Telecom Regulatory Authority of India

Consultation Note

on

Model for Nation-wide Interoperable

and

Scalable Public Wi-Fi Networks

New Delhi

15th November 2016

Mahanagar Door Sanchar Bhawan,
Jawahar Lal Nehru Marg,
Next to Dr. Zakir Hussain College,
New Delhi – 110002

Written Comments on the Consultation Notes are invited from the stakeholders by 25/11/ 2016. Comments will be posted on TRAI's website www.trai.gov.in. The comments may be sent, preferably in electronic form, on the email ID broadbandtrai@gmail.com

For any clarification/ information, Shri Arvind Kumar, Advisor (Broadband & Policy Analysis) may be contacted at Tel. No. +91-11-23220209 Fax: +91-11-23230056.

Contents

Chapter I

Interoperable Architecture for Enabling Wi-Fi Hotspots

A. Introduction

1. 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, the Telecom Regulatory Authority of India (TRAI) released a consultation paper on "**Proliferation of Broadband through Public Wi-Fi Networks**" on 13th July 2016. 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; and (iii) collaborative partnerships between various entities of the ecosystem.

B. Motivation for large scale deployment of Pubic Wi-Fi networks

2. The three components of Digital India envisioned by our Prime Minister include the following:

   a) Digital Infrastructure that forms the backbone.

   b) Software and services provided over the infrastructure that enable provisioning of various types of digital services to citizens.

   c) Digital Empowerment of citizens enabled by the consumption of Digital services.

3. Public Wi-Fi networks can be effective complement to the wired and wireless mobile broadband infrastructure in the country to achieve the vision of Digital India as stated above.

4. The possible uses of public Wi-Fi networks include the following:

a) Provide better in-building coverage.

b) Provide mobile data offload thus relieving capacity in the macro cellular networks which use the scarce licensed spectrum.

c) Possible ubiquitous seamless Internet connectivity.

d) Provide Over-The-Top applications and services much similar to that provided over mobile broadband networks that can be location and context aware and provide opportunities for monetization of the same.

5. In summary, the public Wi-Fi networks should be:

a) Scalable to provide ubiquitous coverage across metros, cities, towns and villages;

b) Provide affordable access;

c) Leverage on relevant technology standards for successful interoperability and adoption.

C. Problems and challenges in large scale deployment of Public Wi-Fi

6. Following problems were cited in large scale deployment of public Wi-Fi:

a) With stagnated growth in landline, backhaul for Wi-Fi networks is a challenge

- Wireless backhaul has spectrum scarcity and assignment challenges
- Wired backhaul (i.e. optic fibre) is still expensive and has Right of Way challenges for large scale roll-outs

b) Authentication is still cumbersome and inflexible; requires mechanisms such as One Time Password (OTP) that necessitates the requirement of mobiles with appropriate SIMs which is a potential problem for foreigners and tourists

c) Providing carrier grade Wi-Fi is a challenge due to inadequacy of associated infrastructure such as power availability, operating conditions, and seamless hand-offs.

d) Payment mechanisms are still evolving and seamless interoperable payment system for Wi-Fi networks is not yet adopted. Hence matured monetization models have not evolved.

e) Not all spectrum in the globally harmonized band for Wi-Fi has been released yet in India.

7. Comments and counter-comments on the Consultation Paper from various stakeholders were received which have been placed on TRAI's website. To augment the consultation process it was decided that a workshop be conducted which would enable holding meaningful discussions and arriving at possible solutions.

8. In the workshop held on 28th September 2016 at Bengaluru. **TRAI,** in academic partnership with the International Institute of Information Technology Bangalore (IIIT-B), set the stage for exploring the issues.

9. The workshop was attended by telcos, Internet Service Providers (ISPs), payment solution firms and start-ups, Wi-Fi solution providers, Wi-Fi/ mobile device makers, academia, system integrators, Network Equipment Manufacturers, Software Vendors, and government officials.

10. Experts from different areas and industry segments presented their view points and shared experiences. Based on the deliberations and inputs received from the workshop, this consultation note intends to explore technical and commercial options for large scale nation wide deployment of Public Wi-Fi network infrastructure in the country.

D. The objective of this consultation note is two-fold:

a) To explore whether the model proposed in this Note can be incorporated in Public Wi-Fi networks to promote appropriate monetization and business models for sustainable and scalable infrastructure deployment.

b) To 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.

E. Authentication and Payment Interoperability using National APIs

11. As indicated, the authentication and payment mechanisms that exist today for accessing Public Wi-Fi networks are cumbersome and tedious. No single standard exists and hence it is not scalable and interoperable across the country.

12. Following are the requirements for implementing an interoperable payment system for Public Wi-Fi:

- Trusted authentication is a necessity;
- Payment information flow should be secure at various stages of the process;
- Should support both pre and postpaid models;

13. One possible way to create such a unified authentication and payment infrastructure is to leverage the national open Application Programme Interfaces (APIs) implemented for Aadhaar, eKYC (e-Know Your Customer), and Unified Payment Interface (UPI).

14. During the workshop a model allowing consumers one-click subscription with no data entry was proposed. The architecture (Figure 1) is primarily for addressing single click subscription across any Wi-Fi hotspot in a

secure and convenient fashion. The objective is to allow any small or large entity to create and offer a public Wi-Fi hotspot(s) with associated authentication and payment mechanisms offered as a software service.

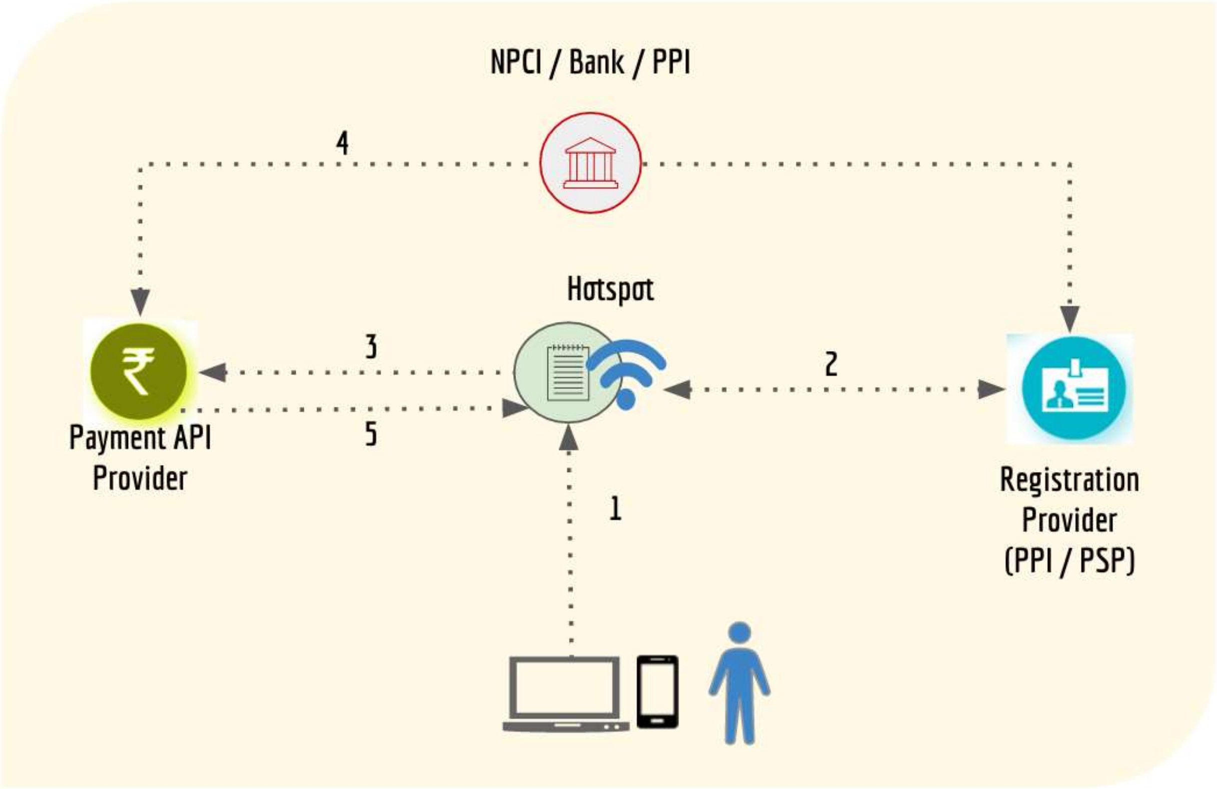

Figure 1 Proposed Architecture for 1-Click authentication and Payment for Public Wi-Fi access

Following are the players/components of such an ecosystem:

a) **Registry**: A central system having information about the hotspot providers. This is a relatively static registry where providers are allowed to register and manage their profiles, their public keys, SSIDs, etc.

- System should allow self-registration of providers in a fully electronic way via a portal and/or APIs. This is critical for achieving scale.

- Registry provider should eliminate manual approval, paper applications, etc. through fully automated electronic validation of entity through their CA certificate and PAN.
- Registry provider should have capability to suspend or blacklist a provider in special situations that require such action.

b) **Hotspot Provider**: Any Indian entity (companies, associations, small merchants, etc.) having a PAN number wanting to provide one or more hotspots to public using either free or paid model. They conform to the governing rules laid out by TRAI under this framework. This entity must be registered in Provider Registry with the following details:

- Entity Name, contact details, Public key to validate their network SSID(s) and locations for easier discovery and validation.

c) **Registration App Provider**: Any wallet or UPI app provider can play this role. Their application should provide features to manages their KYC (mobile or Aadhaar) backed profile and allow users to easily connect to hotspots. These entities should provide their public key for signature validation and be listed on TRAI registry so that hotspot providers can trust their signed authentication responses with user profile data. Following details may be captured within the registry:

- Entity Name, contact details, Public key to validate their DSC, authentication URL (against which hotspot providers will call to authenticate and obtain user profile), App link, etc.

d) **Hotspot 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 Hotspot providers to get everything up and running.

e) **Payment API Provider**: Any entity providing necessary APIs and SDKs to Hotspot provider system to integrate, connect, and collect payment using Wallet and UPI.

15. The proposed system involves two flows: (i) Registration flow to enable registration of Wi-Fi provider and (ii) Subscription flow to enable users to register for Wi-Fi network service, details of which are given below:

a) Registration Flow

i. Users can use the application (mobile/desktop) from any of the User Registration Provider as their preferred application to create profile and use that to connect to any hotspot. Registration app should provide the following key features:

- Users install an app from one of the preferred Registration Providers. Allow users to create a profile with verified mobile/ Aadhaar as they normally do with wallet/UPI apps.

- Optionally allow users to easily add/remove devices (MAC-ID and a name) which they want to connect to various Wi-Fi hotspots.

- Allow users to set up payment rules for Wi-Fi usage (pre-authorize a provider, pre-authorize max amount, etc.).

b) Subscription Flow

i. Whenever users want to connect to public Wi-Fi hotspot using this scheme, they can open their wallet/UPI app, browse Wi-Fi hotspots (app may show matching SSID from registry), and click connect.

ii. App creates an encrypted token (that contains any data required by that application's server, optional list of MAC-IDs, etc.), base-64 encodes it, and creates a standard URI and passes it on to captive portal in a standardized way.

iii. App then connects to the captive portal and passes the encoded URI.

iv. Captive portal then does the following:
- Extracts the provider ID;
- Encrypts the app token with the hotspot provider private key;
- Uses the authentication URL of the provider (obtained and cached from TRAI registry) and proceeds with the authentication process;

v. Registration provider validates the token.

vi. After validation, registration provider should return the relevant following structure back to hotspot provider.

vii. Once Wi-Fi hotspot provider obtains the profile and list of devices, it should allow all devices, including the one that initiated the connection, to be connected within the same session. This allows multiple devices to be connected without multiple payments and repeat authorizations.

viii. Hotspot provider should show the name and last 4 digit of phone number in the captive portal user interface, ask for user to choose a plan, and ask user to accept terms of usage.

ix. Hotspot provider, based on the amount selected, makes the payment call to charge the amount via their payment API provider.

x. Hotspot provider charges the user and allows access to all device IDs under that user profile to seamlessly connect.

xi. When the session is about to expire, hotspot provider can prompt the user and requests extension and charge additional using the payment address. It is expected that payment (wallet or UPI) will explicitly be authorized by user (within the wallet or UPI app based on collect request) to avoid automatic charging without user knowledge.

F. Partnership Models for Public Wi-Fi

16. Nation-wide deployment of public Wi-Fi networks needs to include many hyper local partners such as the following:

- Owners of venues (malls, shops, stores)
- Telcos and Internet Service Providers (ISPs),
- Payment service providers including mobile wallet firms, banks and credit card organizations,
- Content and Application Providers (CAPs),
- Individuals and communities.

17. The number of stakeholders in the public Wi-Fi space have to be many to (i) divide the cost of operations and (ii) to add value from their expertise so as to induce adoption and increase user base.

18. One possible way is to *unbundle* the different components so that each can be taken up by different related entities such as the following:

a) Wi-Fi access point and associated connectivity provided by owners of venues such as malls, coffee shops, restaurants, hotels and kirana stores. The Wi-Fi access can also be provided by local communities as well as individuals.

b) Content Application Provider (CAP) providing local as well as global content contextualized to the situation, including product promotions and advertisements to venue customers. The local content can also be possibly provided by local communities and individuals.

c) Authentication provided through a centralized authentication registry.

d) Payment solution provided by a payment registry.

e) Backhaul and Internet bandwidth provided by Telco/ Internet Service Provider.

19. Following are possible ways to support such a collaborative partnership model:

a) Encourage deployment of public Wi-Fi networks by local entrepreneurs with support from ISP/ telco/ content providers. The systems should be easy to install, maintenance free and of low cost.

b) Include venue owners as important entity in the value chain and build sustainable business models including share of revenue from Wi-Fi services, local content delivery services. Local entrepreneurs and venue owners cannot take up the whole cost of Wi-Fi infrastructure (Capex/Opex). Invent a co-investment model with share of investment by all stakeholders including ISPs, telcos, venue owners, content providers and advertisers. The revenue splitting can also be done accordingly.

c) Local content is very much important to improve adoption of masses, especially in smaller towns and rural areas of the country. The local Wi-Fi access points with associated devices can store the locally generated content and disseminate it without the need for connecting to the global Internet. The content providers can also build suitable monetization models around the content. The local content can be promotions, and advertisements, that are monetizable and hence much like FM Radio (which is non-excludable and non-rival in nature and hence a public good) can be used by private Wi-Fi operators.

d) Neutral third party Wi-Fi providers with seamless authenticated connectivity across mobile operators and ISPs may be a possible solution to encourage large scale deployment. These neutral Wi-Fi providers can connect to any telco/ ISP backhaul in an “unbundled” manner.

e) Completely federated model with citizens putting up Do-It-Yourself Wi-Fi access points (much like HAM radio operators), sharing bandwidth to potential users. However, security and privacy of information need to be taken care of in this case.

Chapter II

Issues for Consultation

It may please be noted that answers/comments to the issues given below should be supported with justification.

Q1. Is the architecture suggested in the consultation note for creating unified authentication and payment infrastructure will enable nationwide standard for authentication and payment interoperability?

Q2. Would you like to suggest any alternate model?

Q3. Can Public Wi-Fi access providers resell capacity and bandwidth to retail users? Is "light touch regulation" using methods such as "registration" instead of "licensing" preferred for them?

Q4. What should be the regulatory guidelines on "unbundling" Wi-Fi at access and backhaul level?

Q5. Whether reselling of bandwidth should be allowed to venue owners such as shop keepers through Wi-Fi at premise? In such a scenario please suggest the mechanism for security compliance

Q6. What should be the guidelines regarding sharing of costs and revenue across all entities in the public Wi-Fi value chain? Is regulatory intervention required or it should be left to forbearance and individual contracting?

List of Acronyms Used

S No.	Acronym	Description
1.	API	Application Programme Interface
2.	CAP	Content and Application Providers
3.	DSC	Digital Signature Certificate
4.	e-KYC	e- Know Your Customer
5.	ISP	Internet Service Provider
6.	MAC-ID	Media Access Control ID
7.	NPCI	National Payments Corporation of India
8.	OTP	One Time Password
9.	PoA	Proof of Address
10.	PoI	Proof of Identity
11.	PPI	Payment Protection Insurance
12.	PSP	Payment Service Provider
13.	SDK	Software Development Kit
14.	SSID	Service Set Identifier
15.	UIDAI	Unique Identification Authority of India (UIDAI)
16.	UPI	Unified Payment Interface
17.	URI	Uniform Resource Identifier
18.	URL	Uniform Resource Locator