Reliance Communications Limited's Response to the Consultation Paper on Proliferation of Broadband through Public Wi-Fi Networks

Executive Summary

A. **No, the architecture suggested in the consultation note for creating unified authentication and payment infrastructure will not be the most suitable to enable nationwide standard for authentication and payment interoperability.**

B. **For increasing affordability of WiFi services, KYC should not be duplicated beyond that of the initial payment bank.**

C. **The registration providers should be mandated to only store the information regarding the payment banks details like amount, account number, IFSC code of the bank, etc, so that the same can be provided to the LEAs as and when required.**

D. **Possibility of authentication of the foreign visitors through MEA's data base of visa's issued should be explored.**

E. **Registration of the users should be at the respective captive portals of the Wi-Fi service provider instead of the payment portal.**

F. **WiFi service providers should be mandated to become a VNO to the TSPs / ISPs. Therefore, WiFi service providers as VNOs should be permitted multiple parenting to build on high capacity, redundant backhaul links.**

G. **A 'PCO' kind of Wi-Fi service provider / a venue owner wishing to resell the internet bandwidth of an ISP / TSP can be modeled as a franchisee of a larger WiFi service provider.**

H. **Wi-Fi hot spot roaming agreements can be mandated amongst the larger Wi-Fi hot spot providers by directing integration of their systems to each other for authentication of users and settlement of payments.**

I. **At the time of registration, provisioning of Visa information can be mandated for the foreigners intending to visit India.**

J. **Public Wi-Fi access providers should be permitted to resell capacity and bandwidth to retail users as a licensed VNO of an ISP / TSP.**

K. **Only and only if the WiFi service provider is an overlay access provider to an ISP / TSP, 'light touch regulation' using 'registration' instead of 'licensing' would be preferable for the WiFi service providers.**

L. **For popularizing and adequately monetization of the WiFi services, it is imperative that the over burdening privacy and security conditions imposed on the TSPs be relaxed and due permission be granted for sharing of anonimized information of the subscriber, with due permission of the subscribers only, for targeted advertising and promotional offers.**

M. **No regulatory intervention is required regarding sharing of costs and revenue across all entities in the public Wi-Fi value chain and it should be left to forbearance and individual contracting.**

Our specific comments on the issues posed by the Authority are given in the subsequent paragraphs.

Detailed Response

Question 1. Is the architecture suggested in the consultation note for creating unified authentication and payment infrastructure will enable nationwide standard for authentication and payment interoperability?

Our Response

No, the architecture suggested in the consultation note for creating unified authentication and payment infrastructure will not be the most suitable to enable nationwide standard for authentication and payment interoperability.

1. A detailed analysis of the authentication and payment architecture suggested in the consultation note reveals that process being suggested is leading to duplicity of existing KYC processes, cost escalation as against increasing affordability of the service and requires additional regulatory oversight for ensuring security and privacy of users personal data. Our detailed comments, including recommendations, on the same are as given below,

    a. **Duplication of KYC.** The proposed registration mechanism is duplicating the effort that has already been done at the source of payments, i.e. banks. Since the money in any e-wallet / UPI is sourced from an individual's bank account / credit card, where stringent KYC procedures are followed, repeating the same process with the registration service provider is not required as, once a customer would pay for availing the service, at the WiFi Hot Spot providers end, the customers' traceability trail automatically gets established.

    b. **Decrease Affordability.** Duplicating the same effort at the registration service provider's end, even with e-KYC, shall entail establishment of adequate storage space for storing the e-KYC information. One of the biggest advantage of digitization is that it enables exploitation of the advantages of economies of scale as the utilization of services grow. Duplicating the efforts for storing KYC information would be going against the principle of economies of scale. The infusion of such scale of additional Capex firstly, would not be possible for a 'PCO' kind of WiFi service provider and secondly, it would lead to escalation of service cost and not be a financially viable option for the WiFi service provider.

    c. Therefore, in order to fulfill the twin aims of KYC as well as ensuring affordability of service it would be prudent to ensure that **KYC being done by the payment agency suffices for any online transactions. The registration providers should be mandated to only store the information regarding the payment banks details like amount, account number, IFSC code of the bank, etc, so that the same can be provided to the LEAs as and when required.**

    d. **Registration of foreigners (Para 6 (b)).** On one hand, the process lists provisioning of OTP as a challenge, especially for the foreigners whereas later it is suggesting usage of Aadhar number for authenticating a user who register's himself with the registration service provider. Since, a foreigner would not have an aadhar card and also the fact that provisioning of visa's for India has been automated, it is suggested that **possibility of authentication of the foreign visitors through MEA's data base of visa's issued should be explored.**

    e. **Mandated Two Factor Authentication for Making Online Payments.** One of the envisaged aim for the process described in the consultation note appears to be able to provide Wi-Fi connectivity to non SIM devices. It is brought out that RBI guidelines have

mandated two factor authentication for online payments. Accordingly, the only option available for non SIM devices to be connected to a Wi-Fi hot spot is through pre paid packages.

Our Recommendations

2. In view of the foregoing, our recommendations are as follows,

   a. **For increasing affordability of WiFi services, KYC should not be duplicated beyond that of the initial payment bank.**

   b. **The registration providers should be mandated to only store the information regarding the payment banks details like amount, account number, IFSC code of the bank, etc, so that the same can be provided to the LEAs as and when required.**

   c. **Possibility of authentication of the foreign visitors through MEA's data base of visa's issued should be explored.**

Question 2. Would you like to suggest any alternate model?

Our Response

1. **Alternate Process.** As per our understanding of the process, the proposed architecture is based on the assumption that the payment portals (E-wallets / UPIs) shall be developing and provisioning the WiFi registration portal, for the users, since the subscription process (Para 15 (b) (i)) is starting with the users accessing their payment portal and browsing Wi-Fi Hot Spots to connect to. However, it is the Wi-Fi service provider who has more incentive for registering its users instead of the payment portal, therefore the **registration of the users should be at the respective captive portals of the Wi-Fi service provider instead of the payment portal.** Just as one can buy e-books on kindle, once a user is registered on the Amazon website with his / her payment details, similarly, once a user is registered at a Wi-Fi service provider's portal, he / she can be provided seamless payment and access at any wi-Fi hot spot. The advantages of such a process would be that,

   a. A user be it Indian or a foreigner can be permitted to register at the Wi-Fi service providers' captive portal and avail of any pre / post paid services through online payment only.

   b. **At the time of registration, provisioning of Visa information can be mandated for the foreigners intending to visit India.**

   c. Since the payments would be online and the WiFi service providers would be storing and processing the same for settlement of payments, the users including foreigners, would be subjected to indirect and automatic KYC for traceability purposes when required by the LEAs.

   d. **A 'PCO' kind of Wi-Fi service provider can be modeled as a franchisee of a larger WiFi service provider.** This shall provide the franchisee access to the larger WiFi service provider's software and other infrastructure for authentication, service provisioning, billing and revenue sharing.

   e. **Wi-Fi hot spot roaming agreements can be mandated amongst the larger Wi-Fi hot spot providers by directing integration of their systems to each other for authentication of users and settlement of payments.** Therefore, in case a user is registers at one Wi-Fi service provider's portal, he can avail the service at a hot spot of any other Wi-Fi service provider.

2. For Wi-Fi services to be competitive and affordable, it is necessary that the bulk rate of data services from the TSPs / ISPs are lesser than those at which they sell to other retail customers. The large Wi-Fi hot spot provider can avail preferential rates for larger data volume business from these backhaul TSPs / ISPs, thereby increasing affordability of his services. This way, even the PCO kind franchisees too would be able to reap the benefit of the bulk rates for data volumes. Depending on the financial viability of service, the Wi-Fi service providers should ideally be VNOs to the TSPs / ISPs. It is felt that for the **WiFi service providers should be mandated to become a VNO and such VNOs should be permitted multiple parenting to build on high capacity, redundant backhaul links.**

Our Recommendations

3. **In view of the foregoing, our recommendations are as follows,**

   a. **Registration of the users should be at the respective captive portals of the Wi-Fi service provider instead of the payment portal.**

   b. **WiFi service providers should be mandated to become a VNO to the TSPs / ISPs. Therefore, WiFi service providers as VNOs should be permitted multiple parenting to build on high capacity, redundant backhaul links.**

   c. **A 'PCO' kind of Wi-Fi service provider can be modeled as a franchisee of a larger WiFi service provider.**

   d. **Wi-Fi hot spot roaming agreements can be mandated amongst the larger Wi-Fi hot spot providers by directing integration of their systems to each other for authentication of users and settlement of payments.**

   e. **At the time of registration, provisioning of Visa information can be mandated for the foreigners intending to visit India.**

Question 3. 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?

Our Response

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 WiFi service providers only and only if the WiFi service provider is an overlay access provider to an ISP / TSP.

1. Provisioning of internet services is a licensed activity as per DoTs UL Access services and ISP authorisations and the respective VNO authorisations. WiFi service providers would provide an alternate access mechanism for accessing and utilizing the TSPs / ISPs bandwidth. There can be two models of selling the native data services of the ISP / TSP viz,

   a. **As a VNO.** An independent WiFi service provider can become a VNO of an ISP / TSP for reselling the data bandwidth of the ISP / TSP under its own brand name. If the WiFi service provider opts to be a VNO, he shall have to comply with all the requirements of the VNO license as spelt out in the UL VNO authorisation. The WiFi service provider and the ISP / TSP have a commercial agreement vide which the data services are provided to the VNO for reselling and the VNO deploys its own billing system. Each licensee is individually responsible for their own audits and LF obligations. Only for LEA requirements, the underlying NSO is responsible for both the licensees.

b. **As an Overlay Access Network Provider.** In this case, the ISP / TSP gets into an agreement with the WiFi service provider for extending the access to the ISP's / TSP's own data services through WiFi. The WiFi service provider has no direct obligations towards LEA requirements. However, the ISP / TSP shall have to have stringent SLAs in place with the WiFi service provider, for providing the session details as and when required by the LEAs. All license related obligations are that of the ISP / TSP only. Commercials are mutually decided between the WiFi service provider and the ISP / TSP for sharing of revenue between them. The WiFi service provider providers the usage details from its Wireless Access Controller (WAC) for billing purposes to the native ISP / TSP only. **In this case, it would be preferable that the WiFi service provider is subjected to 'light touch regulation' using 'registration' instead of 'licensing'.**

Our Recommendations

2. In view of the above, following are our recommendations,

   a. **Public Wi-Fi access providers should be permitted to resell capacity and bandwidth to retail users as a licensed VNO of an ISP / TSP.**

   b. **Only and only if the WiFi service provider is an overlay access provider to an ISP / TSP, 'light touch regulation' using 'registration' instead of 'licensing' would be preferable for the WiFi service providers.**

Question 4. What should be the regulatory guidelines on "unbundling" Wi-Fi at access and backhaul level?

Our Response

For "Unbundling" Wi-Fi at access and backhaul level it is imperative that adequate monetization of the WiFi services be permitted within the realm of security and privacy of the subscribers.

1. A WiFi hot spot creates a microcell in the cellular services ecosystem. Therefore, it has the inherent ability to accurately pin point the location of a mobile device. For the WiFi kind of service to become financially viable and commercially attractive, it is important that the WiFi providers / TSPs should be able to exploit this inherent ability of WiFi hot spot as a means of generating revenue. Given the fact that a mobile device is connected to a hot spot, it is easy for the hot spot provider to push targeted advertising to the mobile device for the consumers' consumption within the coverage area of that WiFi Hotspot. E.g. If a major retail store like BigBazaar or Shoppers Stop or any other show room in a big mall creates a free WiFi zone in its store / a restaurant for its customers, it is possible to send targeted promotional offers, though SMS, to the mobile device of the customer at that time for the benefit of the customer. Since the customer would be registered with the WiFi service provider, the exact location of the customer would be known to the WiFi service provider and hence, the same can be shared with the local retailer for sending targeted promotional offers to the connected device. For the WiFi service provider / WiFi Hot Spot provider, it is also possible to have such an arrangement in coordination with the back haul TSP.

2. The current license conditions do not permit sharing of location information of the subscriber due to privacy and security concerns thereby preventing monetization of such setups. However, a lot of solutions have been developed that enable anonimisation of the users' MDN information. Accordingly, **for popularizing and adequately monetization of the WiFi services, it is imperative that the over burdening privacy and security conditions imposed on the TSPs be relaxed and due permission be granted for sharing of**

anonimized information of the subscriber, with due permission of the subscribers only, for targeted advertising and promotional offers.

Our Recommendations

3. In view of the above, following are our recommendations, **for popularizing and adequately monetization of the WiFi services, it is imperative that the over burdening privacy and security conditions imposed on the TSPs be relaxed and due permission be granted for sharing of anonimized information of the subscriber, with due permission of the subscribers only, for targeted advertising and promotional offers.**

Question 5. 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.

Our Response

Yes, reselling of bandwidth should be allowed to venue owners such as shop keepers through Wi-Fi at premise but only as a franchise of a larger WiFi service provider.

1. It is brought out that the WiFi network architecture has 5 basic components that enable provisioning of carrier grade services, viz,

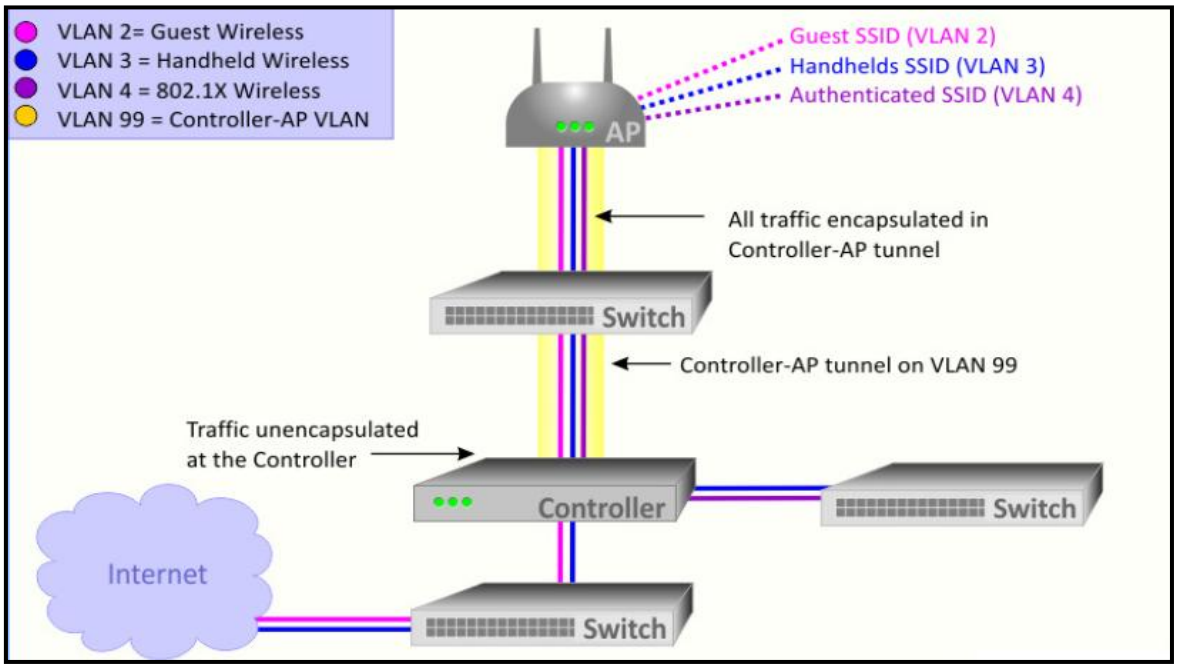

Figure : Showing the Network Architecture of WiFi network

Source : https://community.arubanetworks.com/aruba/attachments/aruba/IAP/5725/1/WLAN%20ARCHITECTURE.pdf

a. **Wireless Access Point (WAP)** – similar to BTS, this provides the access to the network to the users.

b. **Wireless Access Controller (WAC)** – similar to BSC / RNC, this controls the access channels of the AP and keeps a record of each session.

c. **Wireless Access gateway (WAG)** – Similar to the MSC / GGSN, this provides the gateway to the internet.

d. NMS / EMS.

e. BSS / OSS.

2. Since a WiFi service provider would have the responsibility of supporting the ISP / TSP for LEA requirements by providing the information about the devices connected to the WAP and the session of each device it is mandated that the WiFi service deploys all the components of the WiFi network architecture. For a standalone venue owner like a shop keepers, the Capex investment for deploying all the components of the WiFi network architecture shall make provisioning of WiFi services a financially unviable proposition. However, **if the venue owner becomes a franchisee of a larger WiFi service provider like Ozone or Quadgen then it can avail of the facilities of other components of the WiFi network architecture and would be able to fulfill its obligations towards security compliances.**

Our Recommendation

3. In view of the above it is recommended that **reselling of bandwidth should be allowed to venue owners such as shop keepers through Wi-Fi at premise but only as a franchise of a larger WiFi service provider.**

Question 6. 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?

Our Response and Recommendation

No regulatory intervention is required regarding sharing of costs and revenue across all entities in the public Wi-Fi value chain and it should be left to forbearance and individual contracting.