QuadGen Wi-Fi Operations Pvt. Ltd

Response containing written comments

In Response to

TRAI Consultation Note on

Model for Nationwide Interoperable and Scalable Public Wi-Fi Networks

9th December 2016

QuadGen Wi-Fi Operations Pvt Ltd,
#607, Brigade World Trade Center, Dr Rajkumar Road,
Malleswaram West, BANGALORE, INDIA, 560055
Tel: +91 80 3000 4076/77/78/79, URL: www.QuadGenwireless.com

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?

Comments:

- Carrier grade Wi-Fi service providers should conform to standards for centralized authentication, authorization, accounting, billing and customer support systems. These systems along with centralized EMS/NMS for Fault, Configuration, Accounting, Performance and Security(FCAPS) are considered essential elements of a global standard carrier grade Wi-Fi Network.
- The architecture proposed by the authority will lead to the evolution of yet another layer of registry providers in the subscriber authentication process. This will necessitate the Wi-Fi service provider at one level to connect to and provide a gateway to many such registry providers. This will require significant additional costs for integration with numerous registries and maintaining gateway connectivity in terms of bandwidth charges, servers etc.
- The use of these registries for authenticating every Wi-Fi user in the network will also lead to latency in the network, increase authentication time for users and may affect user experience. Any impact on user experience will directly Wi-Fi adoption and proliferation of Wi-Fi networks.
- An implicit pre-requisite is also the need for an app as a mandatory requirement for Wi-Fi service invocation at the hotspot. Wi-Fi consumers will be forced to invoke the Wi-Fi service at hotspot locations only through yet another interface of an app for Wi-Fi service. This may not be a preferred mode for Wi-Fi access for the consumer. This will be an inhibitor for Wi-Fi growth and proliferation.
- The suggested architecture does not address the provision of foreign users being able to register themselves to use Wi-Fi services. Foreign visitors may not be comfortable sharing their passport numbers on a captive portal or app, and even if they do, there is not suggested way to may authenticate these passport numbers.
- In order to have a seamless roaming across Wi-Fi networks, Wi-Fi service providers will have to implement global standards such as Hotspot 2.0, passpoint authentication and EAP- SIM based authentication. The implementation of these standards is still evolving at a global stage to provide roaming between intra country and inter country Wi-Fi service providers. Any mechanisms for seamless mobility, interoperability and authentication across mobile networks is not part of the suggested authentication architecture.

- The KYC authentication mechanisms are mandated to go through a two-factor authentication process. This requirement is considered necessary for security reasons and for the storage of Call data records/IP data records, which are part of the Lawful Intercept Mechanisms (LIM) regulatory requirements for all ISPs.
- The suggested architecture does not address accounting systems which are needed for provisioning Wi-Fi rates, data usage packs for end user consumption.

Summary:

- The suggested architecture in the consultation note may not be the ideal solution to meet the stated goals of enable widespread interoperable Wi-Fi networks and of Public Wi-Fi proliferation.
- Customers and HSSP should have the freedom of choosing and providing Wi-Fi services. Any techno-economic models through such proposed architectures should not be imposed.
- This may lead to a few dominant registry providers which may control the Wi-Fi service rollout.
- Such mandates of having a centralized registry providers might inhibit the Wi-Fi service delivery model and techno-economic feasibilities of the hotspot service provider from widespread proliferation.

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?

Comments:

- Wi-Fi services are always expected to be provided through the ISP model of relevant network architectures by the virtue of being licensed service providers.
- The Wi-Fi service provider has the obligation and needs to conform to the guidelines provided by the licensor to acquire and activate any type of subscriber, be it prepaid or postpaid Wi-Fi service.
- Any licensed Wi-Fi service provider is required maintain to standards and SLAs related to network availability, network reliability, quality of service, session security and compliance to LIM, and customer care as mandated by the licensing authority.
- It is imperative for all Wi-Fi service providers to be compliant to these standards of service quality without which Wi-Fi user experience will suffer.
- ISPs are also required to maintain IPDR/CDRs for LIM compliance and to respond to LEA requests. This requires significant investment of hardware/software and associated maintenance. This needs to be addressed and provided by any Wi-Fi service provider.

- The registration and payment mechanisms suggested in the consultation note will not obviate the above-mentioned licensing requirements for the Wi-Fi service provider.
- Small shop owners, Mall owners etc. can be signed up as franchisees and reseller partners by licensed Wi-Fi service providers. Such franchisees should be allowed to resell Wi-Fi under the license of the Wi-Fi service provider.

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

Comments:

- Wi-Fi access infrastructure equipment deployed by Wi-Fi service Providers should conform to Carrier-grade standards namely maximum availability, high reliability, and centralized maintainability for Fault, Configuration, Accounting, Performance and Security (FCAPS).
- It is also required for the WiFi Access Points and Core WiFi Controllers to conform to carrier-grade requirements with reference to global standards of RF performance, RF TX power levels, Antenna configurations, IP certification like (IP65,IP66,IP67 etc) and Cyber Security Standards etc.
- All WiFi Access equipment deployed should be mandatorily made compliant to the relevant IEEE / 3GPP / WiFi Alliance standards to ensure the best QoS to the end users for standalone WiFi access as well as Mobile Data Offload (MDO) and Hotspot 2.0 requirements
- WiFi Access Controllers, EMS/NMS and OSS/BSS systems on virtual platform based software applications should be mandated for compulsory hosting of such virtual applications on physical servers located within India WiFi Network Operations Centres (NOC).
- Centralized Authentication, authorization and accounting and billing systems along with CDR storage for LIM requests are mandatory for any Wi-Fi service provider as per regulations.
- Non-compliance to the applicable standards will result in a compromise of user experience and lead to increased consumer complaints.
- It is imperative for any licensed Wi-Fi service provider for backhaul and access to conform to global class telco grade requirements to enable rapid proliferation of Wi-Fi networks.
- Any Wi-Fi access infrastructure must conform to the above-mentioned requirements. In this current scenario, it is not recommended to unbundle the access infrastructure provider from an ISP.
- Small shop owners, Mall owners etc. can be signed up as franchisees and reseller partners by licensed Wi-Fi service providers. Such franchisees should be allowed to resell Wi-Fi under the license of the Wi-Fi service provider.

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.

Comments:

- All Wireless Access points(WAP), Wireless Access Controllers(WAC), servers, routers, switches, firewalls etc. need to be in a secure private IP network subnet, such that these network elements cannot be accessed outside this private IP network.
- The end user clients are provided user IPs from NAT system, so that the separation of IP subnets between the network elements and end user clients provides a robust security layer.
- Authorized access to any network element should be provided only for management and control purposes via a secure 128 bit IPSEC encrypted VPN tunnel.
- Wi-Fi Password encryption functionality is also to be provided by a centralized Wireless access controller so no local security breach of password is possible at the hotspot level.
- All telco grade network elements are required to be are fully compliant to cyber security norms and protected from cyber attacks with robust IP address plan backed by carrier grade firewalls at every layer.
- Communication between the WAP and the centralized WAC is encrypted with Secure Shell (SSH)V2 Tunnels
- Secure SSID based Wi-Fi access is provided using a 2 factor OTP based authentication and authorization mechanism needs to be mandated.
- Such a carrier grade network with its centralized OSS/BSS and AAA will capture all relevant call data record (CDR) data like phone number, Client MAC, assigned IP addresses, Hostpot location etc., in real time prior to authorizing use of the Wi-Fi network.
- This security layer ensures no browsing or any other client activity is possible till authentication and authorization is complete and no unauthorized client is allowed to access the Wi-Fi network.
- Wireless Client Isolation is enabled at the WAP for layer2 and layer 3 client-client isolation. This security mechanism prevents clients accessing the Wi-Fi network from connecting to each other.
- LAWFUL INTERCEPT MONITORING (LIM) compliance mandatorily followed for public Service like any 2G/3G/4G Cellular Service. Using this CDR information and DHCP logs, the system provides complete ability to trace, retrieve and respond to LAW ENFORCEMENT AGENCIES (LEA) requests specific to an IP session on the Wi-Fi network

  It is suggested that shop owners, Mall owners etc. can be signed up as franchisees and reseller partners by licensed Wi-Fi service providers. Such franchisees should be

allowed to resell Wi-Fi under the license of the Wi-Fi service provider. In this manner, the Wi-Fi service providers will provide a secure scalable infrastructure that will enable widespread Wi-Fi adoption.

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?

Comments:

It is suggested that the regulator should not encourage or suggest any such mechanisms or guidelines of sharing costs and revenues across the public Wi-fi value chain The market forces and business models should be allowed to drive the evolution of any innovative businesses and commercial arrangements between different stakeholders.