



सत्यमेव जयते



TRAI

20 Glorious Years
(1997-2017)



Report on **TRAI** **Public Open** **Wi-Fi Pilot**

Telecom Regulatory Authority of India, Mahanagar Door Sanchar Bhawan
Jawaharlal Nehru Marg (Old Minto Road), New Delhi: 110 002, INDIA

CONTENTS

CHAPTER-I:	Introduction	4
CHAPTER- II:	Pilot Planning	9
CHAPTER- III:	The Pilot Outcome	15
CHAPTER- IV :	The Way Forward	30
ANNEXURE I	TRAI Summary of Recommendations on Public Wi-Fi	35
ANNEXURE II	Document on Public Open Wi-Fi Pilot	37
ANNEXURE III	Public Open Wi-Fi framework , Architecture and Specification (version 0.5)	45
ANNEXURE IV	Agenda for Workshop	58
ANNEXURE V	TRAI's letter to DoT to seek permission for proposed Wi-Fi Pilot	61
ANNEXURE VI	DoT's response to TRAI's letter to seek permission for proposed Wi-Fi pilot	62
ANNEXURE VII	Wi-Fi Pilot Plan Document	63
ANNEXURE VIII	List of Registered Entities	72
ANNEXURE IX	Preview of Central Registry	75
ANNEXURE X	PDOA's/App provider Weekly Reporting Format	76
ANNEXURE XI	Wi-Fi Pilot Test System Feedback Form	80
ANNEXURE XII	Testimonials	82

ANNEXURE XIII	Stakeholders Feedback Form	84
ANNEXURE XIV	Public Open Wi-Fi framework: Architecture & Specification (version 1.0)	86
ANNEXURE XV	Sample criteria for App and PDOA Certification	103

GALLERY

**ABBREVIATIONS
USED**

CHAPTER I

Introduction

- 1.0 In its “State of Broadband 2017 Report”¹, the ITU’s Broadband Commission for Sustainable Development emphasises the role that Broadband Internet can play in meeting the Sustainable Development Goals, as set out by the United Nations. The report notes that, while creating greater productivity and other economic benefits, the Internet will also create efficiency benefits in the provision of public services. It also emphasises that the role of broadband extends beyond this to ensuring that “citizens have equitable and affordable access to information and knowledge and that their freedoms are protected, including their freedom of expression.” In particular, the Internet can significantly increase access to education for underprivileged and other groups that presently stand excluded for various reasons. Further, the report notes that “the Internet can help overcome limitations imposed by geography, physical disabilities, wealth, gender or age by facilitating citizen communications.”
- 1.1 In order to expand Broadband access, the Government has taken several initiatives to improve the digital infrastructure in the country which are in various stages of implementation. These initiatives go beyond physical infrastructure and also address software and security infrastructure as all the three aspects are required in tandem to ensure the success of Digital India. The success of Digital India further depends on the creation of an ecosystem in which every citizen is digitally empowered and has access to key services made available electronically. While the Government has been

¹ The State of Broadband: Broadband catalysing sustainable development URL: <http://www.broadbandcommission.org/Documents/reports/bb-annualreport2017.pdf>

focused on developing key technology enablers for Digital India; adoption of digital technologies has remained a challenge.

- 1.2 Apart from Internet access, the importance of continuous connectivity and its impact on the productivity and output of a nation is widely recognised. There has been increasing demand from individuals and organizations that high speed uninterrupted data services ('Always On') should be available at an affordable rate. Presently, due to the increased mobile data overload, fulfilment of users' demands is often compromised on account of unwanted network latency and congestion. A wide spread network of Public Wi-Fi hotspots can greatly improve this scenario as a complementary service. Public Wi-Fi services can enable mobile data to be dynamically offloaded/shared to ensure continuous connectivity along with desired Quality of Service (QoS).
- 1.3 In terms of technology, since its emergence on the market in 1999, Wi-Fi has been one of the greatest success stories of the high-tech era. Wi-Fi has become increasingly central in enabling access to the Internet and, can be deployed at relatively low costs. In particular, the cost per Megabyte of deploying Wi-Fi access infrastructure is substantially lower than for 3G or 4G mobile broadband networks. This translates into lower cost to the end-user as compared to other similar technologies. Owing to its low cost, the usage of Wi-Fi has been continuously increasing. Global Internet traffic is anticipated to increase by about three times to 3.3 ZB per year by 2021 from 1.2 ZB per year in 2016² and Wi-Fi, through these billions of devices, will play an important role in driving that growth. It has been estimated that Wi-Fi and mobile devices will account for 63% of IP Traffic in 2021 up from 51% in 2016.

² The Zetabyte Era : Trends and Analysis June 2017 by Cisco

- 1.4 Internationally, public Wi-Fi hotspots are playing a stellar role in delivering Broadband Internet to people. The demand for public Wi-Fi is increasing at a significant pace. The need for ubiquity and demand for high quality Internet connectivity from users is likely to further drive the growth of public Wi-Fi hotspots. As per Cisco report, the number of public Wi-Fi hotspots are set to increase from 94 million in 2016 to 541.6 million in 2021. The density of Wi-Fi hotspots will also increase from 1 hotspot for 150 people to 1 hotspot for 20 people.
- 1.5 One of the most interesting aspects of the significant changes ongoing in the public Wi-Fi ecosystem is the increase of hotspots owned or managed by venues and other brands. According to recent research conducted for iPass by Maravedis-Rethink, 50% of all commercial hotspots are controlled by brands whose core business is not telecommunications. This is because actual sign-on and allocation of passwords is often ultimately controlled by a hotel chain, group of coffee stores or a municipal authority.

Indian scenario:

- 1.6 At present, mobile network data usage in India remains dominant as compared to other forms of Internet usage. This can be attributed to a number of factors, including the cost and affordability of different broadband services, lack of fixed line coverage and relatively small number of public Wi-Fi zones. This situation highlights the need for better proliferation of public Wi-Fi networks that can offer a more affordable and flexible alternative for scaling up of Internet access.
- 1.7 The Authority noted that India significantly lags behind other countries in

terms of providing access to Broadband, especially to people in rural areas. Since there is a significant section of the population still to be connected, there is a need to take some measures so as to provide broadband services to the unconnected. This calls for introduction of new set of small players in the Wi-Fi service provisioning space, who will be able to extend their resources through a process of incentivisation.

TRAI Consultation on “Proliferation of Broadband through Public Wi-Fi Networks”:

- 1.8 Accordingly, in order to have detailed deliberations on the matter, the Authority on 13th July 2016, released a Consultation Paper on “Proliferation of Broadband through Public Wi-Fi Networks”. The Consultation Paper sought to explore the regulatory and commercial constraints that potentially hinder the growth of scalable and ubiquitous Wi-Fi in the country. This included a review of any potential licensing restrictions, measures required to facilitate interoperability between Wi-Fi networks, de-licensing of additional bandwidths for the purpose of expediting the deployment of public Wi-Fi, and several demand-side issues such as roaming capabilities, authentication and payment processes that potentially hinder the uptake of public Wi-Fi.
- 1.9 During the course of the consultation, the Authority in partnership with International Institute of Information Technology (IIIT), Bengaluru conducted a workshop on public Wi-Fi networks on 28th September, 2016. The purpose of this workshop was to explore various models of public Wi-Fi that could address the resource gap in terms of delivering public Wi-Fi in remote areas. The workshop was attended by service providers, payment solution firms and startups, Wi-Fi solution providers, Wi-Fi/ mobile device makers, academia, system integrators, Network Equipment Manufacturers, Software Vendors, and Government officials. Experts from different areas and

industry segments presented their viewpoints and shared experiences. Based on the discussions held at the workshop in relation to exploring viable models for deploying interoperable and scalable public Wi-Fi networks, The Authority also released a Consultation Note on “Model for Nationwide Interoperable and Scalable Public Wi-Fi Networks”. The Consultation Note attempted to (a) explore the roles of different stakeholders in the Public Wi-Fi network value chain and build an ecosystem for promoting scalable and sustainable partnerships for large scale nation wide deployment; and (b) explore viable models that could be adopted towards rapidly deploying affordable and interoperable public Wi-Fi networks.

- 1.10 After considering the comments from the stakeholders and further analysis, the Authority came out with its Recommendations on “Proliferation of Broadband through Public Wi-Fi Networks” dated 09th March, 2017. Summary of the Recommendations is at Annexure I.
- 1.11 In order to demonstrate a proof of concept for interoperability, the Authority decided to conduct a pilot trial of the framework mentioned in the Recommendations. Chapter II of this report describes in brief the various activities leading to the Pilot. Chapter III enumerates the sequence of events of the pilot and the results achieved. Chapter IV details the way forward and further actions required to be undertaken to achieve the objective of proliferation of Public Wi-Fi hotspots in the country.

CHAPTER II

The Pilot Planning

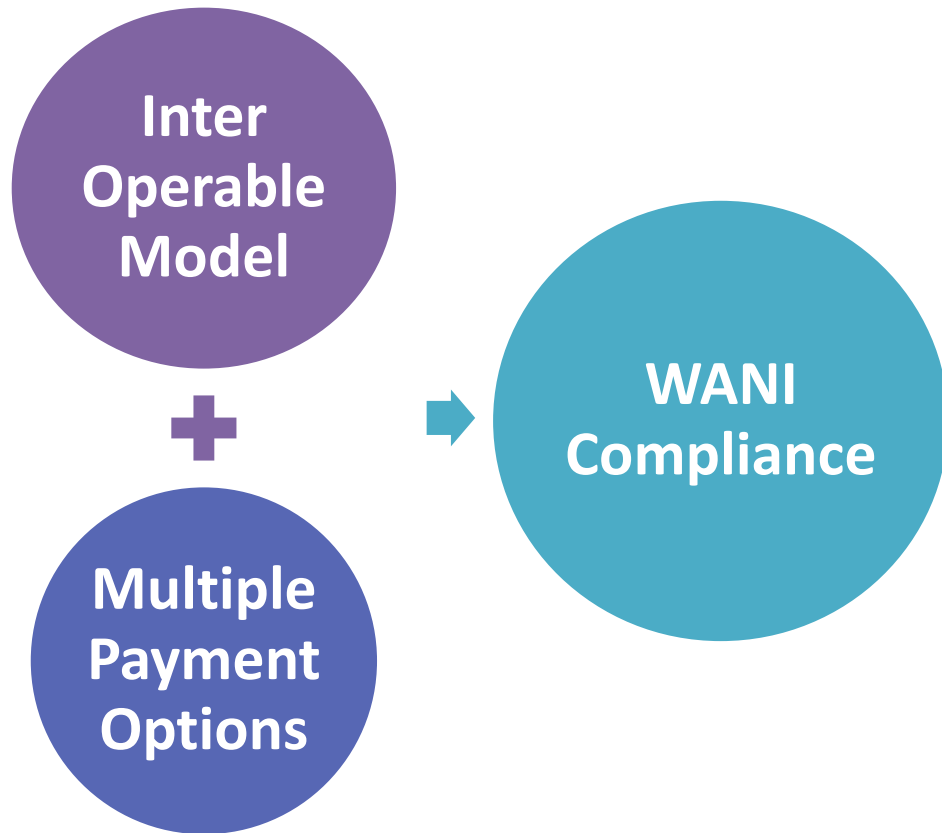
2.0 Consequent upon releasing its Recommendations the Authority decided to conduct a pilot trial. It was prudent to gauge the response from prospective participants in the pilot. Accordingly, a document titled 'Public Open Wi-Fi Pilot' was released on 07th July, 2017. The document provided details of the mission, objectives, and the participation details for the pilot and is attached as Annexure II. The stated mission and objectives of the pilot are:-

A. Mission for Wi-Fi Access Network Interface (WANI)

The vision of this initiative is to establish an Open Architecture based **Wi-Fi Access Network Interface** (WANI), such that;

- (a) Any entity (company, proprietorship, societies, non-profits, etc.) should easily be able to setup a paid public Wi-Fi Access Point.
- (b) Users should be able to easily discover WANI compliant SSIDs, do one click authentication and payment, and connect one or more devices in single session.
- (c) The experience for a small entrepreneur to purchase, self-register, set-up and operate a PDO must be simple, low-touch and maintenance-free.
- (d) The products available for consumption should begin from "sachet-sized", i.e. low denominations ranging from INR 2 to INR 20, etc.
- (e) Providers (PDO provider, Access Point hardware/software, user authentication and KYC provider, and payment provider) are unbundled to eliminate silos and closed systems. This allows multiple parties in the ecosystem to come together and enable large scale adoption. Figure 2.1 shows the pillars of WANI compliance.

Figure 2.1: Pillars of WANI



B. Objectives for the Pilot

- (a) Demonstrate that unbundling of services reduces rework, speeds up development and hence is the most effective way to tackle this complex problem.
- (b) Prove that Multi-provider, inter-operable, collaborative model increases the overall innovation in the system, dismantles monopolies and encourages passing of benefits to end user.
- (c) Test the specifications in real life conditions, and suggest improvements.
- (d) Jointly develop a business model that fairly allocates value to each provider.

- (e) Fine tune the technology and finalize the specifications based on pilot.
- (f) Test out integrated payment methods such as coupons (purchased using cash by user or gifted to user), credit/debit cards, net banking, e-wallets, and UPI.

2.1 WANI Technology Architecture and Specification (Version 0.5) document which provided necessary technology and architecture for allowing multi-provider, interoperable system across the country was released on 12th July, 2017. This was put as a draft specification which was liable to undergo changes before becoming final specifications based on feedback from ecosystem during pilot. A copy of the document is attached as Annexure III. The broad outlines of the Architecture are:-

2.2 **High Level Architecture**

A. **Players in the ecosystem**

PDO/PDOA: Any Indian entity (companies, associations, small merchants, etc.) having a PAN number wanting to provide one or more WANI compliant Wi-Fi hotspots to public using either free or paid model. They conform to the governing rules laid out by TRAI under this framework.

B. Hotspot Hardware/Software/Service Provider: Any software or service provider who is providing necessary software, hardware, services, and/or support for PDOs to setup WANI compliant Wi-Fi hotspot. These can be any software/service provider, either Indian or global. It is expected that these providers will offer a Wi-Fi-in-a-box solution for PDOs. Their software will need to be compliant to specifications laid out in this document. They will also integrate with a bank or a payment gateway for collecting payment from user.

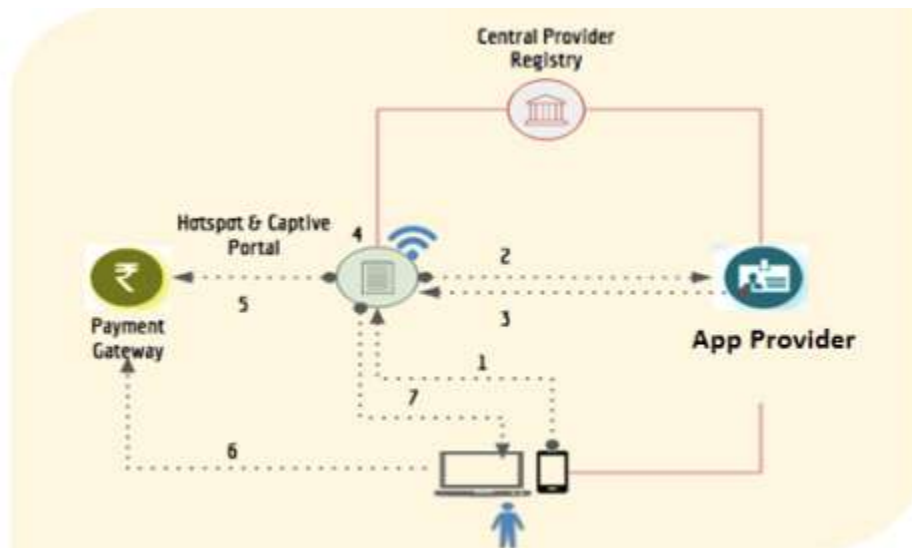
- a. User App Provider: Any company providing a software application and backend authentication infrastructure for users to signup,

discover WANI compliant Wi-Fi hotspots, and do single-click connect from within the app. This app allow users to create a profile, do their KYC (mobile verification), and allow setting up preferences for MAC-IDs for various accessing devices and payment methods. This app should allow users to discover WANI compliant hotspots and connect to it. In addition, App Provider must offer a backend user authentication service that is called by Wi-Fi Captive Portal software whenever user connects to obtain a signed user profile.

- C. Central Registry of Providers (or simply Provider Registry): A central registry managed by DoT/TRAI or an entity approved by DoT/TRAI containing information about the PDOs/PDOAs, and User App providers in a digitally signed XML format. This is a relatively static registry where approved providers are allowed to manage their profiles.

D. High Level Flow

Figure 2.2 Depicts the High Level Flow of WANI Architecture



E. One Time Flow

One time flows are depicted in red lines in above diagram.

PDO/PDOA completes Self-Registration with Provider Registry using their public certificate (for signature validation). They also register their Wi-Fi Access Points, SSIDs, and locations.

User App provider is also registered with Provider Registry along with their authentication URL and public certificate (to validate their digital signature).

User completes one time KYC with App Provider through their App. User App caches trusted SSIDs from Provider Registry from time to time.

F. Usage Flow

Usage flows are depicted in dotted lines in above diagram. Bullet number below corresponds to the number depicted within the diagram above.

- a. User opens the App in which user has already registered and allows discovery and connection to WANI compliant Wi-Fi access points. Within the app, user browses for nearby WANI compliant SSIDs and then chooses one SSID to connect to.
- b. Wi-Fi Captive Portal of the PDO initiates user authentication with App provider backend using the token passed from the app.
- c. App provider backend returns a signed user profile token back to Wi-Fi Captive Portal.
- d. Wi-Fi Captive Portal displays data packs available with their charges. User selects desired data sachet, click to confirm the terms.
- e. Wi-Fi Captive Portal sends request for payment through their payment gateway.
- f. User completes payment.
- g. PDO activates all device MAC-IDs that were part of the signed profile and allows them to connect to the session without additional authentication. Pack is activated and user can begin browsing.

- 2.3 With a view to gauge the response from prospective stakeholders a Workshop on the subject was organised at Bengaluru on 25th July, 2017. The same was targeted at Public Data Office Providers/Aggregators (PDO/PDOA), App providers and Hotspot Hardware/Software/Service Providers. Agenda of the Workshop is attached at Annexure IV. A very enthusiastic response was received from the participants during the Workshop.
- 2.4 The Authority thereafter, approached DoT vide letter dated 11th August, 2017 (Annexure V) to seek permission for proposed Wi-Fi Pilot. In response DoT vide its' letter dated 18th September, 2017(Annexure VI) accorded permission to carry out the trial subject to certain safeguards.

CHAPTER – III

The Pilot Outcome

3.0 Activities for the Pilot commenced with the release of the Pilot plan(Annexure VII). The document enlisted the timelines and the procedural and operating guidelines. These are :-

Timelines

Publish procedural guidelines	15 Sep 2017
Host Central Registry	20 Sep 2017
PDOA & Consumer App Registration	03 Oct 2017
Pilot Go Live Date	16 Oct 2017
Pilot End Date	30 Nov 2017 (subsequently revised)
TRAI Report on the Pilot	15 Dec 2017 (subsequently revised)

Procedural Guidelines

1. It is expected that Software/Hardware/ISP providers will work directly with PDOAs for the pilot.
2. TRAI will work with Consumer App Providers or PDOAs directly for the pilot.
3. PDO/PDOA completes Self-Registration with Provider Registry using their public certificate (for signature validation). They also register their Wi-Fi Access Points, SSIDs, and locations.
4. User App provider is also registered with Provider Registry along with their authentication URL and public certificate (to validate their digital signature).
5. User completes one time KYC with App Provider through their App. User App caches trusted SSIDs from Provider Registry from time to time.

Operating Guidelines

1. SPEED: Each PDO/PDOA has to offer a preferable speed of 2Mbps to every customer.
2. SECURITY: From Access Point(AP) to the registry server IPSEC/GRE tunnel needs to be implemented .
3. KYC: eKYC-wherein it should be linked to Aadhaar card. Alternatively m-KYC based on OTP can also be used.
4. DATA STORAGE: It should be capable of withstanding any cyber attack including malware and Denial of Service(DoS) protecting customer's privacy & data.

3.1 The document also provided a template for operating practice to be submitted by the PDOAs/App providers. Registration under the following categories was carried out for various entities which expressed interest in participation:-

- (a) PDO/PDOA
- (b) App Provider
- (c) Hardware/Software/Service Provider

3.2 List of entities which registered under various categories is attached at Annexure VIII.

3.3 As specified in the architecture the central registry shall be managed by DoT/TRAI or an entity approved by DoT/TRAI containing information about the PDOs/PDOAs, and User App providers in a digitally signed XML format. A preview of the same is attached as Annexure IX. For the pilot it was decided to host the central registry on the TRAI website

Current Status

3.4 The pilot commenced on 16th October, 2017. The entities were required to establish their Access Points at locations of their choice. Figure 3.1 shows the

spread of PDOs across the country. Figure 3.2 shows the time window for which the Access Points were made available by the PDOAs.

Figure 3.1: Spread of PDOs across the Nation

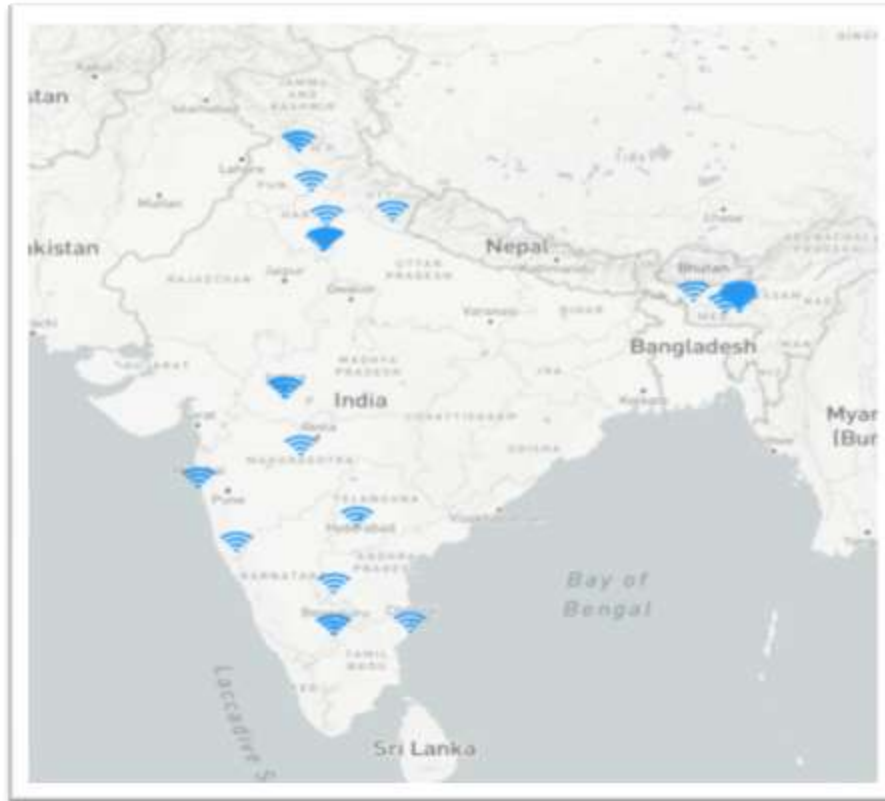


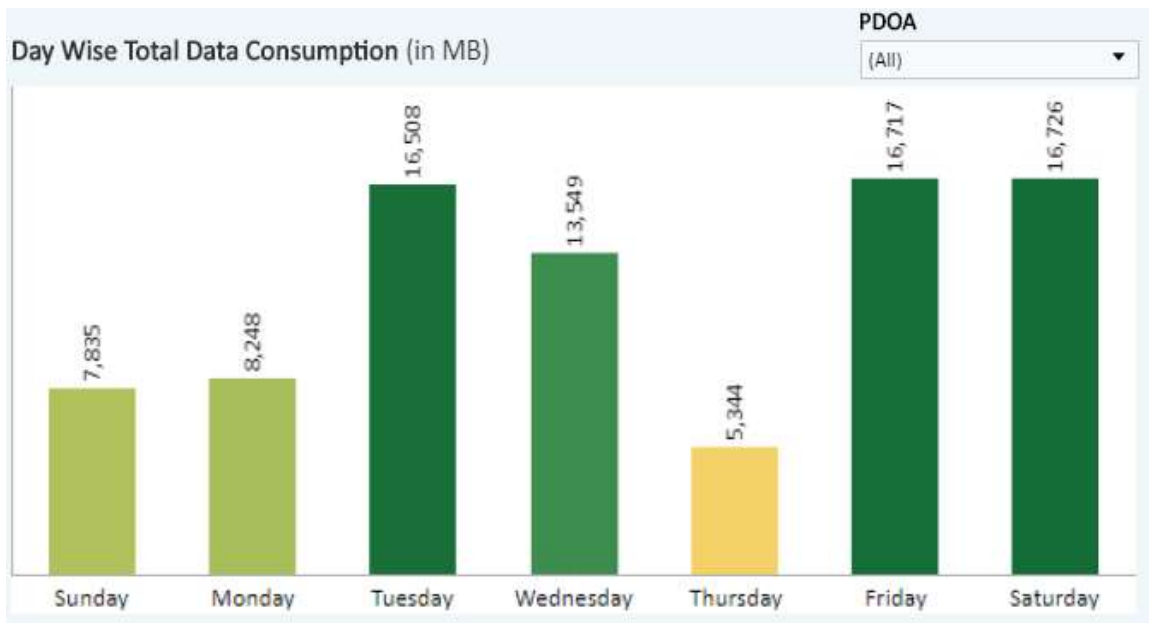
Figure 3.2: Time Window for Hotspots availability

Open Between (in hrs)	Airjaldi Networks Pvt. Ltd.	Bluetown	C-DOT	Citycom Networks Private Limited	Coyledon Technologies	CSC e-Governance Services India Limited	Dexworks Labs Private Limited	Febier technologies	MPG Digital Platform P.Limited	Omnia Information Private Limited	ONEHOP NETWORKS	Techzone Academy	Wifi Dabba	XiFi Smart Networks Private Limited
07-21								📶						
08-21								📶						
09-18												📶		
09-19						📶				📶				
09-21					📶									📶
09-22										📶				
10-18					📶									
10-23							📶							
11-23							📶							
24hrs	📶	📶	📶	📶		📶	📶		📶		📶		📶	

- 3.5 In the last week of October, 2017 a team from TRAI visited Bengaluru to ascertain the progress of the pilot. The team went to the field sites and noticed that although the Access Points were operating independently, some difficulties were being faced in migrating to WANI architecture. It was thereafter decided to get all the participating entities to interact with each other. Accordingly on 03rd November, 2017 the representatives of participating entities assembled at TRAI offices at Delhi and Bengaluru and various aspects related to the WANI architecture were clarified through video conferencing.
- 3.6 The participating entities were prescribed to submit weekly report as per the format at Annexure IX.
- 3.7 While the entities were tirelessly working to achieve the WANI compliance, TRAI initiated the launch of its Wi-Fi Pilot webpage. The webpage was prepared to host the Central Registry and provide the details of the participating entities.

- 3.8 A Dashboard was also prepared to show the following information at a glance
- Number of PDO's marked over map of India in accordance to their geo-location.
 - Data Usage trend for each PDOA according to the reporting done by them as shown in Figure 3.3
 - Number of sessions and unique customers connected.
 - Further analysis and visualization on the parameters such as Average speed, Free minutes usage, Time window.

Figure 3.3: Data visualization of weekly PDOA usage trend



- 3.9 The initial weeks of reporting majorly witnessed nil reports, as the entities strived to achieve WANI compliance. Few of the entities sent the data usage of

their non WANI compliant system as well, thus a surge in the numbers can be seen in the Dashboard.

- 3.10 The race to achieve the WANI compliance in the PDOA category was led by M/s WifiDabba, a Bengaluru based start-up, followed by M/s Omnia Information Pvt. Ltd, a start-up based out of Delhi. Yet, a need for WANI compliant application provider was felt, for the PDOA's to test and fix out any bugs during run time.
- 3.11 The pilot also witnessed some of the late entrants, Facebook through its rural broadband partner AirJaldi Networks Pvt. Ltd participated in the pilot. AirJaldi deployed 2 of its access points in Kangra district of Himachal Pradesh and one in its branch office in Delhi. AirJaldi Networks with its perseverance and technical assistance from TRAI, managed to achieve WANI compliance in a very short time.
- 3.12 The other player that entered into the later phase of the pilot was CSC-e-Governance Services India Ltd. CSC hotspot network spreads across the whole nation, with the count of approximately 70,000 access points. CSC participated in the pilot with two of its access points installed at its Okhla Office.
- 3.13 Omnia information Pvt. Ltd. was the first participant to be able to develop a WANI compliant PDOA system. Figure 3.4 shows the Wi-Fi solution proposed by Omnia Information. Following the footsteps of Omnia, WifiDabba soon came into the league of achievers. Figure 3.5 shows a tea shop at Bengaluru serving as a PDO of WifiDabba.

Figure 3.4 : i2e1 Wi-Fi Solution for the Wi-Fi pilot



Figure 3.5 : Tea shop in Bengaluru as WifiDabba PDO



3.14 Considering the fact that only a few entities were able to achieve the WANI compliance, with the approaching deadline, TRAI decided to extend the end date of the pilot to 15th January 2018, giving additional 6 weeks time. The decision came up on the context that most of the participants were on the verge to achieve the interoperability, the basic requirement of WANI compliance.









Development of Mobile App

3.15 The success of the pilot was contingent on a WANI compliant app, to which these PDOA's could be tested. On 28th November 2017, Mobile Motion Technologies, a Bengaluru based participant, developed a WANI compliant android application, with the name Wifire. By the end of the pilot following entities were able to field a WANI compliant app

- (a) Mobile Motion Technologies- Wifire App(Android and iOS version).
- (b) Omnia Information Ltd- *Wi-Fi SwApp* (Android version).
- (c) One97 Communications Pvt. Ltd WANI compliant version of *Paytm* app(Android version).

3.16 The total number of access points installed by various participating entities is as listed in Figure 3.6.

Figure 3.6: Entity wise access point listing

	Omnia Information Pvt.Ltd. <ul style="list-style-type: none">• No. of Access Points installed: 157
	WiFi Dabba <ul style="list-style-type: none">• No. of Access Points installed:430
	Cotyledon Technologies <ul style="list-style-type: none">• No. of Access Points installed: 3
	Febler Technologies <ul style="list-style-type: none">• No. of Access Points installed: 2
	Xi-Fi Networks <ul style="list-style-type: none">• No. of Access Points installed: 2
	Airjaldi Networks Pvt. Ltd. <ul style="list-style-type: none">• No. of Access Points installed: 3
	OneHop Networks Pvt. Ltd. <ul style="list-style-type: none">• No. of Access Points installed:4
	CSC - e Governance Services Limited <ul style="list-style-type: none">• No. of Access Points installed: 2

3.17 On 13th January 2017 it was decided by TRAI to deploy the access points at its Bengaluru and Delhi office to perform the load testing of the developed system with all the successful entities. The move was intended to carryout live testing and to identify any shortcomings.

3.18 By this time, entities were ready to provide both the offline (coupon) and online payment options (wallet, credit card, debit card, UPI, Netbanking). Figure 3.7 shows the preferred payment partner of the entities. The

integration of the payment partners/gateways enables the subscribers to have multiple payment options.

Figure 3.7 : Entity wise opted Payment Partner.

Entity	Integrated payment provider
Wi-Fi Dabba	 
I2e1 (Omnia information)	 
Febler Technologies	
Cotyledon Technologies	
One hop networks	
Airjaldi Networks	 

3.19 The period of testing lasted for 15 days. All officers and staff of TRAI were instructed to make maximum use of the ‘Wi-Fi Pilot Test system’ installed. To acquaint the users of the newly developed system, a user guide (Annexure X) was also prepared. A Live Demonstration of system was organised wherein, demonstration of the app usage and the login procedure was carried out.

3.20 Figures 3.8 and 3.9 show the various access points installed at the TRAI Delhi Office.

**Figure 3.8: Airjaldi access point
deployed at TRAI office, Delhi**



**Figure 3.9: i2e1 Access Point
deployed at TRAI office, Delhi**



3.21 After the completion of the testing period, the usage data was analyzed on various aspects. The summary of the same is depicted in the Figures below:

Figure 3.10

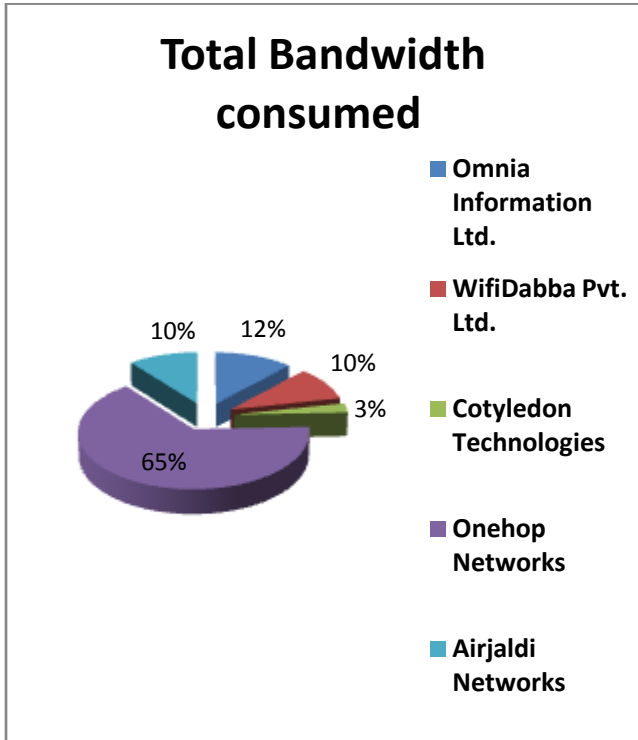


Figure 3.11

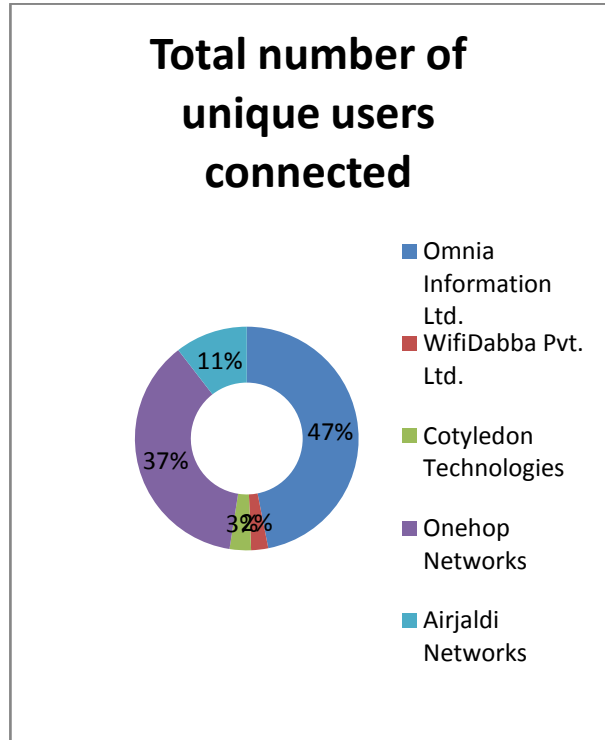


Figure 3.12

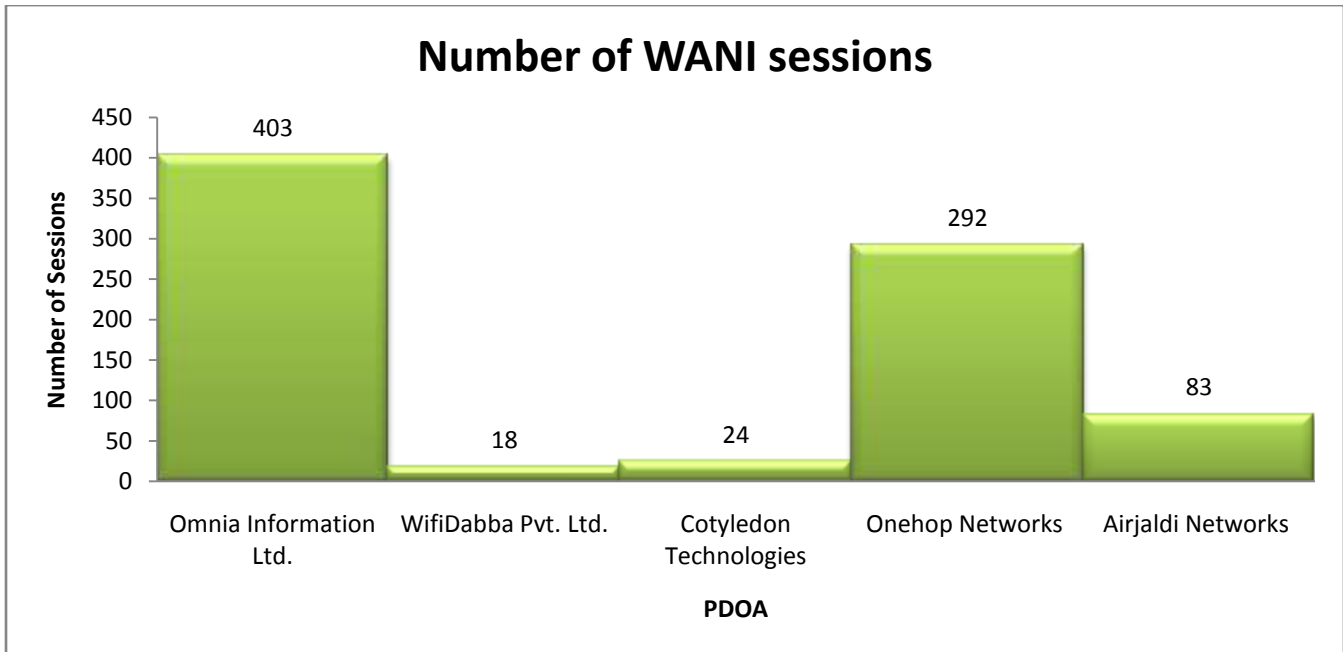


Figure 3.13

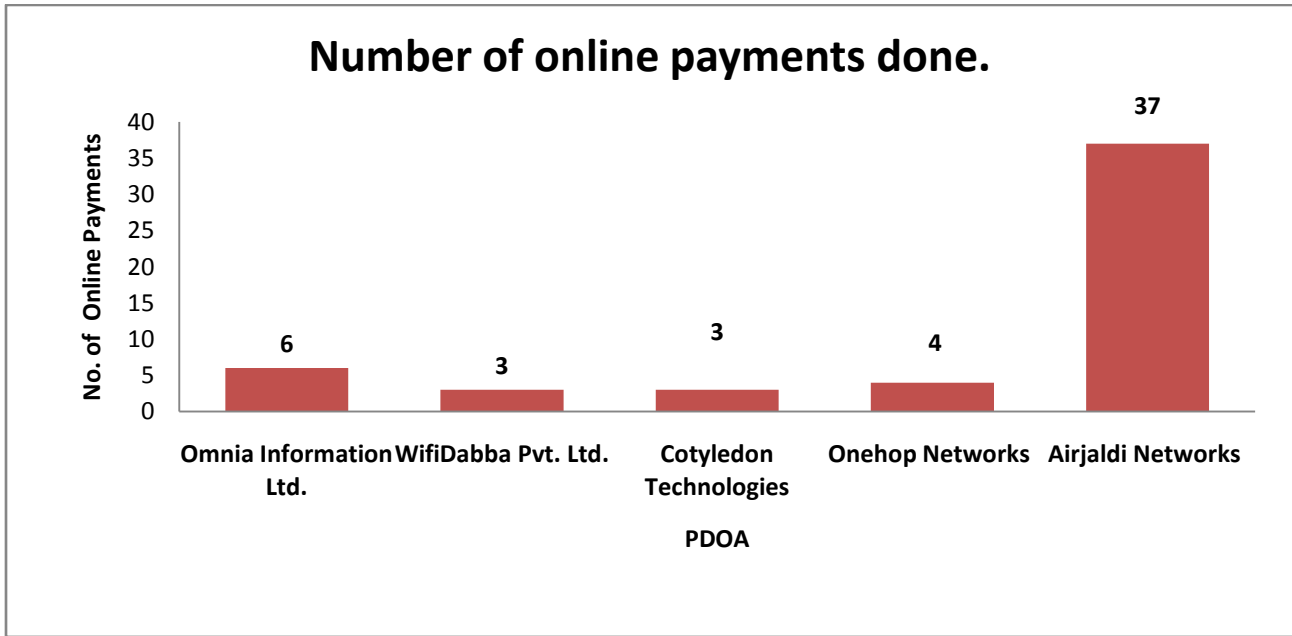
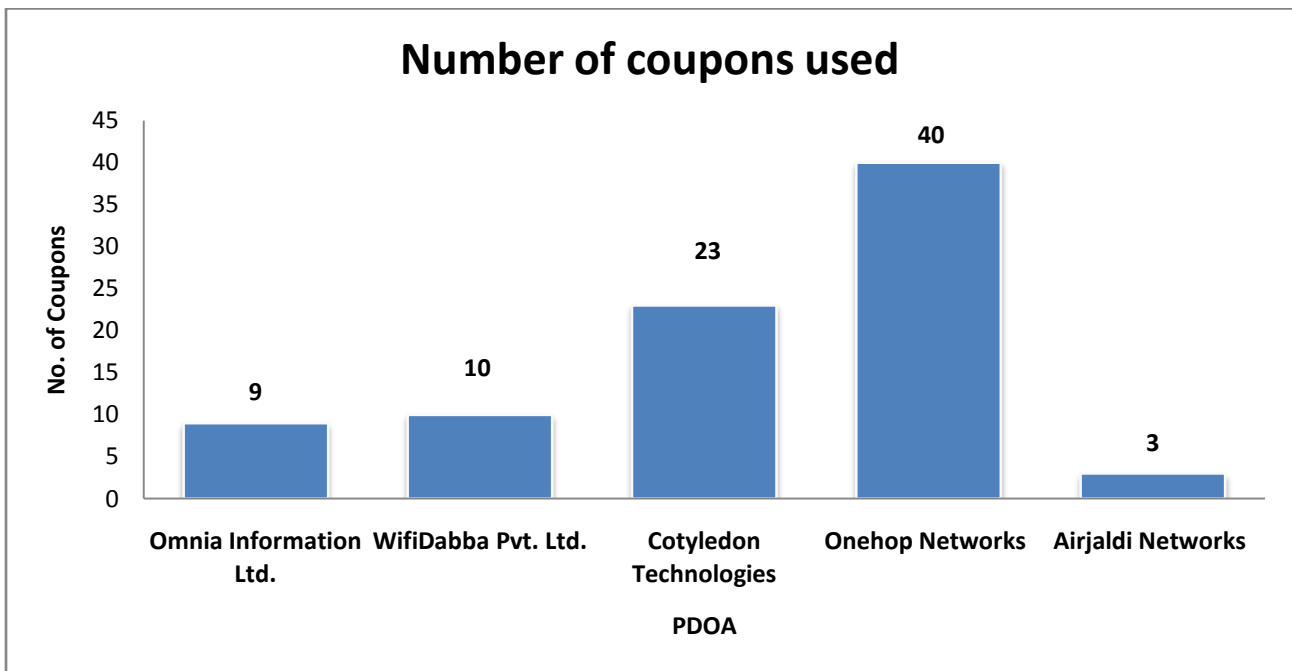


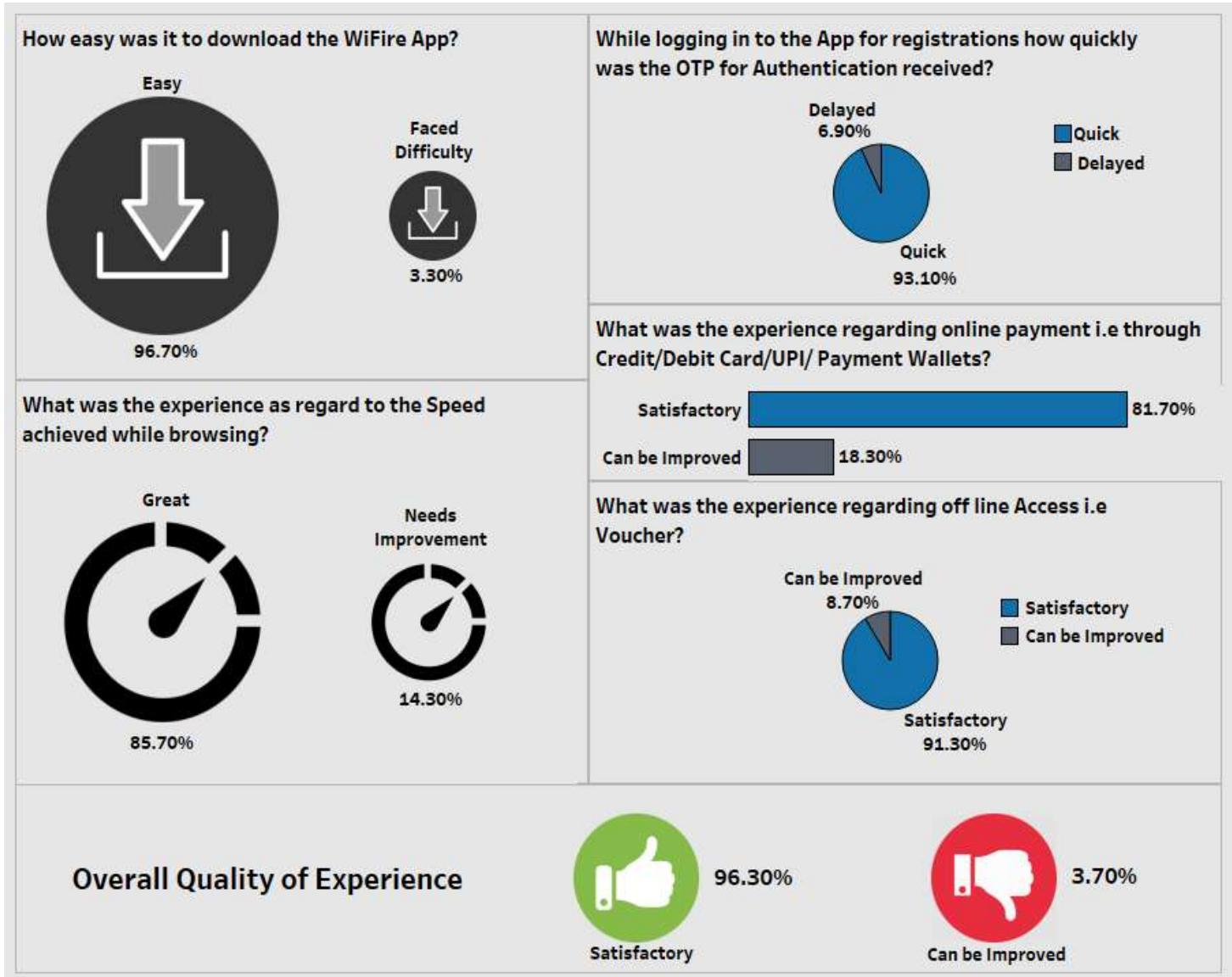
Figure 3.14



3.22 After the completion of testing period feedback was sought from the staff of Delhi and Bengaluru TRAI office, to know the level of contentment among the users. A detailed feedback form (Annexure XI) was prepared for the same.

3.23 With the intent to improvise the system so as to converge it to perfection, TRAI opened the stage for suggestions, through its feedback mechanism. Figure 3.15 shows the detailed analysis of the user experience.

Figure 3.15



- 3.24 The success of the pilot can be gauged from the fact that 96.3% of the persons found the system user friendly. 3.7% of the persons believed that there is still a scope of improvement. The suggestions received have since been incorporated to further refine the system. Some testimonials of PDOs and users are at Annexure XII.
- 3.25 In the Architecture document it had been clearly mentioned that “*This is a draft specification which may undergo changes before becoming final specifications based on feedback from ecosystem during pilot*”. Accordingly, feedback was obtained from the various participating entities as per the form at Annexure XIII. The suggestions were deliberated upon and the ‘Public Open Wi-Fi framework: Architecture & Specification’(version 1.0) document has been prepared (Annexure XIV).

CHAPTER – IV

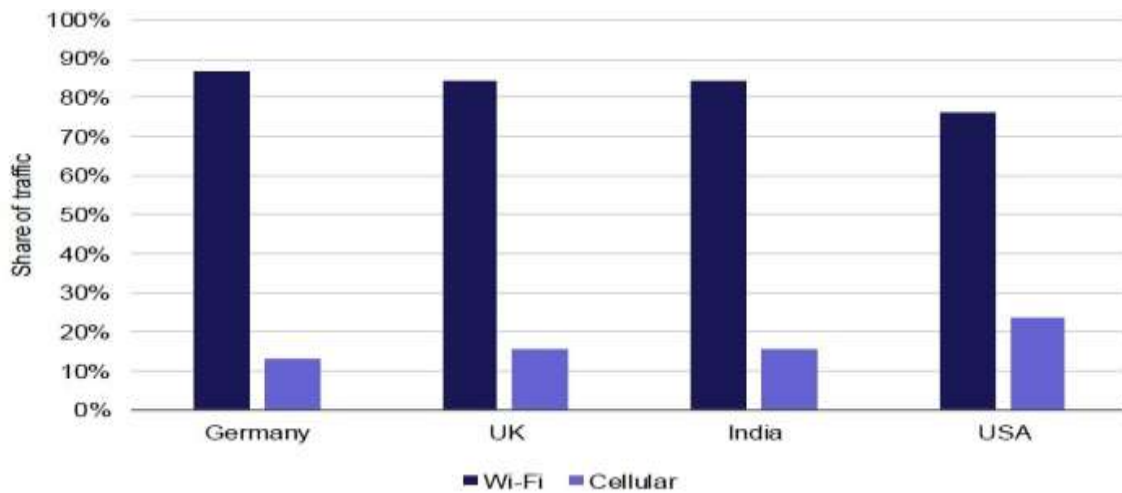
The Way Forward

- 4.0 Wi-Fi as a technology can play a pivotal role in connecting the unconnected. Globally, the pace of change is accelerating across the public Wi-Fi ecosystem. These are driven by several overall trends:
- (a) The increasing shift from best effort Wi-Fi to full carrier-grade Wi-Fi, enabling many new business models.
 - (b) The use of Wi-Fi as a strategic platform by an increasing variety of service providers including pure -plays, aggregators, Mobile network operators (MNOs), MSOs and vertical market operators.
 - (c) Wider applicability of Wi-Fi technologies as standards evolve and the needs of service providers change e.g. the move of Wi-Fi into the Internet of Things (IoT).
 - (d) The start of the process of defining 5G standards and the role of Wi-Fi and other unlicensed technologies in the next generation multi-technology wireless platform.
- 4.1 Wi-Fi has been deployed by venue and network owners across retail, hospitality, service, leisure, and transport sectors, as a means of improving the customer experience and increasingly, driving customer engagement and behavioural insights. Evidence from Analysys Mason’s Consumer Smartphone survey in Germany, India, the UK and the USA, which used a passive on device monitoring app, shows that in these markets Wi-Fi as a technology accounted for three quarters of smart phone traffic in 2016 as shown in

Figure 4.1³. During normal working hours, the cellular share of traffic did not rise above 20% in India.

Figure 4.1

Wi-Fi Share of Smartphone Traffic in Germany, the UK, India & the USA

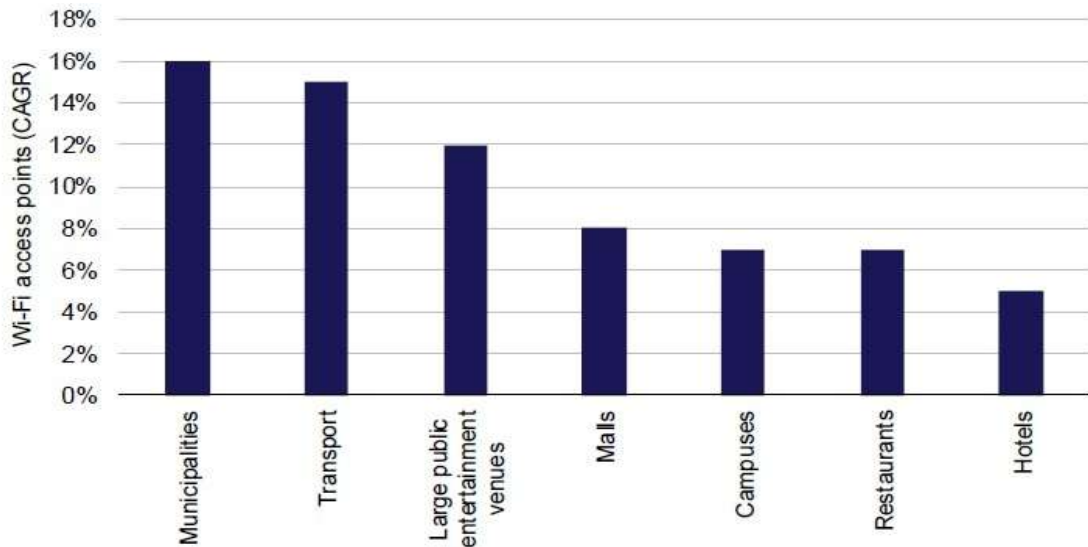


4.2 As per the same report, the importance of Wi-Fi for public venues is reflected in the global forecasts for growth in the number of hotspots across a variety of different venue types. As per the forecast, the number of hotspots deployed in malls will rise at a compound annual growth rate (CAGR) of 8% and at a CAGR of 7% for restaurants. There will also be strong growth in Municipality Wi-Fi networks for which the forecast is 16% CAGR as shown in Figure 4.2

³ White paper -Managed services provider Wi-Fi networks: significant opportunities for growth abound by Analysys Mason, November 2017.

Figure 4.2

Growth in Number of Wi-Fi Hotspots across different Venue Types



- 4.3 The Public Wi-Fi pilot outcome aims to offer a seamless experience to end users. To provide a simplified, consistent experience across hotspots from various providers means unbundling authentication, payment and accounting from hardware and software running on the Access Point. This will allow small entrepreneurs such as tea shops, grocery shops etc. to set up and maintain Access Points. Whereas, device manufacturers, payment companies, ISPs/Telcos and Consumer Internet companies can provide the remaining pieces to set up Public Data Offices (PDOs).
- 4.4 The unbundling is also important from the point of view of scale. PDOs will be akin to the PCOs that connected all of India, even at the time when tele-density was less than 7 telephones per 100 people. It is also suggested that the Public Wi-Fi Hotspots store community interest data locally, and allow access to it through negligible costs. Overall, the introduction of public Wi-Fi

network, should encourage the PDOs to become bustling centres of economic activity.

Actions Required

4.5 Accordingly, the pilot was envisaged to test the technology specifications designed and published by TRAI to prove interoperability between multiple systems. It would be pertinent to mention that the pilot initiative was ably supported by iSPIRT team. As can be observed from the outcomes, Phase I of the pilot has been highly successful in meeting the said objectives. The path from here onwards is envisaged as under:

- (a) DoT may consider approval of the TRAI recommendations on “Proliferation of Broadband through Public Wi-Fi Networks’ dated 09 March, 2017. This will also involve creation of a registration framework for PDO/PDOAs.
- (b) Moving ahead from the Pilot to the next phase which will involve working with the participants of the pilot in two large cities i.e. Delhi & Bengaluru to make all public Wi-Fi Hotspots WANI compliant including the airports, railway/metro stations, bus stands and other public places. This will allow testing WANI framework at scale. Existing hotspots from the pilot will continue to operate as it is.
- (c) An App testing and certification framework will have to be created. The framework will need to focus on testing KYC guidelines, interoperability and security of mobile apps. This will involve evaluation and appointing external agencies who can partner in the certification process. Initially, provisional certification could be undertaken by TRAI. Sample criteria for App and PDOA certification is at Annexure XV.
- (d) The Central Registry (CR) has presently been hosted on the TRAI website. A decision needs to be taken regarding its future management by DoT/TRAI or an entity approved by DoT/TRAI The CR contains

information about the PDOs/PDOAs, and User App providers in a digitally signed XML format.

4.6 It was mentioned in our Consultation Paper that '*The situation of Wi-Fi hotspots is not encouraging in India as we represent one sixth of the world population whereas our share in Wi-Fi hotspots is less than 1/1000*'. The success of the pilot addresses the issues of interoperability and payment options. The WANI architecture would, unleash the power of Wi-Fi and provide an impetus to the number of Public Wi-Fi hotspots in the country thereby providing the user a good quality of service and also a foolproof payment system.

Annexure I

TRAI Summary of Recommendations on Public Wi-Fi

1. The Department of Telecommunication (DoT) may amend the terms of the ISP license to allow for sharing of active infrastructure, in line with the Unified License (UL). Further, the Authority recommends that a clarification be provided in respect of all license categories, that sharing of infrastructure related to Wi-Fi equipment such as Wi-Fi router, Access point, and backhaul is also allowed
2. The DoT may re-visit the TRAI's earlier recommendations and consider de-licensing spectrum in the 5.725 - 5.825 GHz spectrum band for outdoor usage, and expedite decision on allocating E-band (71-76 GHz and 81-86 GHz) and V-band (57-64 GHz) to service providers.
3. Subject to the DoT's agreement with the Authority's interpretation, the DoT issue a clarification in respect of Clause (1)(xxii) of the UL VNO Guidelines, specifically clarifying that there is no exclusivity requirement upon UL VNO licensees for internet services i.e. a UL VNO can parent to multiple NSO for providing internet service.
4. Existing requirement of authentication through OTP for each instance of access may be done away with. Authentication through eKYC, eCAF and other electronic modes be allowed for the purposes of KYC obligations. In consultation with the security agencies, DoT may consider authentication by MAC ID of the device or through a mobile APP which stores eKYC data of the subscriber and automatically authenticate the subscriber.

5. The import duty applicable upon Wi-Fi access point equipment be revisited in coordination with the Ministry of Commerce. This will reduce cost of providing Wi-Fi service in the country leading to proliferation of broadband services.
6. A new framework should be put in place for setting up of Public Data Offices (PDOs). Under this framework, PDOs in agreement with Public Data Office Aggregators (PDOAs), should be allowed to provide public Wi-Fi services. This will not only increase number of public hotspots but also make internet service more affordable in the country.
7. PDOAs may be allowed to provide public Wi-Fi services without obtaining any specific license for the purpose. However, they would be subject to specific registration requirements (prescribed by the DoT) which will include obligations to ensure that e-KYC, authentication and record-keeping requirements (for customers, devices and PDOs enlisted with the PDOAs) are fulfilled by the PDOAs. This will encourage village level entrepreneurship and provide strong employment opportunities, especially in rural areas.
8. Authentication through eKYC, eCAF and other electronic modes be allowed for the purposes of KYC obligations cast upon PDOAs. This would enable PDOAs to obtain eKYC information and automatically authenticate the user device based on parameters such as the device's MAC ID or through a mobile APP, which will store data required for authentication of the subscriber. This will further improve user experience.
9. PDOAs be allowed to enter into agreements with third party application/ service providers for the purposes of managing authentication and payment processes. Appropriate guidelines may be issued to ensure that customer consent is obtained, and other issues surrounding privacy and protection of sensitive personal information are addressed. This will encourage innovation in authentication and payment processes resulting in ease in access of the Wi-Fi services.

Annexure II



Telecom Regulatory Authority of India



Public Open Wi-Fi Pilot

07th July, 2017

Mahanagar Door Sanchar Bhawan, Jawahar Lal Nehru Marg,
New Delhi – 110002

INTRODUCTION

1. The Internet is the single most self-empowering infrastructure available for a citizen in the 21st century. The World Bank observed that a 10% increase in Internet penetration leads to a 1.4% increase in GDP. Access to the Internet is considered a basic human right by many countries globally, including Estonia, Finland and France. In India, access to data is still limited due to poor coverage of fiber/telecom and prohibitive pricing of cellular data.
2. Wi-Fi is a complementary, not competing technology to LTE. Public hotspots hold an important place in the last-mile delivery of broadband to users. Wi-Fi is much easier to scale than adding new LTE towers. It bolsters connectivity inside buildings, airports, etc. where LTE penetration is inherently limited. It allows for offloading from telecom networks to ease congestion, and will be crucial when the next billion IoT devices come online. Yet, there are only 31,000 public Wi-Fi hotspots in India, compared to 13 million in France, and 10 million in the United States of America.
3. It is not enough to only install more routers. TRAI aims to offer a seamless experience to end users, both residents and international travelers. To provide a simplified, consistent experience across hotspots from various providers means unbundling authentication, payment and accounting from hardware and software running on the Access Point. This will allow small entrepreneurs such as tea shops, to set up and maintain Access Points. Whereas, device manufacturers, payment companies, ISPs/Telcos and Consumer Internet companies can provide the remaining pieces to set up Public Data Offices (PDOs).
4. The unbundling is also important from the point of view of scale. PDOs will be akin to the PCOs that connected all of India, even when tele-density was less than 7 telephones per 100 people. It is also suggested that the Public Wi-Fi Hotspots store community interest data locally, and allow access to it through negligible costs. Overall, these suggestions encourage the PDOs to become bustling centers of economic activity, where consumption of data for the average Indian becomes as common as consuming a cup of hot chai.
5. Based on the recommendation of TRAI “Proliferation of Broadband through Public Wi-Fi Networks” issued on 9th March 2017, TRAI invites all interested entities to be a part of this Pilot to establish nation-wide, pay-as-you-go PDOs.

CONSULTATIONS ON PUBLIC Wi-Fi

6. Recognizing the importance of public Wi-Fi networks in Indian context, TRAI initiated a consultation process on this subject in July, 2016. The motivation behind the consultation process was to identify issues in proliferation of public Wi-Fi in the country. As part of this process, TRAI released the "**Consultation on Proliferation of Broadband through Public Wi-Fi Networks**". The consultation paper (CP) highlighted issues like interoperability between the Wi-Fi networks of different service providers, de-licensing of additional bands for public Wi-Fi deployment and challenges in authentication and payments procedure of public Wi-Fi networks. On the issue of authentication and payments, the CP sought inputs on a hub-based model along the lines suggested by the Wireless Broadband Alliance (WBA), where a central third party AAA (Authentication, Authorization and Accounting) hub facilitates interconnection, authentication and settlement of payments between different network providers.
7. TRAI also conducted a stakeholder workshop on this issue on 28th September 2016, in collaboration with IIIT, Bengaluru. During the discussions, difficulties in authentication and payments were identified as some of the roadblocks in the uptake of public Wi-Fi services from the user's point of view. Following that, TRAI released another consultation note on this particular issue. Released in November 2016, the 'Consultation Note on Model for Nation-wide Interoperable and Scalable Public Wi-Fi Networks' proposed an authentication and payment architecture for public Wi-Fi networks and solicited the views of the stakeholders.
8. Subsequent to the processes mentioned above, TRAI issued a recommendation to the government entitled "**Proliferation of Broadband through Public Wi-Fi Networks**" on 09.03. 2017.

MISSION & OBJECTIVES OF PILOT

Mission for WANI

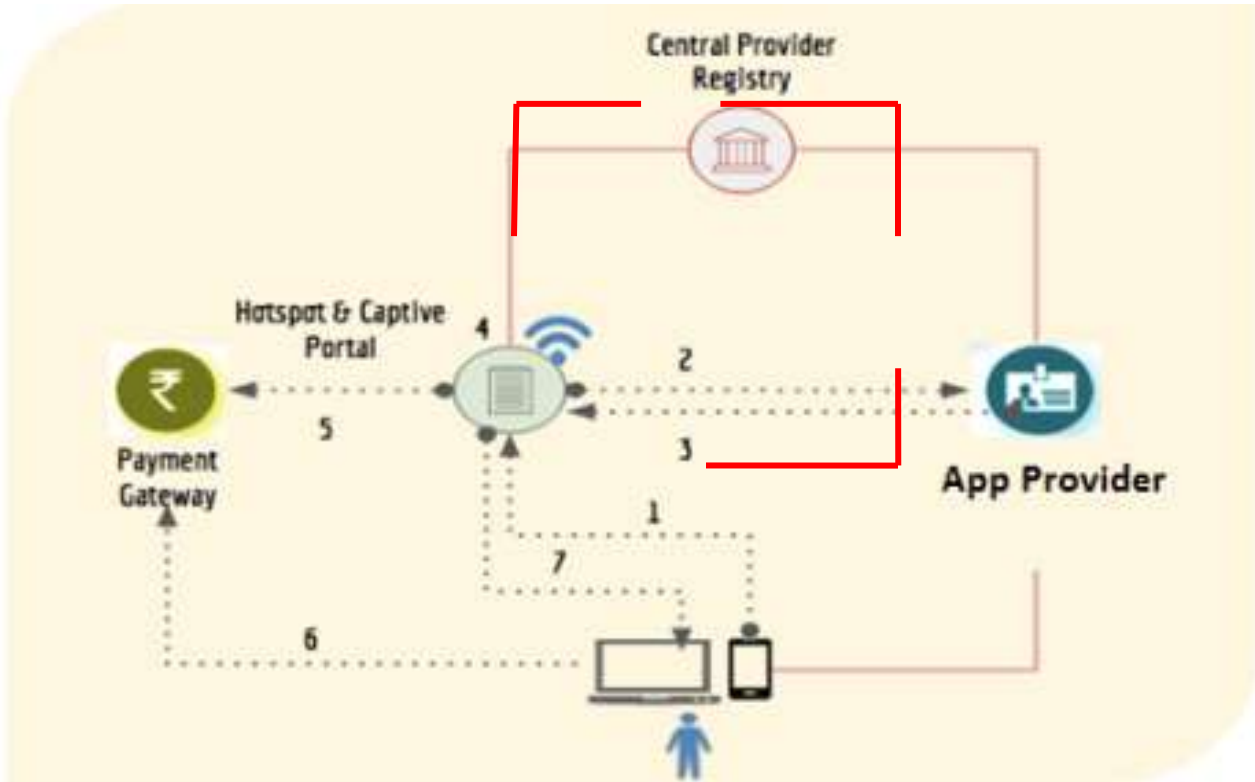
9. The vision of this initiative is to establish an Open Architecture based Wi-Fi Access Network Interface (WANI), such that;
 - (a) Any entity (company, proprietorship, societies, non-profits, etc.) should easily be able to setup a paid public Wi-Fi Access Point.

- (b) Users should be able to easily discover WANI compliant SSIDs, do one click authentication and payment, and connect one or more devices in single session.
 - (c) The experience for a small entrepreneur to purchase, self-register, set-up and operate a PDO must be simple, low-touch and maintenance-free.
 - (d) The products available for consumption should begin from “sachet-sized”, i.e. low denominations ranging from INR 2 to INR 20, etc.
 - (e) Providers (PDO provider, Access Point hardware/software, user authentication and KYC provider, and payment provider) are unbundled to eliminate silos and closed systems. This allows multiple parties in the ecosystem to come together and enable large scale adoption.
10. WANI Technology Architecture document which will provide the necessary technology and architecture for allowing multi-provider, interoperable system across the country will also be published within 3-4 days.

Objectives for the Pilot

11. For the pilot, TRAI has decided on a set of short-term objectives alongside the mission of WANI. Stakeholders are highly encouraged to join the pilot. Objectives of the pilot are:
- (a) Demonstrate that unbundling of services reduces rework, speeds up development and hence is the most effective way to tackle this complex problem.
 - (b) Prove that Multi-provider, inter-operable, collaborative model increases the overall innovation in the system, dismantles monopolies and encourages passing of benefits to end user.
 - (c) Test the specifications in real life conditions, and suggest improvements.
 - (d) Jointly develop a business model that fairly allocates value to each provider.
 - (e) Fine tune the technology and finalize the specifications based on pilot.
 - (f) Test out integrated payment methods such as coupons (purchased using cash by user or gifted to user), credit/debit cards, net banking, e-wallets, and UPI.

HIGH LEVEL FLOW



One Time Flows (Red)

1. PDO completes Self-Registration with Central Provider Registry their public certificate (for signature validation). They also registers SSIDs and locations of access points they operate.
2. App provider is registered with Central Provider registry along with their authentication URL and public certificate (to validate their digital signature)
3. User completes KYC with App Provider through mobile OTP through registration app. User registration app caches trusted SSIDs from central registry from time to time.

Connection and Usage Workflow (Dotted Lines)

1. User opens the registration app and discovers nearby WANI compliant SSIDs.
2. User chooses one SSID and connects using Registration App.
3. PDO requests user authentication from App provider using the token passed from the app during connection.
4. APP provider returns a signed user token to PDO.
5. Captive Portal displays data packs available. User selects desired data sachet.
6. Captive Portal sends request for through a payment gateway to user.
7. User completes payment.
8. PDO activates all device Mac-IDs that were part of the request and allows them to connect to the session.
9. Pack is activated and user can begin browsing.

For more details of the architecture and API details, refer to WANI Technology Architecture which will be published in 3-4 days.

PARTICIPATING IN PILOT

WHO SHOULD PARTICIPATE

1. **Public Data Office Provider/Aggregator (PDO/PDOA):** Any Indian entity (companies, associations, small merchants, etc.) having a PAN number wanting to provide one (PDO) or more (PDO Aggregator) hotspots to public using either free or paid model can be a hotspot provider.
2. **App Provider:** Any consumer internet App provider. Their application should provide features to manage user's KYC (mobile or Aadhaar) backed profile, allow all digital payment methods, and allow users to easily connect to hotspots.
3. **Hotspot Hardware/Software/Service Provider:** Any software or service provider who is providing necessary software, hardware, services, and/or support to Hotspot Providers. These can be any software/service provider, either local or global, making it easier for PDOs to get up & running.

HOW TO PARTICIPATE

12. Following are the requirements for providers wanting to participate in this pilot.

1. Must be an entity registered in India.
2. Must provide their PAN number and official contact details.
3. Must play the role of a PDO provider or Wi-Fi software/hardware provider or user registration provider. The provider may opt for multiple roles if desired.
4. To ensure full testing of interoperability, each pilot must have different entities playing different roles.
5. Must mandatorily comply with the specifications laid out in WANI Technology Architecture document as per their role.

How to Apply

13. Any interested entity (company, proprietorship, societies, non-profits, etc.) registered in India can apply to TRAI with the following details latest by 25th July 2017:

- (a) Name of the entity
- (b) Legal Status i.e. company, proprietorship, societies, non-profits, etc
- (c) Date of formation and Registration number
- (d) PAN Number
- (e) Official contact Details
- (f) Email address
- (g) *Role(s) in the Public Pilot Wi-Fi (PDO/PDOA, App Provider/Hardware provider/Software provider)*

Details can be submitted to TRAI on the following email:

arvind@traigov.in or alternatively: kapilhanda@traigov.in

In case of any clarification/information, Shri Arvind Kumar, Advisor (BB&PA) may be contacted at 011-23220209.

CONCLUSION

14. The events of the last 6 months in the telecom industry have dropped data prices, and we've seen user consumption go up proportionately. According to reports, Indians consumed more cellular data than China, and as much as the USA in the current cellular data pricing regime. The Indian Consumer is hungry for data, the question is who can provide her convenient and affordable access to the same.
15. TRAI believes that by adopting an Open Architecture approach, we place emphasis on innovation and consumer experience as the winning criteria and not deep pockets. The pilot is the first step in shaping this eco-system and ensuring the rules are established in a fair and transparent manner that encourages participation from all.
16. The Wi-Fi Access Network Interface (WANI) represents an exciting opportunity to do for data what PCOs did for Long Distance Calling. It will bring a new generation of users on to the internet in an assisted manner. It will also boost the consumption of data by the price-sensitive Indian customer who rations her cellular data usage. The opportunities created are immense, and we invite all eligible startups and incumbents to collaborate on this unique multi-provider model and be part of the conversation.



Telecom Regulatory Authority of India



Public Open Wi-Fi framework

Architecture & Specification (Version 0.5)

12th July, 2017

Mahanagar Door Sanchar Bhawan, Jawahar Lal Nehru Marg,
New Delhi – 110002

Table of Contents

- Introduction
- Project Mission.....
- Document Objectives
- Glossary of Terms.....
- Detail Specifications
- High Level Architecture
- Players in the ecosystem
- High Level Flows
- Specifications
- Provider Registry.....
- User Signup and Profile Management.....
- Access Point Discovery.....
- Connecting to Access Point and Usage
- Compliance Aspects
- Wi-Fi Provider.....
- App Provider
- CONCLUSION.....

Introduction

The Internet is the single most self-empowering infrastructure available for a citizen in the 21st century. The World Bank observed that a 10% increase in internet penetration leads to a 1.4% increase in GDP. Access to the Internet is considered a basic human right by many countries globally, including Estonia, Finland and France. In India, access to data is still limited due to poor coverage of fiber/telecom and prohibitive pricing of cellular data.

Wi-Fi is a complementary, not competing technology to LTE. Public hotspots hold an important place in the last-mile delivery of broadband to users. Wi-Fi is much easier to scale than adding new LTE towers. It bolsters connectivity inside buildings, airports, etc. where LTE penetration is inherently limited. It allows for offloading from telecom networks to ease congestion, and will be crucial when the next billion IoT devices come online. Yet, there are only 31,000 public Wi-Fi hotspots in India, compared to 13 million in France, and 10 million in the United States of America.

It is not enough to only install more routers. TRAI aims to offer a seamless experience to end users, both residents and international travelers. To provide a simplified, consistent experience across hotspots from various providers means unbundling authentication, payment and accounting from hardware and software running on the Access Point. This will allow small entrepreneurs such as tea shops, to set up and maintain Access Points. Whereas, device manufacturers, payment companies, ISPs/Telcos and Consumer Internet companies can provide the remaining pieces to set up Public Data Offices (PDOs).

The unbundling is also important from the point of view of scale. PDOs will be akin to the PCOs that connected all of India, even when tele-density was less than 7 telephones per 100 people. It is also suggested that the Public Wi-Fi Hotspots store community interest data locally, and allow access to it through negligible costs. Overall, the introduction of public Wi-Fi network, should encourage the PDOs to become bustling centers of economic activity.

TRAI has conducted multiple consultations regarding this which began in July 2016 and has released papers and notes regarding this. TRAI has also initiated a pilot in July 2017 to conduct field trials. All related documents are available on TRAI.

Project Mission

The vision of this initiative is to establish an Open Architecture based **Wi-Fi Access Network Interface** (WANI), such that;

1. Any entity (company, proprietorship, societies, non-profits, etc.) should easily be able to setup a paid public Wi-Fi Access Point.
2. Users should be able to easily discover WANI compliant SSIDs, do one click authentication and payment, and connect one or more devices in single session.
3. The Experience for a small entrepreneur to purchase, self-register, set-up and operate a PDO must be simple, low-touch and maintenance-free.
4. The products available for consumption should begin from “sachet-sized”, i.e. low denominations ranging from INR 2 to INR 20, etc.
5. Providers (PDO provider, Access Point hardware/software, user authentication and KYC provider, and payment provider) are unbundled to eliminate silos and closed systems. This allows multiple parties in the ecosystem to come together and enable large scale adoption.

Document Objectives

This document intends to provide detailed technology specifications for various providers to ensure full WANI system interoperability. All providers must ensure compliance with this specifications to be part of this initiative. This is a technical document and does not fully cover detailed policy aspects and enabling framework.

TRAI believes that through unbundling of services, multi-provider ecosystem, and easy regulatory process, millions of Wi-Fi access points can be enabled across the country that allows users to connect via single-click authentication and use it with ease.

NOTE: This is a draft specification which may undergo changes before becoming final specifications based on feedback from ecosystem during pilot.

Glossary of Terms

PDO	Public Data Office
PDOA	Public Data Office Aggregator
APP	Application – mobile app provisioned as frontend for users to access and connect to the available Wi-Fi hotspots
AP	Access points distributed across the city
IP	Internet protocol address assigned to all the elements in the
JSON	JavaScript Object Notation
URI/URL	Uniform Resource Identifier/Locator
CP	Wi-Fi Captive Portal
OTP	One Time Password
SSID	Service Set Identifier
MAC	Media Access Control – A globally unique ID/address given to physical network devices.
ACCE SS	Wireless hardware device that allows other devices to connect over - to a network/Internet.
HOTSPOT	A physical location where Wi-Fi Access Point is available for people to connect to Internet.

Detail Specifications

High Level Architecture

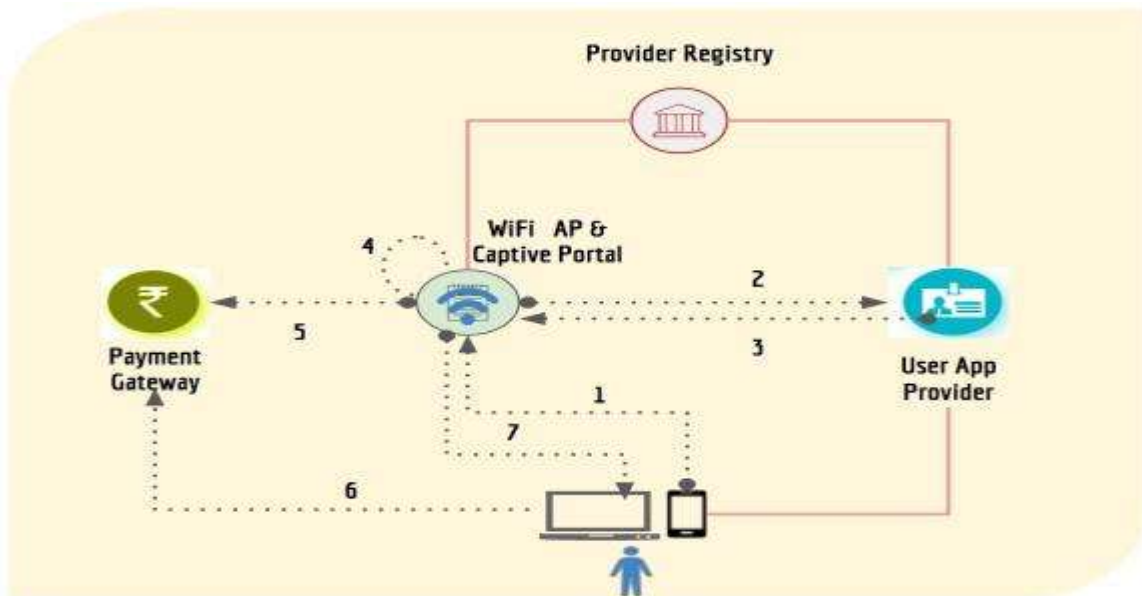
Players in the ecosystem

- **PDO/PDOA:** Any Indian entity (companies, associations, small merchants, etc.) having a PAN number wanting to provide one or more WANI compliant Wi-Fi hotspots to public using either free or paid model. They conform to the governing rules laid out by TRAI under this framework.
- **Hotspot Hardware/Software/Service Provider:** Any software or service provider who is providing necessary software, hardware, services, and/or support for PDOs to setup WANI compliant Wi-Fi hotspot. These can be any software/service provider, either Indian or global. It is expected that

these providers will offer a Wi-Fi-in-a-box solution for PDOs. Their software will need to be compliant to specifications laid out in this document. They will also integrate with a bank or a payment gateway for collecting payment from user.

- **User App Provider:** Any company providing a software application and backend authentication infrastructure for users to signup, discover WANI compliant Wi-Fi hotspots, and do single-click connect from within the app. This app allow users to create a profile, do their KYC (mobile verification), and allow setting up preferences for MAC-IDs for various accessing devices and payment methods. This app should allow users to discover WANI compliant hotspots and connect to it. In addition, App Provider must offer a backend user authentication service that is called by Wi-Fi Captive Portal software whenever user connects to obtain a signed user profile.
- **Central Registry of Providers (or simply Provider Registry):** A central registry managed by DoT/TRAI or an entity approved by DoT/TRAI containing information about the PDOs/PDOAs, and User App providers in a digitally signed XML format. This is a relatively static registry where approved providers are allowed to manage their profiles. Actual specification of the registry is provided later in this document.

High Level Flow



One Time Flow

One time flows are depicted in red lines in above diagram.

- PDO/PDOA completes Self-Registration with Provider Registry using their public certificate (for signature validation). They also register their Wi-Fi Access Points, SSIDs, and locations.
- User App provider is also registered with Provider Registry along with their authentication URL and public certificate (to validate their digital signature).
- User completes one time KYC with App Provider through their App. User App caches trusted SSIDs from Provider Registry from time to time.

Usage Flow

Usage flows are depicted in dotted lines in above diagram. Bullet number below corresponds to the number depicted within the diagram above.

1. User opens the App in which user has already registered and allows discovery and connection to WANI compliant Wi-Fi access points. Within the app, user browses for nearby WANI compliant SSIDs and then chooses one SSID to connect to
2. Wi-Fi Captive Portal of the PDO initiates user authentication with App provider backend using the token passed from the app.
3. App provider backend returns a signed user profile token back to Wi-Fi Captive Portal.
4. Wi-Fi Captive Portal displays data packs available with their charges. User selects desired data sachet, click to confirm the terms.
5. Wi-Fi Captive Portal sends request for payment through their payment gateway.
6. User completes payment.
7. PDO activates all device MAC-IDs that were part of the signed profile and allows them to connect to the session without additional authentication. Pack is activated and user can begin browsing.

Specifications

Following sections describe the technical specifications for Provider Registry, user signup, user authentication, and usage. Providers must ensure they comply with these specifications for ensuring interoperability across the country.

Provider Registry

Provider registry is maintained by DoT/TRAI for ensuring all authorized providers are identified, discovered, and trusted by the ecosystem. Providers will be given an account on the site where registry is maintained for managing their profile, public keys, and other details.

Currently the Provider Registry XML will be made available on the following URL:

https://tra.gov.in/wani/registry/wani_providers.xml

This registry XML will be updated whenever data changes in provider database. Applications reading this and caching the registry should respect the “ttl” (Time to Live) parameter and ensure it is refreshed to get latest data. It is also critical to ensure sub-registries linked via the main registries also need to be downloaded based on the need.

Schema (XSD will be made available separately) for wani_providers.xml is:

```
<WaniRegistry lastUpdated="" ttl="">
  <PDOAs>
    <PDOA id="" name="" phone="" email="" apUrl="" status="" rating="">
      <Keys>
        <Key exp="">base-64 encoded public key</Key>

        <Keys>
      </PDOA>
    </PDOAs>
  <AppProviders>
    <AppProvider id="" name="" phone="" email="" authUrl="" status="" rating="">
      <Keys>
        <Key exp="">base-64 encoded public key</Key>

      <Keys>
    </AppProvider>
  </AppProviders>
</WaniRegistry>
```

</AppProvider>

</AppProviders>

</Signature>

</WaniRegistry>

Element/Attribute	Description
WaniRegistry	Root element of the registry
WaniRegistry->lastUpdated	Timestamp in YYYYMMDDhhmmss format providing when the registry XML was last updated. Useful for cache refresh.
WaniRegistry->ttl	Time To Live in hours suggesting how long this data should be cached before checking for change. Default is "24".
WaniProvider->PDOAs	Parent element for listing of all PDOAs.
PDOAs->PDOA	Repeating element providing one entry per PDOA.
PDOA->id	Unique provider ID within the registry.
PDOA->name	Name of the provider entity.
PDOA->phone	Contact number of the provider entity.
PDOA->email	Email of the provider entity.
PDOA->apUrl	URL to the signed XML where all Wi-Fi Access Points of this providers along with MAC-IDs, and location is listed. This list is grouped by location to make it easier for applications to cache parts of this. At a later point, when the number of entries are in millions, this list itself may be further split with URLs pointing to sub-lists. Applications should start from this main registry and use the URLs within these XMLs to auto navigate
PDOA->status	Current status of the provider. Valid values are INPROCESS, TEMPORARY, ACTIVE, INACTIVE, SUSPENDED,
PDOA->rating	User rating of the provider. This is a decimal value between 0 and 5. This is meant for future use.
PDOA->Keys	Parent element where public keys are listed.

Element/Attribute	Description
Keys->Key	Individual public keys to validate the signature of the PDOA. When integrating via APIs across ecosystem partners, it is necessary to sign the API requests and responses to establish trust. This element will contain the base-64 encoded certificate in X509 V3 format. Currently SHA256withRSA

Key->exp	Expiry of the key in YYYYMMDD format. This is provided to support co- existence of multiple keys and is required for key
Waniprovider ->AppProviders	Parent element for listing of all user application providers.
AppProviders ->AppProvider	Element representing individual app provider.
AppProvider->id	Unique id of the app provider within the registry.
AppProvider->name	Name of the app provider.
AppProvider->phone	Contact number of the app provider.
AppProvider->email	Email of the app provider.
AppProvider->authUrl	Authentication URL (API endpoint) of the app provider against which Wi-Fi Captive Portal will call to authenticate and obtain the signed user profile. This must be an HTTPS URL into which authentication input data can be sent in the
AppProvider->status	Current status of the provider. Valid values are INPROCESS, TEMPORARY, ACTIVE, INACTIVE, SUSPENDED,
AppProvider->rating	User rating of the provider. This is a decimal value between 0 and 5. This is meant for future use.
AppProvider->Keys	Parent element where public keys are listed.
Keys->Key	Individual public keys to validate the signature of the AppProvider. When integrating via APIs across ecosystem partners, it is necessary to sign the API requests and responses to establish trust. This element will contain the base-64 encoded certificate in X509 V3 format. Currently
Key->exp	Expiry of the key in YYYYMMDD format. This is provided to support co- existence of multiple keys and is required for key

Wi-Fi Access Points (pointed by "apUrl" parameter of the PDOA) XML format:

```

<WaniAPList lastUpdated="" ttl="" providerId="">
  <!-- location element repeats -->
  <Location type="DISTRICT" name="" state="">
    <AP macid="" ssid="" status="" rating="" geoLoc="">
      <Tag name="OPENBETWEEN" value=""/>
      <Tag name="AVGSPEED" value=""/>

      <Tag name="FREEBAND" value=""/>
      <Tag name="PAYMENTMODES" value=""/>
    </AP>
  </Location>
</Signature>
</WaniAPList>

```

Element/Attribute	Description
WaniAPList	Root element of the registry where all WANI compliant Wi-Fi Access Points are listed for a provider.
WaniAPList->	Timestamp in YYYYMMDDhhmmss format providing when the registry XML was last updated. Useful for cache refresh.
WaniAPList->ttl	Time To Live in hours suggesting how long this data should be cached before checking for change. Default is "24".
WaniAPList->providerId	Id of the provider. This is same id as the WaniRegistry XML.
WaniAPList->Location	Repeating element organized by location of the Access Point.
Location->type	Type of location used for grouping. Currently it will be grouped by DISTRICT. In future further grouping may be
Location->name	Name of the location which is used for AP grouping. Currently this will be name of the district.
Location->state	Name of the State in which this Access Point is located.
Location->AP	Element depicting one Access Point. This element repeats.
AP->macid	MAC-ID of the Access Point.
AP->ssid	SSID of the Access Point.
AP->status	General status of the AP. Valid values are ACTIVE, INACTIVE.
AP->rating	User rating of the provider. This is a decimal value between 0
AP->Tag	<p>Various tags describing the AP features.</p> <ul style="list-style-type: none"> • OPENBETWEEN – value should be in the format hh-hh where hh represents time between 00 and 24. E.g., 09-17 (depicting 9 am to 5 pm) or 00-24 (depicting 24 hr availability). • AVGSPEED – Average speed in Mbps of the AP. It should be a positive integer. E.g., 2 meaning 2 Mbps. • FREEBAND – If this AP offers any free band in minutes. E.g., a value 10 depicts 10 free minutes. A Special value - 1 depicts ALWAYS free. • PAYMENTMODES – Allowed payment modes. Values can be CASH, COUPON, CREDITCARD, DEBITCARD,

User Signup and Profile Management

Users are expected to use some software application (mobile/desktop/etc.) provided by the "App Provider" for user signup, KYC, and profile management. User App should provide the following key features during user signup and profile management:

1. Users install an app from the App Provider.

2. App MUST capture user mobile number and does a mobile number verification (via OTP or GSM Mobile Connect or any other mechanisms).
3. App also allows creation of mandatory “username” which is unique within the App Provider system. This is shared with Wi-Fi provider during authentication and used for audit and traceability.
4. App should allow user to setup profile with additional **optional** attributes:
 - a. Email – user should be able to optionally setup email for getting alerts, etc.
 - b. Preferred payment address – This is ONLY for capturing UPI or Wallet address in the form **upi://vpa/token** (VPA is Virtual Payment Address for UPI collect transaction) or **wallet://acc-no@ppi/token**. App provider MUST NOT capture or store ANY sensitive information such as credit card number. All other types of payment will be directly handled by Wi-Fi Captive Portal.
 - c. If the User App is also a payment app (like UPI/Wallet app), then additional optional token string can be used to provide auto-deduct/offline/other additional payment functionalities.
5. App MUST also allow users to easily add/remove devices (MAC-ID and a name) which they want to connect to various Wi-Fi hotspots.
 - a. This allows the user to have more than one device to be connected to Wi-Fi hotspots within same session.
 - b. This is critical to allow IoT devices used by user to also connect using the common app and authentication. For example, by connecting the mobile phone to the Wi-Fi network, user may also connect his/her laptops or connected cars or other future devices.
 - c. Optionally app may also provide “device group” profiles to allow users to define named group of devices so that they can choose one group vs another during connecting.

Access Point Discovery

1. User App should allow users to discover nearby WANI compliant Access Points by detecting nearby SSIDs and verifying the MAC-IDs against the SSID Registry.
2. In addition, optionally user App can provide location specific searches and allow users to discover “nearby” Wi-Fi hotspots without being the Wi-Fi range. SSID registry can be cached locally by app smartly for doing location level searches.
3. App should also optionally allow users to save “favorites”, “most recent”, etc. for easy selection of regular connections.
4. In addition, ideally App may also provide easy sorting and selection of access points based on the “Tag” attributes such as when AP is available, average speed, rating, etc. This allows users to select best AP within available selections.
5. App must provide a mechanism for users to rate the access points and providers.

Connecting to Access Point and Usage

1. Whenever users want to connect to public Wi-Fi hotspot using this scheme, they can open their App, browse WANI compliant Wi-Fi hotspots (see section on discovery above), and click connect.
2. App creates a token **waniapptoken** which needs to be passed to Wi-Fi Captive Portal. This token is created as below:

```
waniapptoken = <app-provider-id>|<enc-token>
```

enc-token MUST NOT be a fixed value to ensure it is not can be reused beyond a session. It MUST be encrypted using App provider public key so that only App provider backend can decrypt tis token. It is created as below:

```
enc-token = base-64(RSA-Encrypt(token))
```

```
token = {
```

```
    "ver": "1.0", // version of the token structure
```

```
    "timestamp": "YYYYMMDDhhmmss",
```

```
    "username": "", // username of user
```

```

"appId": "", // App id to handle multiple apps from same provider
"appVer": "", // version of app to handle multiple app versions
"totp": "", // TOTP generated by the app. This is essential to
                ensure App provider server can trust origin of this token
"custData": {} // any custom JSON data structure needed by the app
}

```

3. App base-64 encodes the token and passes it on to captive portal using parameter name waniapptoken (can be passed as part of GET parameter). E.g.,

```

http://portal.com/?waniapptoken=
FG23A|ZDM3MzQxM2RIYjc0NGIyNGM2MjI2MTM2MTY0MGVmN2Q3MGI4YjcxZjlm
MTMyOTQ4NzdmNmY5O
WViZjFINTk3Yg==

```

4. Wi-Fi provider's Captive Portal should look for waniapptoken parameter and process it as below:

- a. Extract the App Provider ID from the token prefix (string until the "|" delimiter within the token).
- b. Verify the App Provider ID against the locally cached WANI Registry (WaniRegistry->Appproviders->Appprovider[id={id}]) and obtain authDomain for that App provider.

- c. Encrypts the waniapptoken using PDOA private key as below to create a new token **wanipdoatoken**

```

wanipdoatoken = <PDOA-Id>|<key-Exp>|<base-64(RSA-
Encrypt(waniapptoken))>

```

- d. Calls the authDomain by passing the signed token wanipdoatoken as part of the URL parameter. This MUST BE an https call.

```

https://auth.app-provider.com/?wanipdoatoken=
12GF34|MjAxODA4MTV8NTIyOTM5NTdBRTI4N0Q3RDdBOTFEMEUI
OEU2RTQ3OUU4NDZkIyMDQwM0U5N0ZGQzQ1RTE1RDRBMjcwMw==

```

5. App Provider backend server should do the following on their server:

- a. Extract the PDOA-Id from the parameter (token prefix).
- b. Verify the PDOA ID against the locally cached WANI Registry (WaniRegistry->PDOAs->PDOA[id={id}]).

- c. Once verified, take the public key of the PDOA corresponding to the key-exp parameter from WANI registry (WaniRegistry->PDOAs->PDOA[id={id}]->Keys->Key[exp={key-exp}])-
 - d. Decrypt using the waniapptoken from the wanipdoatoken using the public key of the PDOA.
 - e. Decrypt waniapptoken using their own private key and verify the token structure, TOTP, etc.
6. After validation of the waniapptoken, App Provider should return the following structure back to Wi-Fi Captive Portal:

```
{
  "ver": "1.0", // version of the profile format

  "app-provider-id": "", // mandatory - ID from WaniRegistry
  "app-provider-name": "", // name from WaniRegistry
  "timestamp": "YYYYMMDDhhmmss", // current timestamp
  "Username": "", // mandatory

  "payment-address": "", // upi://vpa/token or wallet://ac-no@ppi/token
  "Devices": [], // device MAC-IDs array if any for current session  "signature": "",
  // computed for this structure (see below)

  "key-exp": "" // Key->exp value of the key pair used for signature
}
```

Signature is computed as below:

signature = base-64(RSA-Encrypt(hash))

hash = SHA-256(timestamp+username+payment-address+devices[0]+...+devices[i])

7. Once Wi-Fi hotspot provider obtains response, it needs to do the following verification:
 - a. Decrypting the hash from signature using the public key of the App provider (that corresponds to Key->exp value from registry).
 - b. Calculate the hash and verify if the hash is matching.
 - c. If matching, proceed with next steps. If not, show error and allow user to disconnect and connect again (try again).
8. After verification, Captive Portal should show the user available packages. Once the user chooses a package, user should be directed to make payment on the portal.
9. If user profile had preferred payment address, then it should be

defaulted and allow user to do payment without any data entry on the portal.

10. Wi-Fi provider will have to allow user to make payment during which time user must be given temporary Internet access to payment provider's server.
11. Once payment is confirmed, Wi-Fi Access Point should now allow all devices (MAC-IDs within user profile) to be connected to same session and share the package. This is critical for single-click access to Internet for multiple devices that users typically carry around these days without each devices having to go through same process. This is a MANDATORY compliance requirements for WANI PDO/PDOAs.
12. When the session is about to expire, hotspot provider can prompt the user and requests extension of the session and charge additional amount ONLY WITH explicit user consent without user having to go through all steps again.
 - a. Note that users who connect to their favorite Wi-Fi hotspots can “pre-authorize” payment through Wallet or UPI e-mandate (part of UPI 2.0) which makes even payment a single click seamless experience. This also allows Wi-Fi providers to easily extend user sessions with single user click “extend my session (charge Rs.xx)” without any further steps to make payment.

IMPORTANT NOTE: With single click user authentication through authorized Apps and payment pre-authorization via e-mandates, connecting and using public Wi-Fi will be a seamless, friction free experience for users.

Compliance Aspects

Wi-Fi Provider

1. Captive portal must allow standard connection and authentication as per this specification.
2. Wi-Fi Provider must provide choice to user to select a package with clear details of the package.
3. Captive portal should respect and handle preferred payment scheme for users and allow seamless collection of payment once the package

is selected.

4. Wi-Fi provider must comply and be certified with regulatory and security rules for payment transactions, auditing, and storage/handling of any sensitive payment information.

App Provider

1. App provider must provide an App to user (for any device/OS based on market needs) and comply with user sign up, profile management, and authentication specifications as per this document.
2. App provider must ensure user data is strongly protected to ensure user privacy and data security is ensured.
3. App provider must have a mechanism to allow regular app update and improvements.
4. App is encouraged to provide good user interface for consumers to easily discover, search, find best access points, and connect to it with single-click.

CONCLUSION

Telecom industry is seeing rapid transformation through drop in data prices, increased speed, and increased consumption of data packs. India is also creating a slew of digital platforms to help its citizens with better access to various services. According to reports, Indians consumed more cellular data than China, and as much as the USA in the current cellular data pricing regime. TRAI believes that by adopting an Open Architecture approach, emphasis on innovation and consumer experience is placed as the winning criteria.

This document provide technical architecture specifications for an interoperable ecosystem. The Wi-Fi Access Network Interface (WANI) represents an exciting opportunity to do for data what PCOs did for Long Distance Calling. It will bring a new generation of users and entrepreneurs into the market to bridge the need of last mile connectivity. The opportunities created are immense and will benefit 100's of millions of users in India waiting to get affordable access to Internet.

----- END -----

Workshop Agenda

**Workshop on
Public Open Wi-Fi Pilot
25 July 2017 (Tuesday)**

Venue: **Hotel Radisson Blue Atria, Bengaluru**

Register at: <https://goo.gl/forms/Q7Uxg9LujsUbjJ9D2>

Timings: Registration -2:00-2:30 pm

Conduct of Workshop- 2:30-5:00 pm

Telecom Regulatory Authority of India (TRAI) released a consultation paper on “**Proliferation of Broadband through Public Wi-Fi Networks**” on 13th July 2016 realizing the importance of public Wi-Fi networks as complementary to existing landline and cellular mobile infrastructure in improving broadband penetration and adoption in the country. A few of the important issues pointed out in the consultation paper for a successful, scalable and sustainable public Wi-Fi infrastructure in the country include

- I. Technical interoperability and seamless connectivity of Wi-Fi networks
- II. Innovative payment, commercialization, and monetization models;
- III. Collaborative partnerships between various entities of the ecosystem.

After considering the comments from the stakeholders and further analysis, the Authority came out with its Recommendations on “Proliferation of Broadband through Public Wi-Fi Networks” on 09th March, 2017. Some of the recommendations were:

1. A new framework should be put in place for setting up of Public Data Offices (PDOs). Under this framework, PDOs in agreement with Public

Data Office Aggregators (PDOAs), should be allowed to provide public Wi-Fi services. This will not only increase number of public hotspots but also make internet service more affordable in the country.

2. PDOAs may be allowed to provide public Wi-Fi services without obtaining any specific license for the purpose. However, they would be subject to specific registration requirements (prescribed by the DoT) which will include obligations to ensure that e-KYC, authentication and record-keeping requirements (for customers, devices and PDOs enlisted with the PDOAs) are fulfilled by the PDOAs. This will encourage village level entrepreneurship and provide strong employment opportunities, especially in rural areas.

Based on the recommendations, the Authority released a document on 07th July, 2017 inviting all interested parties to be part of Pilot Wi-Fi project. The framework architecture and specifications for the pilot were subsequently released on 12 July, 2017.

The Workshop is targeted at Public Data Office Providers/Aggregators (PDO/PDOA), App providers and Hotspot Hardware/Software/Service Providers.

The idea is to get valuable feedback and comments from the above stakeholders that can be input to TRAI on this very important theme.

Accordingly, all the prospective stakeholders are invited to attend the Workshop.

Time	Sessions
14:00-14:30	Registration & Networking
14:30-15:00	<p>Opening Session</p> <p>Welcome Address: Shri U.K. Srivastava, Pr. Advisor, TRAI</p> <p>Inaugural Speech: Shri. R.S. Sharma, Chairman, TRAI</p> <p>Overview of the Public Open Wi-Fi Pilot: Shri. Arvind Kumar, Advisor, TRAI</p>
15:00-15:45	<p>Presentation on Public Open Wi-Fi Framework:</p> <p>Dr Pramod Varma,</p> <p>Chief Architect- Aadhaar, Architect-India Stack</p>
15:45- 16:30	Question and Answer Session
16:30-16:45	<p>Concluding remarks: Shri. R.S. Sharma, Chairman, TRAI</p> <p>Vote of Thanks: Shri. U. K. Srivastava, Principal Advisor, TRAI</p>
16:45-17:00	High Tea



भारतीय दूरसंचार विनियामक प्राधिकरण
TELECOM REGULATORY AUTHORITY OF INDIA
भारत सरकार / Government of India



महानगर दूरसंचार भवन, जवाहर लाल नेहरू मार्ग,
Mahanagar Doorsanchar Bhawan, Jawahar Lal Nehru Marg
(पुराना मिनटो रोड) नई दिल्ली / (Old Minto Road), New Delhi-110002
फैक्स / Fax : +91-11-23213294, ईपीबीएक्स नं० / EPBX No. : +91-11-23664145

F. No. 4-5/2016-BB&PA

Dated : 9th March, 2017

To
Secretary,
Department of Telecommunications,
Sanchar Bhawan, 20, Ashoka Road,
New Delhi-110001

Sub.: Recommendations dated 09.03.2017 on "Proliferation of Broadband through public Wi-Fi Networks"

The Authority issued a Consultation Paper on "Proliferation of Broadband through public Wi-Fi Networks" on 13th July 2016 to examine the need of encouraging deployment of public Wi-Fi networks in the country from a public policy point of view. The paper also discussed various issues in Public Wi-Fi proliferation to find out solutions for the same. The comments and counter-comments received from the stakeholders were placed on the TRAI's website.

2. To augment the consultation process, a Workshop was held on 28th September, 2016 at Bengaluru in academic collaboration with International Institute of Information Technology, Bangalore (IIIT-Bangalore). Based on the discussions held at the workshop, in relation to exploring viable models for deploying interoperable and scalable public Wi-Fi networks, the Authority released a Consultation Note on "Model for Nation-wide Interoperable and Scalable Public Wi-Fi Networks" on 15th November 2016 inviting written comments on the issues from the stakeholders. Further, an Open House Discussion (OHD) with stakeholders was organized on 9th January, 2017.

3. After analyzing the various issues involved and considering the comments received from stakeholders in their written response and during the OHD, the Authority has finalized its Recommendations titled "Proliferation of Broadband through public Wi-Fi Networks". The Authority recommendations are enclosed herewith.

4. In keeping with practice, a copy of this letter, along with the recommendations, is being placed on the website of TRAI (www.trai.gov.in).

This letter issues with the approval of the Authority.

Encl: as above


(Sudhir Gupta)
Secretary TRAI

Annexure VI

**Government of India
Ministry of Communications
Department of Telecommunications
(Data Services Cell)**

File No: 16/13/2017-DS-III

Dated: 18.09.2017

To


The Secretary,
Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan,
Jawahar Lal Nehru Marg,
Old Minto Road, New Delhi – 110001

Subject: Pilot on Public Open Wi-Fi.

Reference: TRAI letter No. 4-5/2016-BB&PA dated 11.08.2017.

I have been directed to state that TRAI may carry out the trial. However, the following safeguards may be observed:

- (i) The pilot should be purely for experimental purpose.
- (ii) No third party/ long term interests should be created. It is to be kept in view that as per present licensing regime, only a company registered under Companies Act having appropriate license under section 4 of Indian Telegraph Act 1885 can provide telecom services.
- (iii) It is presumed that this pilot is being carried out for providing only internet services only and public voice telephony is not in the scope of this pilot.
- (iv) The resources, connectivity etc. should be only for the duration of the pilot and it should be stopped/wind up immediately thereafter.
- (v) Department of Telecommunications should be fully indemnified for all claims, cost, charges or damages etc., if any, arising in this respect.


(P.C.Sharma)
Director(DS-III)

Copy for kind information to:

- (1) Sr. DDG(AS)
- (2) Sr. DDG(TERM), HQ.

Annexure VII

Telecom Regulatory Authority of India



Public Wi-Fi Pilot Project Plan



15.09.2017

Mahanagar Door Sanchar Bhawan, Jawahar Lal Nehru Marg,
New Delhi – 110002

Document Structure:

- a. [Introduction to the Pilot](#)
- b. [Goals of the Pilot](#)
- c. [Timeline](#)
- d. [Procedural Guidelines](#)
- e. [Example flow Diagram](#)
- f. [Operating Guidelines](#)
- g. [Certification Framework](#)
- h. [Audit Framework](#)
- i. [Conclusion](#)

Introduction to the Pilot

1. The Internet is the single most self-empowering infrastructure available for a citizen in the 21st century. The World Bank observed that a 10% increase in Internet penetration leads to a 1.4% increase in GDP. Access to the Internet is considered a basic human right by many countries globally, including Estonia, Finland and France. In India, access to data is still limited due to poor coverage of fiber/telecom and prohibitive pricing of cellular data.
2. Wi-Fi is a complementary, not competing technology to LTE. Public hotspots hold an important place in the last-mile delivery of broadband to users. Wi-Fi is much easier to scale than adding new LTE towers. It bolsters connectivity inside buildings, airports, etc. where LTE penetration is inherently limited. It allows for offloading from telecom networks to ease congestion, and will be crucial when the next billion IoT devices come online. Yet, there are only 31,000 public Wi-Fi hotspots in India, compared to 13 million in France, and 10 million in the United States of America.
3. It is not enough to only install more routers. TRAI aims to offer a seamless experience to end users, both residents and international travelers. To provide a simplified, consistent experience across hotspots from various providers means unbundling authentication, payment and accounting from hardware and software running on the Access Point. This will allow small entrepreneurs such as tea shops, to set up and maintain Access Points. Whereas, device manufacturers, payment companies, ISPs/Telcos and Consumer Internet companies can provide the remaining pieces to set up Public Data Offices (PDOs).
4. The unbundling is also important from the point of view of scale. PDOs will be akin to the PCOs that connected all of India, even when tele-density was less than 7 telephones per 100 people. It is also suggested that the Public Wi-Fi Hotspots store community interest data locally, and allow access to it through negligible costs. Overall, these suggestions encourage the PDOs to become bustling centers of economic activity, where consumption of data for the average Indian becomes as common as consuming a cup of hot chai.
5. Based on the recommendation of TRAI “Proliferation of Broadband through Public Wi-Fi Networks” issued on 9th March 2017, TRAI invites all interested entities to be a part of this Pilot to establish nation-wide, pay-as-you-go PDOs.

Objectives of the Pilot

For the pilot, TRAI has decided on a set of short-term objectives alongside the mission of WANI. Stakeholders are highly encouraged to join the pilot. Objectives of the pilot are:

1. Demonstrate that unbundling of services reduces rework, speeds up development and hence is the most effective way to tackle this complex problem.
2. Prove that Multi-provider, interoperable, collaborative model increases the overall innovation in the system, dismantles monopolies and encourages passing of benefits to end user.
3. Test the specifications in real life conditions, and suggest improvements.
4. Jointly develop a business model that fairly allocates value to each provider.
5. Fine tune the technology and finalize the specifications based on pilot.
6. Test out integrated payment methods such as coupons (purchased using cash by user or gifted to user), credit/debit cards, net banking, e-wallets, and UPI.

Goals of the Pilot *

Geographies	Bengaluru, Delhi (Not restrictive)
No of PDOs	In excess of 500
No of Consumer Apps	Minimum 5
No of Consumers KYC enabled for WANI	Minimum 5,000
No of sessions/consumer	Minimum 2
Total no of sessions	1,00,000

*** The Figures are tentative . We shall confirm up after the pilot goes live**

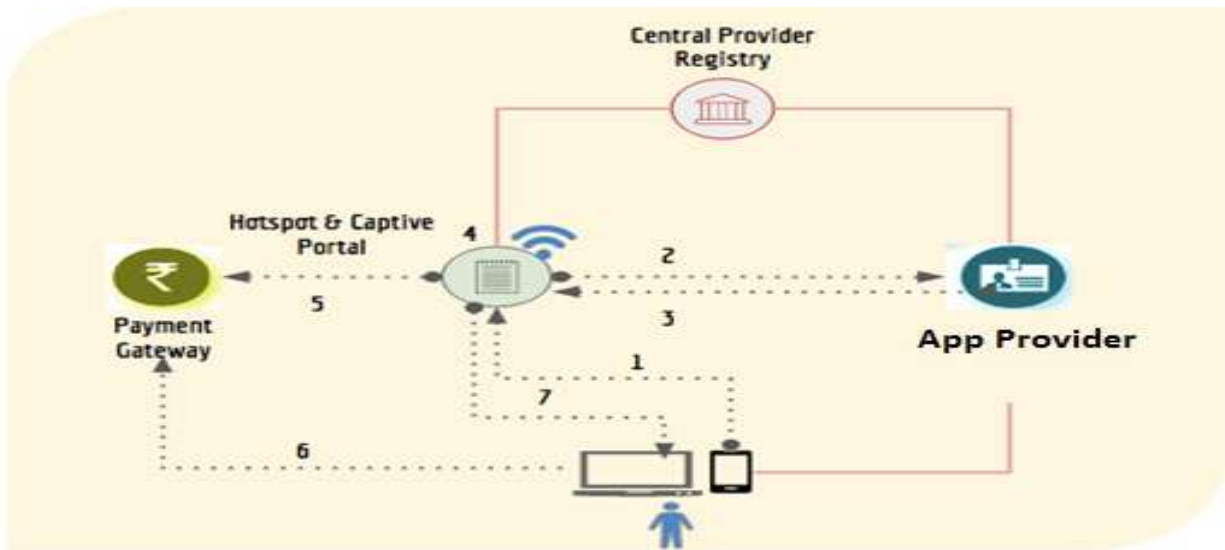
Timeline

Publish procedural guidelines	15 Sep 2017
Host Central Registry	20 Sep 2017
PDOA & Consumer App Registration	1 Oct 2017
Pilot Go Live Date	15 Oct 2017
Pilot End Date	30 Nov 2017
TRAI Report on the Pilot	15 Dec 2017

Procedural Guidelines

1. It is expected that Software/Hardware/ISP providers will work directly with PDOAs for the pilot;
2. TRAI will work directly with Consumer App Providers or PDOAs directly for the pilot
3. PDO/PDOA completes Self-Registration with Provider Registry using their public certificate (for signature validation). They also register their Wi-Fi Access Points, SSIDs, and locations.
4. User App provider is also registered with Provider Registry along with their authentication URL and public certificate (to validate their digital signature).
5. User completes one time KYC with App Provider through their App. User App caches trusted SSIDs from Provider Registry from time to time

Example Flow Diagram



Operating Guidelines

1. SPEED: Each PDO/PDOA has to offer a minimum speed of 2Mbps to every customer
2. SECURITY: From Access Point(AP) to the registry server IPSEC/GRE tunnel needs to be implemented
3. KYC: eKYC-wherein it should be linked to Aadhar card.
4. DATA STORAGE: It should be capable of withstanding any cyber attack including malware and Denial of Service(DoS).

Operating Practice Template

Template for PDOA/Consumer App Practice Statement that needs to be provided by each participant

Contents

1. PDOA System Description

a. Introduction

Overview of the solution

i. Contact Details

b. Detailed System Architecture Diagram

- c. Hardware details
- d. Sample User Flow
- e. Directory of PDOs
- f. PDO Sign Up (Provide the flow for PDO sign up, including the how PDO's identification is strongly authenticated, how user's demographic details are validated prior to opening of account)
- g. Data plans & Pricing
 - i. Cost of Data plans for consumer apps
 - ii. Payment Settlement Details
- h. PDO Contract Details
 - i. Terms & Conditions
 - ii. Dispute Resolution procedures
 - iii. Grievance Redressal Mechanism
- i. Detailed Marketing & Branding Plan
- j. Goals & Milestones for the pilot

2. Consumer System Description

- a. Introduction
 - i. Overview of the solution
 - ii. Contact Details
- b. Detailed system architecture diagram
- c. User functions (Provide flows for Sign up, KYC, Sign In, forgot password, reset password, view profile, update profile, access to available hotspots and any other functions to be provided to the user).
- d. Integration with PDOAs (Provide overview/procedure to integrate with PDOAs)
- e. Pricing
 - i. Data plans/offers planned for the consumer
 - ii. Modes of payment enabled for consumer
 - iii. PDOA Payment settlement process
 - iv. Refund Policy
- f. Consumer Contract Details
 - i. Terms & Conditions
 - ii. Dispute Resolution procedures
 - iii. Grievance Redressal Mechanism
- g. Detailed Marketing & Branding Plan

- h. Goals & Milestones for the pilot

Reporting Practice Template

1. PDOAs

- a. No of PDOs (15 days Active or Inactive)
- b. No of successful connections
- c. Avg Amount of Data/Active Session
- d. Day wise Data Consumption
- e. Total amount of Data till Date
- f. Total Revenue Earned
- g. Consumer app wise consumption data

2. Consumer Apps

- a. Total no of customers KYC
- b. Total no of customers connected at least once
- c. Avg no of sessions/customer
- d. Avg data/customer
- e. Total data consumed
- f. Day wise data consumption
- g. Total Revenue Earned
- h. PDO wise connection data

Certification Framework

The app needs to be hosted on Google Playstore and the link for downloading is shared with Wi-Fi Pilot Google Group.

Audit Framework

The Audit Framework would consist of following checkpoints:

- End- to- end authentication
- Encryption
- Interoperability between two different operators
- Seamless working of payment mechanism
- Setting up of a PDO, how much time it takes to activate and how all registrations are getting stored in PDOA, its data integrity and how information is shared with other PDOAs.

Conclusion

One of the most interesting aspects of the significant changes ongoing in the public Wi-Fi ecosystem is the increase of hotspots owned or managed by venues and other brands. According to recent research conducted for iPass by Maravedis-Rethink, 50% of all commercial hotspots are controlled by brands whose core business is not telecommunications. This is because actual sign-on and allocation of passwords is often ultimately controlled by a hotel chain, group of coffee stores or a municipal authority. The country is still in a green field deployment phase in terms of adoption of public Wi-Fi services. There is thus a need to resolve the challenges and risks being faced in the process and lay a strong foundation for the development of new and innovative models that support the expansion of Wi-Fi enabled Broadband connectivity. In order to provide a thrust to proliferation of Wi-Fi hotspots in the country the pilot project has been planned as a proof of concept for interoperability.

Annexure VIII

List of Registered Entities

S.No	Entity Name	Role
1	Innovative Traders	PDOA
2	Technocrat Industries	Technology provider
3	Kumar Rohit Consultancy	PDOA/Technology provider
4	Rishira Infolabs Private Limited	PDOA/Technology provider
5	Manendra Kumar Paswan	PDOA
6	Fizzy Software Pvt. Limited	Technology provider
7	FiberNet Cable & Datacom (P) Limited	PDOA
9	Nisquare Technologies Opc Private Limited	Technology provider
10	Mohd Firoz Alam	PDOA
11	FreeG WiFi Technologies Private Limited	PDOA/Technology provider
12	Mojo Networks	Hardware provider
13	Chinar Electrical	PDOA/PDOA
14	ONE97 Communications Limited	PDOA/Technology provider
15	Kenstel Networks Limited	Technology provider
16	Omnia Information Private Limited	Technology provider
17	Netvision Awadh Networks Private Limited	PDOA/Technology provider
18	Alacrity Services Private Limited	PDOA/Technology provider
19	XiFi Smart Networks Private Limited	PDOA/Technology provider
20	SABO Online Services	PDOA/Technology provider
21	Cotyledon	PDOA
22	Giant Tech Labs Private Limited	PDOA/Technology provider
23	Bluetown	PDOA/Technology provider
24	COSGrid Systems Private Limited	PDOA/Technology provider
25	OptiTrans Solutions Private Limited	Technology provider
26	S M Associates	PDOA/Technology provider
27	Inventum Technologies Private Limited	PDOA/Technology provider
28	Dexworks Labs Private Limited	PDOA/Technology provider
29	WiMark Systems	PDOA/Technology provider
30	MPG Digital	PDOA/Technology provider
31	10I Commerce Services Private Limited	PDOA/Technology provider

32	Aura Ventures Private Limited	PDOA/Technology provider
33	Sheng Li Telecom India Private Limited	PDOA/Technology provider
34	Nanovie Technologies LLP	PDOA/Technology provider
35	Janya Info Solutions India Private Limited	PDOA/Technology provider
36	Pronto Networks Inc	PDOA/Technology provider
37	Sanil Enterprises	PDOA
38	Citycom Networks Private Limited	PDOA/Technology provider
39	Airmesh Communications Limited	PDOA/Technology provider
40	Tranfode Technologies	PDOA/Technology provider
41	Tejas Networks Limited	PDOA/Technology provider
42	Mi-Fi networks Private Limited	PDOA/Technology provider
43	Seven Hills Opticommunication Private Limited	Technology provider
44	RCV Innovations Private Limited	PDOA/Technology provider
45	Satpar Infotech Private Limited	PDOA/Technology provider
46	T.N. Consumer Federation	PDOA/Technology provider
47	Trimax It Infrastructure Services	Technology provider
48	WiFi Dabba India Private Limited	PDOA/Technology provider
49	Maestros Technical Services Private Limited	PDOA/Technology provider
50	Machraa skills	PDOA/Technology provider
51	Onehop networks	PDOA/Technology provider
52	CDoT	PDOA/Technology provider
53	CJ Online Private Limited	PDOA/Technology provider
54	delDSL Internet Private Limited	PDOA/Technology provider
55	QuadGen Wireless Solutions Private Limited	PDOA/Technology provider
56	SIFY Technologies Limited	PDOA/Technology provider
57	Telexcell Information Systems Limited	PDOA/Technology provider
58	S. Shivasankar,	PDOA/Technology provider
59	IBUS Network & Infrastructure Private Ltd	PDOA/Technology provider
60	Netaccess Communications Limited	PDOA/Technology provider
61	Indus Towers Limited	PDOA/Technology provider
62	Virtual Netax Private Limited	PDOA/Technology provider
63	Vistara Network Private Limited	PDOA/Technology provider
64	Febler Technologies Private. Limited	PDOA/Technology provider
65	Janastu	Technology provider
66	Servelots Infotech Private Limited.	PDOA/Technology provider
67	Siddharth Desai	Technology provider

68	Verticle Technologies Private Limited.	PDOA/Technology provider
69	Nextrack Technologies Private Limited.	PDOA/Technology provider
70	D-VoiS Communications Private Limited	PDOA/Technology provider
71	Eko India Financial Services Private Limited	PDOA/Technology provider
72	CSC e-Governance Services India Ltd.	PDOA/Technology provider
73	Rural Broadband Private Limited	PDOA/Technology provider
74	Mobile motion Technologies Private Limited	Technology provider

PDOA's/App provider Weekly Reporting Format

Weekly Reporting to TRAI by App Providers

This needs to be completed on a weekly basis. These responses will be used by TRAI for internal consumption only and shall be kept confidential. At the end of the pilot, a Wi-Fi Pilot Report by TRAI containing only aggregated responses will be shared with all the participants.

* Required

1. Email address *

2. App Provider ID *

Your UUID

3. Reporting Period (Start Date) *

Example: December 15, 2012

4. Reporting Period (End Date) *

Example: December 15, 2012

5. Total Number of Customers that completed
KYC in the past one week *

6. Total Number of Unique Customers connected
at least once in the past one week *

7. Average Number of Sessions/Customer *

8. Average Data (MB) Consumed/Customer *

9. Total Data (MB) Consumption on Monday *

10. Total Data (MB) Consumption on Tuesday *

11. Total Data (MB) Consumption on Wednesday *

12. Total Data (MB) Consumption on Thursday *

13. Total Data (MB) Consumption on Friday *

14. Total Data (MB) Consumption on Saturday *

15. Total Data (MB) Consumption on Sunday *

16. Total Revenue Earned *

17. PDO-wise Connection Data *

Weekly Reporting to TRAI by PDO/PDOAs

This needs to be completed on a weekly basis. These responses will be used by TRAI for internal consumption only and shall be kept confidential. At the end of the pilot, a Wi-Fi Pilot Report by TRAI containing only aggregated responses will be shared with all the participants.

* Required

1. Email address *

2. Reporting Period (Start Date) *

Example: December 15, 2012

3. Reporting Period (End Date) *

Example: December 15, 2012

4. PDO/PDOA ID *

Your UUID

5. Number of PDOs (Active) in the past one week *

6. Number of PDOs (Inactive) in the past one week *

7. Number of Successful Connections in the past one week *

8. Average Amount of Data/Active Session *

9. Total Data (MB) Consumption on Monday *

10. Total Data (MB) Consumption on Tuesday *

11. Total Data (MB) Consumption on Wednesday *

12. Total Data (MB) Consumption on Thursday *

13. Total Data (MB) Consumption on Friday *

14. Total Data (MB) Consumption on Saturday *

15. Total Data (MB) Consumption on Sunday *

16. Total Revenue Earned in the past one week *

17. App Provider-wise Data Consumption in the
past one week *

Annexure XI

Wi-Fi Pilot Test System Feedback Form

	Yes	No	Remark
1. Did you find any difficulty in finding the App in Play Store?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
2. Did you find any difficulty in downloading the App?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
3. Did you receive OTP on time for the authentication?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
4. Did you find user interface of the App user friendly?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
5. Did you experience any crashing of the App on your phone?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
6. Were you satisfied by the size and the battery consumption by the App?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
7. Were you satisfied by the Access Point login through the App?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
8. Is the App sending too many notifications?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
9. Were you able to access all the Access Points installed in your building?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
10. Were you able to Access two different Access Points of different entities present on the same location?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
11. Were you able to access the same Access Points of same entity present over different location?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
12. Did you experience Wi-Fi Signal drop even if rooted to the same spot?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>

13. Did the Wi-Fi get connected seamlessly when you come back to the original position?
14. Did you experience uninterrupted service, when moving over different Wi-Fi zones ?
15. When connected, were the plan details and data quota, mentioned on the welcome screen?
16. Were you satisfied by the information displayed on the welcome screen?
17. Did you face any difficulty in paying online?
18. Did you face any difficulty in paying through a particular CC/DC/Netbanking?
19. Were you satisfied by the payment options provided by the hotspot provider?
20. Were you satisfied by the usage plans provided by the Wi-Fi provider?
21. Did you face any difficulty in using the coupon?

Overall experience of TRAI's Public Wi-Fi Pilot

Excellent Very Good Good Can be Improved

Any other remarks on App usage:

Any other remarks on Wi-Fi usage:

Name:
Division:

Annexure XII

Testimonials

(as translated from local language)

"This Wifi Dabba has helped us stand out in our community to offer a product which everyone needs today. It has helped me get more business for my tea as people spend more time here. With data available at my shop at super affordable prices, I am able to collect online payments directly in my account. Super useful for both my customers and me".

KrishnaMurthy,
owner Kabalamma condiments,
Bangalore.



"Service is really useful. When I come for my break after driving my taxi, cheap and fast internet helps me rejoice and relax for a while. Watching youtube videos and news is my favourite thing on Wifi Dabba. Thank you for this innovation."

Rajaram Rajendran
OLA/UBER driver Bangalore



"I have been using Dabba internet for 2 months now. I am a regular user as the signals are available in my PG. Super affordable, fast and reliable internet. What more you want in life!" –

Ankit,
Wifi Dabba user since December 2017.
Koramangla, Bangalore.



Testimonials (continued)
(as translated from local language)

“After putting the Wi-Fi router at my shop, the place has become popular among young people, students, and women. The Rs. 5 pack is the most popular as it is affordable as well as sufficient for a shorter duration. These women and students get their friends along with them which has increased in-store daily footfall by 50%. The Wi-Fi router has mobile charging points as well which is a big convenience. to attracting people in the vicinity. A lot of time it happens, people come to top-up their pre-paid phone when they notice pre-paid wi-fi packs. Because of the router, my daily business has witnessed an increase of 15%. I am thankful to TRAI and i2e1 for installing the Wi-Fi Router. Now, even my family has an easy access to the internet”.

Alam S,

Kirana Store owner, Naraina Delhi.



“Initially, my daily earning used to be Rs. 700(approx.). Around two-and-a-half months ago, I got i2e1 Wi-Fi router installed at my shop and started selling pre-paid Wi-Fi coupons for between Re.1 to Rs.100. Post installation, I have noticed 30% growth in the number of people coming to my shop. Mostly, younger people, between the ages of 15 and 25 buy the coupons. The maximum selling is Re. 1 coupon that gives users a five-minute connection. My daily earnings have now increased to Rs. 800(approx.). I have asked a lot of my friends to get this Wi-Fi Router.”

Braham Prakash,

Stationery Shop Sangam Vihar Delhi



Stakeholders Feedback Form

Technical Feedback: Public Open Wi-Fi Architecture & Specification (v0.5)

Reference Architecture & Specification:

http://www.trai.gov.in/sites/default/files/Public_Wifi_Architecture_12072017_1.pdf

Please submit any technical feedback (feature ideas, bugs, etc) you may have. Based on your feedback, we shall make necessary improvements to the architecture before publishing the final version.

* Required

1. **Email address ***

2. **App Provider, PDO, or PDOA ID ***

Your UUID

3. **Feedback: New Features / Ideas / Bugs ***

For New Features and Ideas, please provide a detailed explanation of the expected functionality along with the reasoning behind the same. If you're reporting a bug, please provide the precise steps to reproduce, expected results and actual results.

Business Feedback: Public Open Wi-Fi

* Required

1. Email address *

2. App Provider, PDO, or PDOA ID *

Your UUID

3. Do you believe that the Public Open WiFi Framework enables the creation of sustainable and scalable business models? *

Mark only one oval.

Yes *Stop filling out this form.*

No *Skip to question 3.*

Business Feedback: Public Open Wi-Fi

4. Why does the Public Open WiFi Framework not enable the creation of sustainable and scalable business models? *

Please be specific in your response.



Telecom Regulatory Authority of India



Public Open Wi-Fi framework

Architecture & Specification (Version 1.0)

Mahanagar Door Sanchar Bhawan, Jawahar Lal Nehru
Marg, New Delhi – 110002

Table of Contents

Introduction.....	
Project Mission	
Document Objectives	
Glossary of Terms	
Detail Specifications.....	
High Level Architecture	
Players in the ecosystem.....	
High Level Flows	
Specifications.....	
Provider Registry	
User Signup and Profile Management	
Access Point Discovery	
Connecting to Access Point and Usage	
Compliance Aspects	
Wi-Fi Provider	
App Provider	
CONCLUSION	

Introduction

The Internet is the single most self-empowering infrastructure available for a citizen in the 21st century. The World Bank observed that a 10% increase in internet penetration leads to a 1.4% increase in GDP. Access to the Internet is considered a basic human right by many countries globally, including Estonia, Finland and France. In India, access to data is still limited due to poor coverage of fiber/telecom and prohibitive pricing of cellular data.

WiFi is a complementary, not competing technology to LTE. Public hotspots hold an important place in the last-mile delivery of broadband to users. WiFi is much easier to scale than adding new LTE towers. It bolsters connectivity inside buildings, airports, etc. where LTE penetration is inherently limited. It allows for offloading from telecom networks to ease congestion, and will be crucial when the next billion IoT devices come online. Yet, there are only 31,000 public WiFi hotspots in India, compared to 13 million in France, and 10 million in the United States of America.

It is not enough to only install more routers. TRAI aims to offer a seamless experience to end users, both residents and international travelers. To provide a simplified, consistent experience across hotspots from various providers means unbundling authentication, payment and accounting from hardware and software running on the Access Point. This will allow small entrepreneurs such as tea shops, to set up and maintain Access Points. Whereas, device manufacturers, payment companies, ISPs/Telcos and Consumer Internet companies can provide the remaining pieces to set up Public Data Offices (PDOs).

The unbundling is also important from the point of view of scale. PDOs will be akin to the PCOs that connected all of India, even when tele-density was less than 7 telephones per 100 people. It is also suggested that the Public WiFi Hotspots store community interest data locally, and allow access to it through negligible costs. Overall, the introduction of public WiFi network, should encourage the PDOs to become bustling centers of economic activity.

TRAI has conducted multiple consultations regarding this which began in July 2016 and has released papers and notes regarding this. TRAI has also initiated a pilot in July 2017 to conduct field trials. All related documents are available on TRAI website.

Project Mission

The vision of this initiative is to establish an Open Architecture based **WiFi Access Network Interface** (WANI), such that;

1. Any entity (company, proprietorship, societies, non-profits, etc.) should easily be able to setup a paid public WiFi Access Point.
2. Users should be able to easily discover WANI compliant SSIDs, do one click authentication and payment, and connect one or more devices in single session.
3. The Experience for a small entrepreneur to purchase, self-register, set-up and operate a PDO must be simple, low-touch and maintenance-free.
4. The products available for consumption should begin from “sachet-sized”, i.e. low denominations ranging from INR 2 to INR 20, etc.
5. Providers (PDO provider, Access Point hardware/software, user authentication and KYC provider, and payment provider) are unbundled to eliminate silos and closed systems. This allows multiple parties in the ecosystem to come together and enable large scale adoption.

Document Objectives

This document intends to provide detailed technology specifications for various providers to ensure full WANI system interoperability. All providers must ensure compliance with this specifications to be part of this initiative. This is a technical document and does not fully cover detailed policy aspects and enabling framework.

TRAI believes that through unbundling of services, multi-provider ecosystem, and easy regulatory process, millions of WiFi access points can be enabled across the country that allows users to connect via single-click authentication and use it with ease.

NOTE: This is a draft specification which may undergo changes before becoming final specifications based on feedback from ecosystem during pilot.

Glossary of Terms

PDO	Public Data Office
PDOA	Public Data Office Aggregator
APP	Application – mobile app provisioned as frontend for users to access and connect to the available WiFi hotspots
AP	Access points distributed across the city
IP	Internet protocol address assigned to all the elements in the architecture
JSON	JavaScript Object Notation
URI/URL	Uniform Resource Identifier/Locator
CP	WiFi Captive Portal
OTP	One Time Password
SSID	Service Set Identifier
MAC	Media Access Control – A globally unique ID/address given to physical network devices.
ACCESS POINT	Wireless hardware device that allows other devices to connect over WiFi to a network/Internet.
HOTSPOT	A physical location where WiFi Access Point is available for people to connect to Internet.

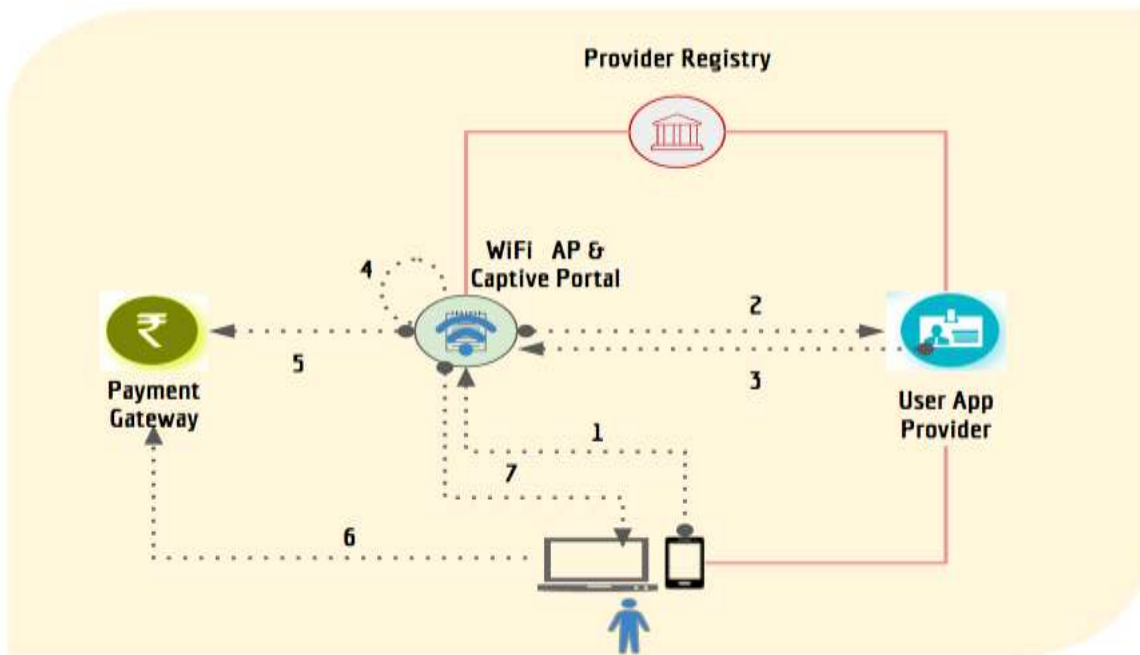
Detail Specifications

High Level Architecture

Players in the ecosystem

- **PDO/PDOA:** Any Indian entity (companies, associations, small merchants, etc.) having a PAN number wanting to provide one or more WANI compliant WiFi hotspots to public using either free or paid model. They conform to the governing rules laid out by TRAI under this framework.
- **Hotspot Hardware/Software/Service Provider:** Any software or service provider who is providing necessary software, hardware, services, and/or support for PDOs to setup WANI compliant WiFi hotspot. These can be any software/service provider, either Indian or global. It is expected that these providers will offer a WiFi-in-a-box solution for PDOs. Their software will need to be compliant to specifications laid out in this document. They will also integrate with a bank or a payment gateway for collecting payment from user.
- **User App Provider:** Any company providing a software application and backend authentication infrastructure for users to signup, discover WANI compliant WiFi hotspots, and do single-click connect from within the app. This app allow users to create a profile, do their KYC (mobile verification), and allow setting up preferences for MAC-IDs for various accessing devices and payment methods. This app should allow users to discover WANI compliant hotspots and connect to it. In addition, App Provider must offer a backend user authentication service that is called by WiFi Captive Portal software whenever user connects to obtain a signed user profile.
- **Central Registry of Providers (or simply Provider Registry):** A central registry managed by DoT/TRAI or an entity approved by DoT/TRAI containing information about the PDOs/PDOAs, and User App providers in a digitally signed XML format. This is a relatively static registry where approved providers are allowed to manage their profiles. Actual specification of the registry is provided later in this document.

High Level Flow



One Time Flow

One time flows are depicted in red lines in above diagram.

- PDO/PDOA completes Self-Registration with Provider Registry using their public certificate (for signature validation). They also register their WiFi Access Points, SSIDs, and locations.
- User App provider is also registered with Provider Registry along with their authentication URL and public certificate (to validate their digital signature).
- User completes one time KYC with App Provider through their App. User App caches trusted SSIDs from Provider Registry from time to time.

Usage Flow

Usage flows are depicted in dotted lines in above diagram. Bullet number below corresponds to the number depicted within the diagram above.

1. User opens the App in which user has already registered and allows discovery and connection to WANI compliant WiFi access points. Within the app, user browses for nearby WANI compliant SSIDs and then chooses one SSID to connect to.
2. WiFi Captive Portal of the PDO initiates user authentication with App provider backend using the token passed from the app.
3. App provider backend returns a signed user profile token back to WiFi Captive Portal.

4. WiFi Captive Portal displays data packs available with their charges. User selects desired data sachet, click to confirm the terms.
5. WiFi Captive Portal sends request for payment through their payment gateway.
6. User completes payment.
7. PDO activates all device MAC-IDs that were part of the signed profile and allows them to connect to the session without additional authentication. Pack is activated and user can begin browsing.

Specifications

Following sections describe the technical specifications for Provider Registry, user signup, user authentication, and usage. Providers must ensure they comply with these specifications for ensuring interoperability across the country.

Provider Registry

Provider registry is maintained by DoT/TRAI for ensuring all authorized providers are identified, discovered, and trusted by the ecosystem. Providers will be given an account on the site where registry is maintained for managing their profile, public keys, and other details.

Currently the Provider Registry XML will be made available on the following URL:

https://tra.gov.in/wani/registry/wani_providers.xml

This registry XML will be updated whenever data changes in provider database. Applications reading this and caching the registry should respect the “ttl” (Time to Live) parameter and ensure it is refreshed to get latest data. It is also critical to ensure sub-registries linked via the main registries also need to be downloaded based on the need.

Schema (XSD will be made available separately) for wani_providers.xml is:

```
<WaniRegistry lastUpdated="" ttl="">
  <PDOAs>
    <PDOA id="" name="" phone="" email="" apUrl="" status=""
rating="">
      <Keys>
        <Key exp="">base-64 encoded public key</Key>
      <Keys>
    </PDOA>
  </PDOAs>
  <AppProviders>
    <AppProvider id="" name="" phone="" email="" authUrl="" status=""
rating="">
      <Keys>
        <Key exp="">base-64 encoded public key</Key>
```

```

    <Keys>
  </AppProvider>
</AppProviders>
</Signature>
</WaniRegistry>

```

Element/Attribute	Description
WaniRegistry	Root element of the registry
WaniRegistry→last Updated	Timestamp in YYYYMMDDhhmmss format providing when the registry XML was last updated. Useful for cache refresh.
WaniRegistry→ttl	Time To Live in hours suggesting how long this data should be cached before checking for change. Default is "24".
WaniProvider→PDOAs	Parent element for listing of all PDOAs.
PDOAs→PDOA	Repeating element providing one entry per PDOA.
PDOA→id	Unique provider ID within the registry.
PDOA→name	Name of the provider entity.
PDOA→phone	Contact number of the provider entity.
PDOA→email	Email of the provider entity.
PDOA→apUrl	URL to the signed XML where all WiFi Access Points of this providers along with MAC-IDs, and location is listed. This list is grouped by location to make it easier for applications to cache parts of this. At a later point, when the number of entries are in millions, this list itself may be further split with URLs pointing to sub-lists. Applications should start from this main registry and use the URLs within these XMLs to auto navigate the complete registry.
PDOA→status	Current status of the provider. Valid values are INPROCESS, TEMPORARY, ACTIVE, INACTIVE, SUSPENDED, BLACKLISTED.
PDOA→rating	User rating of the provider. This is a decimal value between 0 and 5. This is meant for future use.
PDOA→Keys	Parent element where public keys are listed.
Keys→Key	Individual public keys to validate the signature of the PDOA. When integrating via APIs across ecosystem partners, it is necessary to sign the API requests and responses to establish trust. This element will contain the base-64 encoded certificate in X509 V3 format. Currently SHA256withRSA (2048 bit key) is the supported signing algorithm.
Key→exp	Expiry of the key in YYYYMMDD format. This is provided to support co-existence of multiple keys and is

	required for key rotations.
Waniprvider →AppProviders	Parent element for listing of all user application providers.
AppProviders →AppProvider	Element representing individual app provider.
AppProvider→id	Unique id of the app provider within the registry.
AppProvider→name	Name of the app provider.
AppProvider→phone	Contact number of the app provider.
AppProvider→email	Email of the app provider.
Appprovider→authUrl	Authentication URL (API endpoint) of the app provider against which WiFi Captive Portal will call to authenticate and obtain the signed user profile. This must be an HTTPS URL into which authentication input data can be sent in the body.
AppProvider→status	Current status of the provider. Valid values are INPROCESS, TEMPORARY, ACTIVE, INACTIVE, SUSPENDED, BLACKLISTED.
AppProvider→rating	User rating of the provider. This is a decimal value between 0 and 5. This is meant for future use.
AppProvider→Keys	Parent element where public keys are listed.
Keys→Key	Individual public keys to validate the signature of the AppProvider. When integrating via APIs across ecosystem partners, it is necessary to sign the API requests and responses to establish trust. This element will contain the base-64 encoded certificate in X509 V3 format. Currently SHA256withRSA (2048 bit key) is the supported signing algorithm.
Key→exp	Expiry of the key in YYYYMMDD format. This is provided to support co-existence of multiple keys and is required for key rotations.

WiFi Access Points (pointed by "apUrl" parameter of the PDOA) XML format:

```

<WaniAPList lastUpdated="" ttl="" providerId="">
  <!-- location element repeats -->
  <Location type="DISTRICT" name="" state="">
    <AP macid="" ssid="" cpUrl="" status="" rating="" geoLoc="">
      <Tag name="OPENBETWEEN" value="" />
      <Tag name="AVGSPEED" value="" />
      <Tag name="FREEBAND" value="" />
      <Tag name="PAYMENTMODES" value="" />
    </AP>
  </Location>
</Signature>
</WaniAPList>

```

Element/Attribute	Description
WaniAPList	Root element of the registry where all WANI compliant WiFi Access Points are listed for a provider.
WaniAPList→lastUpdated	Timestamp in YYYYMMDDhhmmss format providing when the registry XML was last updated. Useful for cache refresh.
WaniAPList→ttl	Time To Live in hours suggesting how long this data should be cached before checking for change. Default is "24".
WaniAPList→providerId	Id of the provider. This is same id as the WaniRegistry XML.
WaniAPList→Location	Repeating element organized by location of the Access Point.
Location→type	Type of location used for grouping. Currently it will be grouped by DISTRICT. In future further grouping may be supported.
Location→name	Name of the location which is used for AP grouping. Currently this will be name of the district.
Location→state	Name of the State in which this Access Point is located.
Location→AP	Element depicting one Access Point. This element repeats.
AP→macId	MAC-ID of the Access Point.
AP→ssid	SSID of the Access Point.
AP→cpUrl	URL of the WiFi Captive Portal
AP→status	General status of the AP. Valid values are ACTIVE, INACTIVE.
AP→rating	User rating of the provider. This is a decimal value between 0 and 5.
AP→Tag	<p>Various tags describing the AP features.</p> <ul style="list-style-type: none"> ● OPENBETWEEN – value should be in the format hh-hh where hh represents time between 00 and 24. E.g., 09-17 (depicting 9 am to 5 pm) or 00-24 (depicting 24 hr availability). ● AVGSPEED – Average speed in Mbps of the AP. It should be a positive integer. E.g., 2 meaning 2 Mbps. ● FREEBAND – If this AP offers any free band in minutes. E.g., a value 10 depicts 10 free minutes. A Special value -1 depicts ALWAYS free. ● PAYMENTMODES – Allowed payment modes. Values can be CASH, COUPON, CREDITCARD, DEBITCARD, NETBANKING, UPI, and WALLET. More enumerations may be added based on RBI approved payment schemes in India.

User Signup and Profile Management

Users are expected to use some software application (mobile/desktop/etc.) provided by the “App Provider” for user signup, KYC, and profile management. User App should provide the following key features during user signup and profile management:

1. Users install an app from the App Provider.
2. App MUST capture user mobile number and does a mobile number verification (via OTP or GSM Mobile Connect or any other mechanisms).
3. App also allows creation of mandatory “username” which is unique within the App Provider system. This is shared with WiFi provider during authentication and used for audit and traceability.
4. App should allow user to setup profile with additional **optional** attributes:
 - a. Email – user should be able to optionally setup email for getting alerts, etc.
 - b. Preferred payment address – This is ONLY for capturing UPI or Wallet address in the form **upi://vpa/token** (VPA is Virtual Payment Address for UPI collect transaction) or **wallet://acc-no@ppi/token**. App provider MUST NOT capture or store ANY sensitive information such as credit card number. All other types of payment will be directly handled by WiFi Captive Portal.
 - c. If the User App is also a payment app (like UPI/Wallet app), then additional optional token string can be used to provide auto-deduct/offline/other additional payment functionalities.
5. App MUST also allow users to easily add/remove devices (MAC-ID and a name) which they want to connect to various Wi-Fi hotspots.
 - a. This allows the user to have more than one device to be connected to WiFi hotspots within same session.
 - b. This is critical to allow IoT devices used by user to also connect using the common app and authentication. For example, by connecting the mobile phone to the WiFi network, user may also connect his/her laptops or connected cars or other future devices.
 - c. Optionally app may also provide “device group” profiles to allow users to define named group of devices so that they can choose one group vs another during connecting.

Access Point Discovery

1. User App should allow users to discover nearby WANI compliant Access Points by detecting nearby SSIDs and verifying the MAC-IDs against the SSID Registry.
2. In addition, optionally user App can provide location specific searches and allow users to discover “nearby” WiFi hotspots without being the WiFi range. SSID registry can be cached locally by app smartly for doing location level searches.
3. App should also optionally allow users to save “favorites”, “most recent”, etc. for easy selection of regular connections.
4. In addition, ideally App may also provide easy sorting and selection of access points based on the “Tag” attributes such as when AP is available, average speed, rating, etc. This allows users to select best AP within available selections.
5. App must provide a mechanism for users to rate the access points and providers.

Connecting to Access Point and Usage

1. Whenever users want to connect to public Wi-Fi hotspot using this scheme, they can open their App, browse WANI compliant Wi-Fi hotspots (see section on discovery above), and click connect.
2. App creates a token **waniapptoken** which needs to be passed to WiFi Captive Portal. This token is created as below:

```
waniapptoken = <app-provider-id>|<enc-token>
enc-token MUST NOT be a fixed value to ensure it is not can be reused
beyond a session. It MUST be encrypted using App provider public key
so that only App provider backend can decrypt this token. It is created
as below:
enc-token = base-64(RSA-Encrypt(token))
token = {
  "ver": "1.0", // version of the token structure
  "timestamp": "YYYYMMDDhhmmss",
  "username": "", // username of user
  "appId": "", // App id to handle multiple apps from same provider
  "appVer": "", // version of app to handle multiple app versions
  "totp": "", // TOTP generated by the app. This is essential to ensure
                App provider server can trust origin of this token
  "custData": {} // any custom JSON data structure needed by the app
}
```

3. App base-64 encodes the token and passes it on to captive portal using parameter name **waniapptoken** (can be passed as part of GET parameter). E.g.,

```
http://portal.com/?waniapptoken=
FG23A|ZDM3MzQxM2RIYjc0NGIyNGM2MjI2MTM2MTY0MGVmN2Q3MGI
4YjcxZjlmMTMyOTQ4NzdmNmY5OWViZjFINTk3Yg==
```

4. WiFi provider's Captive Portal should look for waniapptoken parameter and process it as below:

- a. Extract the App Provider ID from the token prefix (string until the "|" delimiter within the token).
- b. Verify the App Provider ID against the locally cached WANI Registry (WaniRegistry→Appproviders→Appprovider[id={id}]) and obtain authUrl for that App provider.
- c. Encrypts the waniapptoken using PDOA private key as below to create a new token **wanipdoatoken**

```
wanipdoatoken = <PDOA-Id> | <key-Exp> | <base-64(RSA-
Encrypt(waniapptoken))>
```

- d. Calls the authUrl by passing the signed token wanipdoatoken as part of the URL parameter. This MUST BE an https call.

```
https://auth.app-provider.com/?wanipdoatoken=
12GF34|MjAxODA4MTV8NTI0MDIyOTM5NTdBRTE4N0Q3RDdBOTF
EMEU1OEU2RTQ3OUU4NDAzRkIyMDQwM0U5N0ZGQzQ1RTE1RD
RBMjcwMw==
```

5. App Provider backend server should do the following on their server:
 - a. Extract the PDOA-Id from the parameter (token prefix).
 - b. Verify the PDOA ID against the locally cached WANI Registry (WaniRegistry→PDOAs→PDOA[id={id}]).
 - c. Once verified, take the public key of the PDOA corresponding to the key-exp parameter from WANI registry (WaniRegistry→PDOAs→PDOA[id={id}]→Keys→Key[exp={key-exp}])-
 - d. Decrypt using the waniapptoken from the wanipdoatoken using the public key of the PDOA.
 - e. Decrypt waniapptoken using their own private key and verify the token structure, TOTP, etc.

6. After validation of the waniapptoken, App Provider should return the following structure back to WiFi Captive Portal:

```
{
  "ver": "1.0", // version of the profile format
  "app-provider-id": "", // mandatory - ID from WaniRegistry
```



```

"app-provider-name": "", // name from WaniRegistry
"timestamp": "YYYYMMDDhhmmss", // current timestamp
"Username": "", // mandatory
"payment-address": "", // upi://vpa/token or wallet://ac-
no@ppi/token
"Devices": [], // device MAC-IDs array if any for current session
"signature": "", // computed for this structure (see below)
"key-exp": "" // Key→exp value of the key pair used for signature
}

```

Signature is computed as below:

signature = base-64(RSA-Encrypt(hash))

hash = SHA-256(timestamp+username+payment-
address+devices[0]+...+devices[i])

7. Once Wi-Fi hotspot provider obtains response, it needs to do the following verification:
 - a. Decrypting the hash from signature using the public key of the App provider (that corresponds to Key→exp value from registry).
 - b. Calculate the hash and verify if the hash is matching.
 - c. If matching, proceed with next steps. If not, show error and allow user to disconnect and connect again (try again).
8. After verification, Captive Portal should show the user available packages. Once the user chooses a package, user should be directed to make payment on the portal.
9. If user profile had preferred payment address, then it should be defaulted and allow user to do payment without any data entry on the portal.
10. WiFi provider will have to allow user to make payment during which time user must be given temporary Internet access to payment provider's server.
11. Once payment is confirmed, WiFi Access Point should now allow all devices (MAC-IDs within user profile) to be connected to same session and share the package. This is critical for single-click access to Internet for multiple devices that users typically carry around these days without each devices having to go through same process. This is a MANDATORY compliance requirements for WANI PDO/PDOAs.
12. When the session is about to expire, hotspot provider can prompt the user and requests extension of the session and charge additional amount ONLY WITH explicit user consent without user having to go through all steps again.

- a. Note that users who connect to their favorite WiFi hotspots can “pre-authorize” payment through Wallet or UPI e-mandate (part of UPI 2.0) which makes even payment a single click seamless experience. This also allows WiFi providers to easily extend user sessions with single user click “extend my session (charge Rs.xx)” without any further steps to make payment.

IMPORTANT NOTE: With single click user authentication through authorized Apps and payment pre-authorization via e-mandates, connecting and using public WiFi will be a seamless, friction free experience for users.

Compliance Aspects

WiFi Provider

1. Captive portal must allow standard connection and authentication as per this specification.
2. WiFi Provider must provide choice to user to select a package with clear details of the package.
3. Captive portal should respect and handle preferred payment scheme for users and allow seamless collection of payment once the package is selected.
4. WiFi provider must comply and be certified with regulatory and security rules for payment transactions, auditing, and storage/handling of any sensitive payment information.

App Provider

1. App provider must provide an App to user (for any device/OS based on market needs) and comply with user sign up, profile management, and authentication specifications as per this document.
2. App provider must ensure user data is strongly protected to ensure user privacy and data security is ensured.
3. App provider must have a mechanism to allow regular app update and improvements.
4. App is encouraged to provide good user interface for consumers to easily discover, search, find best access points, and connect to it with single-click.

CONCLUSION

Telecom industry is seeing rapid transformation through drop in data prices, increased speed, and increased consumption of data packs. India is also creating a slew of digital platforms to help its citizens with better access to various services. According to reports, Indians consumed more cellular data than China, and as much as the USA in the current cellular data pricing regime. TRAI believes that by adopting an Open Architecture approach, emphasis on innovation and consumer experience is placed as the winning criteria.

This document provide technical architecture specifications for an interoperable ecosystem. The WiFi Access Network Interface (WANI) represents an exciting opportunity to do for data what PCOs did for Long Distance Calling. It will bring a new generation of users and entrepreneurs into the market to bridge the need of last mile connectivity. The opportunities created are immense and will benefit 100's of millions of users in India waiting to get affordable access to Internet.

----- END -----

Sample Criteria for App Provider Certification

Parameter	Yes	No	Remarks
Is the app available on Android?			
Is the app available on iOS?			
Is the app compatible with most/latest android/iOS versions?			
Does the app experience regular crashing on a particular android/iOS version? If so please mention.			
Does the app usually send OTP within 30 seconds for the authentication?			
Does the app comply with the user sign-up specifications as per the document on WANI?			
Does the app comply with the user profile management specifications as per the document on WANI?			
Does the app comply with the authentication specifications as per the document on WANI ?			
Does the App send too many notifications?			
Does the app provide optimal battery consumption performance?			
Does the app provide a good user interface for consumers to easily discover, search, find best access points, and connect to them with single-click?			
Does the app provide seamless/smooth access point login experience?			
Does the app be able to login onto two different Access Points of different PDOA's present on the same location?			
Does the app be able to login onto two different Access Points of different PDOA's present on the different location?			
Does the app-provider have a publicly accessible user guide/ FAQs page?			
Does the app-provider have a support contact number/email ID for addressing queries/ grievances in regards to the app?			
Does the app have proper error handling and present appropriate user-friendly error messages, especially for common issues?			
Does the app provide response to any action on the app within 5 seconds?			

Sample Criteria for App Provider Certification

Parameter	Yes	No	Remarks
Does the captive portal provide standard connection and authentication as per the specifications in WANI document?			
Does the Wi-Fi provider furnishing satisfactory payment options as per the WANI document?			
Does the Wi-Fi provider furnishing satisfactory usage plans as per the WANI document?			
Does the captive portal provide a choice to the user to select a package with clear details of the package?			
Does the captive portal have a responsive UI such that it can be easily used on devices with different screen sizes?			
Does the captive portal respect and handle preferred payment scheme for users and allow seamless collection of payment once the package is selected?			
Is the Wi-Fi provider certified with regulatory and security rules for payment transactions, auditing, and storage/handling of any sensitive payment information?			
Does the captive portal UI render well on the latest 2 major versions of Chrome-Mobile?			
Does the Wi-Fi provider cater the issue of Wi-Fi Signal drop even if rooted to the same spot?			
Does the Wi-Fi provider cater the uninterrupted user experience, when moving over different Wi-Fi zones?			
Does the Wi-Fi provider provide an email/case-ticket management or contact number support for addressing queries/ grievances in regards to the installation of Access Point and operation of a PDO?			
Is there a mechanism to log and export on demand the details of any data consumption including the User account ID, session duration, devices connected, data packets consumed (with app and website breakdown)?			
Is there a captive portal screen wherein the user could view his data consumption history including session duration, devices connected, data packets consumed (with app and website breakdown)?			
Is there a captive portal provide a screen wherein the user could view his payment history at PDOs along with details of time-stamp, location, payment amount, payment medium etc.?			
Does the captive portal have proper error handling and present appropriate user-friendly error messages, especially for common issues?			

Gallery Various PDO's across Nation



Access Points Deployed at TRAI Offices



Abbreviations Used

S.No.	Abbreviation	Description
1	AAA	Authentication, Authorization, Accounting
2	BB	Broadband
3	CIF	Customer Identification
4	eCAF	Electronic Customer Application Form
5	eKYC	e-Know Your Customer
6	GDP	Gross Domestic Product
7	GSMA	GSM Association
8	IEEE	Institute of Electrical and Electronics Engineers
9	IIIT	International Institute of Information Technology
10	ISP	Internet Service Provider
11	MAC	ID Media Access Control
12	MWA	Microwave Access
13	MWB	Microwave Backbone
14	NOC	No Objection Certificate
15	NSO	Network Service Operator
16	OTP	One Time Password
17	POP	Point of Presence
18	PCO	Public Calling Office
19	PDO	Public Data Office
20	PDOA	Pubic Data Office Aggregator
21	RoW	Right of Way
22	SIM	Subscriber Identity Module
23	SSID	Service Set Identifier
24	TSP	Telecom Service Provider
25	UASL	Unified Access Service License
26	UL	Unified License
27	UPI	Unified Payment Interface
28	VNO	Virtual Network Operator
29	WANI	Wi-Fi Access Network Interface
30	WBA	Wireless Broadband Alliance
31	WLAN	Wireless Local Area Network
32	Wi-Fi	Wireless Fidelity