be captured: Data consumption history including session duration, devices connected, data consumed, data remaining and validity
4.4	The captive portal screen shall provide user the option to view his payment history along with details of time-stamp, payment amount, payment medium etc.	Test shall be conducted in Certification Lab	Screen capture with following information to be captured: Payment history with details of time-stamp, payment amount, payment medium
5.0	Verification of Data Plan selection by User		

5.1	PDOA shall allow a user to choose a data plan of his/her choice which is displayed on the captive portal page	Test shall be conducted in Certification Lab	Covered as part of (4.2)
6.0	Verification of working of Payment Gateway		
6.1	PDOA shall offer multiple payment options to users to purchase data plans.	Test shall be conducted in Certification Lab	(Debit card, credit card, netbanking and wallet details to be provided by the PDOA for testing)
6.2	Captive portal shall respect and handle preferred payment schemes for users and allow seamless collection of payment once the data plan is selected	Test shall be conducted in Certification Lab	Snapshot of testing done with various payment modes: Debit Card, Credit Card, Netbanking and Wallet
6.3	PDOA shall be certified with regulatory and security rules for payment transactions, auditing, and storage/handling of any sensitive payment information	Declaration from PDOA	
7.0	Verification of applicability of Data plan on PDOA network		
7.1	Users shall get data volume, validity, speed etc. as per the data plan obtained by the user (free or paid data plan) from a PDOA when connected to any Access point serviced by the same PDOA.	Declaration from PDOA	
8.0	Verification of User session Log		
8.1	PDOA shall be able to generate user session logs for each user who connects to the access point serviced by its network indicating parameters such as username, IP address of the client device, start time, stop time, data consumed, activity time, MAC ID of access point, device MAC ID, session unique ID, session termination cause	Test shall be conducted in Certification Lab	Verification of the log at PDOA having the following details: Username, IP address of the client device, start time, stop time, data consumed, activity time, MAC ID of access point, device MAC ID, session unique ID, session termination cause Timestamp should be accurate.
8.2	PDOA shall be able to generate log of each user connection indicating the APP ID from where Access is initiated	Test shall be conducted in Certification Lab	Verification of access log at PDOA having the timestamp of access along with APPID. Timestamp should be accurate.
9.0	Verification of Data Plan Purchase Log		
9.1	PDOA shall be able to generate data plan purchase logs for each user who obtains plans (free or paid) indicating time of plan	Test shall be conducted in	Same as 4.4

	purchase, plan id, amount paid, mode of payment, status of payment	Certification Lab	
10.0	Verification of User data usage log		
10.1	PDOA shall be able to generate and export the user data usage log indicating username, client device source IP, static/dynamic IP, source port number, translated IP, translated port number, destination IP, destination port number, start timestamp, end timestamp	Test shall be conducted in Certification Lab	Verification of the log at PDOA having the following details: username, client device source IP, static/dynamic IP, source port number, translated IP, translated port number, destination IP, destination port number, start timestamp, end timestamp. Timestamp should be accurate.
11.0	Ticket management, Phone/email for user grievances		
11.1	PDOA shall provide a ticket management portal to users to raise complaint.	Test shall be conducted in Certification Lab	Snapshot of the portal providing the option to user to raise complaints.
11.2	PDOA 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 the portal providing the customer care phone no. and email Id.
12.0	Wi-Fi Access point		
12.1	Access Point serviced by PDOA shall support SSID based roaming or Fast BSS Transition (802.11r) roaming	Declaration	
12.2	The Access Point or associated nodes (router/controller) shall be deployed with a storage facility so as to be able to transfer the user data usage log to PDOA after end of session or periodically after every 24 hours or frequency defined by PDOA.	Test shall be conducted in Certification Lab	Transfer of user data usage logs between Access points and PDOA to be verified as per PDOA defined policy. User data usage log at PDOA to be saved.
12.3	As backup, the Access Point or associated nodes (router/controller) shall be deployed with a minimum storage to ensure above logging of all users connected to the access point/router/controller for minimum 3 days or as defined by PDOA.	Test shall be conducted in Certification Lab	Storage available on access point to be confirmed as defined by PDOA.
12.4	Access Point should be time synchronized with the PDOA software deployed on cloud.	Test shall be conducted in Certification Lab	Timestamp on access point to be same as that of the PDOA cloud software.

4. Summary of Test Results

Saral Sanchar Registration No. _____

PDOA Name _____

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

*[Add as per requirement]****Date:******Place:******Signature of Applicant / Authorized Signatory******Signature & Name of C-DOT testing Officer******End of Document***