Association of Unified Telecom Service Providers of India

AUSPI/12/2016/034

9th December, 2016

Shri Arvind Kumar,
Advisor (Broadband & Policy Analysis),
Telecom Regulatory Authority of India,
Mahanagar Doorsanchar Bhawan,
JawaharLal Nehru Marg,
New Delhi - 110002.

Subject: AUSPI's Response to the TRAI's Consultation Note on 'Model for Nationwide Interoperable and Scalable Public Wi-Fi Networks'

Dear Sir,

Please find enclosed AUSPI's Response to the TRAI's Consultation Note on 'Model for Nationwide Interoperable and Scalable Public Wi-Fi Networks' for your consideration.

Thanking you,

Yours sincerely,

Ashok Sud
Secretary General
Mob: 9312941515

Encl: As above

Copy to :

1. **Shri R S Sharma, Chairman, TRAI**
2. **Shri Anil Kaushal, Member, TRAI**
3. **Shri Sudhir Gupta, Secretary, TRAI**

B-601, Gauri Sadan, 5, Hailey Road, New Delhi - 110 001
Tel. : 23358585, 23358989 Fax : 23327397
E-mail : auspi@auspi.in Web : www.auspi.in

AUSPI's Response to the TRAI's Consultation Note on
'Model for Nationwide Interoperable and Scalable Wi-Fi Networks'

Licensing framework has been an integral part of India's telecommunication services. The TSPs /ISPs are governed by the various license conditions for ensuring that the QoS parameters are met by the service providers. Besides the various regulatory guidelines for ensuring quality of service, the TSP/ISP do have internal checks and guidelines with the aim to ensure a good quality of experience for their customers. Also all Services providers are required to ensure appropriate security mechanisms (like LEA requirements).

The licensees over the years have developed an adequate telecommunication infrastructure as it is the key to rapid economic and social development of the country. TSPs continuously work/upgrade service for better performance in terms of capacity and consistency and not just the availability of service.

We do agree that public work Wi-Fi program would help in meeting the TRAI's expectation of affordable access and ubiquitous coverage across metros, cities, towns and villages; however, we are not sure on the workability of the model as:

- In light of the proposed architecture, the impact of such changes and integrations on current investments and flows by Telcos and ISPs need to be evaluated.
- TSPs together have 1 billion customers and are in a best possible position to manage the customer experience of users. The KYC managed by TSPs/ISPs and Banks should be considered sufficient for authentication as KYC has already been done for this pool of customers. For new customers, profile addition needs to be added.
- While the architecture allows for multiple logins using the same credentials, the DOT regulations explicitly prohibit simultaneous sessions using the same credentials.

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?

As per our understanding the main objective of the consultation note is to allow any small or large entity to offer Wi-Fi with associated authentication and payment mechanisms. The architecture proposed is complicated, as there are many ambiguities in making the model workable.

Some of the clarifications needed and suggestions as follows need to be considered before going for the Wi-Fi model proposed in the consultation note:

A. While the architecture addresses authentication model, key issues in the proliferation of pubic Wi-Fi still remain. Some of the key issues that need to be solved to improve proliferation of public Wi-Fi are:

   - Right of way permissions for last mile fiber
   - Rental requirements from venue operators
   - Free Wi-Fi requirement which limits the revenue options and hence profitability
   - Use of Street Furniture at zero costs to enable more public Wi-Fi availability

B. The framework has too many players in the value chain leading to a no single ownership of key parameters like customer experiences, QoS, security and also raises questions on economic viability for all partners in the value chain.

C. The proposed architecture puts the role of Registration APP solely on Wallets and Payment Apps which raises the basic question regarding ability of the Registrar.

D. The proposed architecture is unclear on the guidelines applicable to Hotspot Providers, Registration App providers and registry. Key questions on the ability of the smaller players to provide QoS and appropriate security mechanisms need to be evaluated in detail.

E. The telecom operators have approximately 1 billion customers for whom KYC has already been done. The framework should evaluate how this data base can be leveraged for easier and faster authentication.

F. The consultation note mentions ease of access to data service for foreigners, however, the suggested architecture does not cater for their authentication. It is suggested that the MEA's Visa data base be used for authenticating the non-Indian Citizens.

G. In the architecture proposed in the consultation note, the responsibility for the security of the network and data privacy of its user is not laid out. The criteria and tests to certify each provider of its ability to secure its own network needs to be defined a-priori. Again, expecting a small hotspot provider to do this would be extremely cumbersome and reduce the viability of a hotspot.

H. As a part of its guidelines, Hotspot providers are required to maintain the Syslog and other information required for traceability of customers. The architecture indicates that this would fall in the realm of the hotspot providers. A small hotspot provider to maintain this would be extremely cumbersome and reduce the viability of a hotspot. Moreover distributing

such critical information collection over multiple entities would lead to issues in enforcing this critical security measure.

I. The following should also be a part of the standardized architecture:
   - Ability to integrate with the existing data packs of users with their telecom is important
   - Interconnectivity to International Wi-Fi aggregators. Who will do this? Registry or registration APP providers or Individual hotspot owners?
   - Points about infrastructure and roaming are not clear in the architecture. Any regulation on whether all hotspots would be open to all is to be defined
   - Authentication of devices in an IOT scenario

Q2. Would you like to suggest any alternate model?

The alternate model suggested by AUSPI is that the following be allowed to be a Wi-Fi provider:

- Internet Service provider
- Telecom Service provider
- A Franchise to Internet / Telecom Service provider
- MVNO of ISP / TSP can also become a Wi-Fi provider by taking a licence for carrying out a licenced activity.

As brought out in our response to question 1 above, the onus of building the infrastructure for fulfilling LEA requirements shall have to be borne by the Wi-Fi Hot spot provider, thereby escalating the cost of the service. The suggested models will take care of the concerns related to affordability of services, an individual's privacy, Security agencies' requirements, QoS issuese etc. Access to data being a licensed activity, the licensee becomes responsible for ensuring these requirements as part of his license conditions.

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?

Yes, Public Wi-Fi access providers can resell capacity and bandwidth to retail users as a licensed VNO of an ISP / TSP.

Yes, 'light touch regulation' using 'registration' instead of 'licensing' would be preferable for the Wi-Fi service providers only and only if the Wi-Fi service provider is an overlay access provider / a Franchisee to an ISP / TSP.

In the proposed models suggested by AUSPI, the approach should be a light touch regulation as the providers would be working under the ambit of the TSPs/ISPs.

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

Unbundling of Wi-Fi at access and backhaul cannot and should not be allowed as access to data services is a licensed activity. However, for popularizing and proliferating Wi-Fi services, it is imperative that adequate monetization opportunities be provided for the WiFi service provider and the ISP / TSP by pragmatic re-alignment of the existing licensing conditions to benefit the subscriber. WiFi being a micro cell, it has the ability to identify pin point location of the subscriber. The WiFi provider in coordination with its backhaul service provider can utilize this inherent pointed location information for providing focus and targeted advertising to the subscribers. The monetization of this location information can be preconditioned with,

a. Utilization of location / any other additional information, like the subscriber belonging to a certain range of age, etc, to be permitted only with explicit consent of the subscriber.

b. The WiFi service provider and ISP / TSP to provide this service within the realm of the subscribers' privacy and security.

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.***

According to us in the consultation note the proposed model and architecture the capacity and bandwidth is equivalent to reselling ,which is a licenced activity that brings with it security and QoS compliance and adherence hence this should not be permissible in the model suggested by TRAI. However, if the Wi-Fi provider adopts one of the model as suggested by AUSPI then in that case this can be made permissible.

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?***

The revenue share and costing should be left to forbearance and individual contracting.

****