Cisco Inc response to TRAI Consultation on Nation-wide Interoperable and Scalable Public Wi-Fi Networks

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?

Limitations in TRAI proposed model
The proposed model for providing unified authentication and payment infrastructure is intended to be easy to use for users.However, it hassome limitationshighlighted below:

- In proposed model, users need to maintain separate accounts from multiple service providers and thus would require separate accounts for accessing services fromdifferent Service Providers.
- Users may not be able to use prepaid services from Wi-Fi Service providers, as the same services may not work at all hotspots provided by different service providers in absence of standard app that can enable the same. App compatibility with mobile OS/ hardware requirements may also bring in additional challenges in providing unified authentication and seamless access.
- Emergence of too many apps would make it challenging for Service Providers to have integration with numerous app providers and therefore offer services.
- The proposed model would also limit the business models that the SPs might want to use, e.g., offer free access to selected services from their hotspots, or advertising through the captive portals, as the captive portals would not be visible to the end users but would only talk to the App provider.

Wi-Fi CERTIFIED Passpoint is a better approach
Cisco recommend TRAI evaluate Wi-Fi CERTIFIED Passpoint, which provides technology for solutions that are supportive of the business model issues that TRAI are trying to solve.

As Cisco understand the Digital India vision, success will be measured by the large scale deployment of public Wi-Fi networks, providing affordable, fee-based or free access, with seamless roaming. This collection of public Wi-Fi networks would exist to complement licensed service provider networks, and potentially extend the reach of broadband to citizens who do not have broadband access today.

TRAI have correctly recognized that achievement of this desired outcome presents technology challenges, as well as business model challenges. Answering the technology questions correctly will lessen the business model challenges.

The problem of defining a unified authentication and payment infrastructure is a business model issue. But that issue can be simplified if the underlying public networks support secureand seamless roaming. The technology for secure, seamless roaming exists today. The Wi-Fi industry, through its trade association the Wi-Fi Alliance,usingthe IEEE 802.11u standard, created Wi-Fi CERTIFIED Passpoint– the trademarked name referring to technologies sometimes called “Hotspot 2.0” or “Next Generation Hotspot”. Passpoint allows a user to automatically and securely (based on WPA2- Enterprise) link to any hotspot for which it has credentials. Those credential can be provided by the owner of the hotspot or one of many other credential providers. Individual logins and individual authentication at every hotspot becomes unnecessary.

To make Passpoint effective,business arrangementsmust be struck by participating credential providers. This has proved to be the most challenging aspect of the wide deployment of Passpoint globally. In the context of India, TRAI could sponsor efforts to encourage the formation of roaming consortiums so that most Indian credential providers (and approved foreign credential providers) are available at most Passpoint hotspots across India. Where a user does not have access to appropriate credentials for a particular Passpoint hotspot, Passpoint also specifies mechanisms for On-line Signup. On-line Signup will also allow foreign travelers in India relatively easy access to Passpointhotspot services, with sign up only required at the first Passpoint hotspot that is encountered in India.

In addition, Passpoint enables (but does not require) operators to monetize the use of their network, using either pre-pay or post-pay models. And because Passpoint is secure, the end user can have confidence that any payment details will not be compromised in transmission, compared to open and unsecured Wi-Fi hot spot access. That said, there is an increasing trend for hotspot access to be free or be included as part of some other subscription in many foreign markets, and there is no reason to think this will not also eventually occur in India.

At present, the use of Passpoint remains voluntary – network operators can implement it or choose not to do so. Given the goals of Digital India, however, TRAI could decide to incent public networks to deploy Passpointhotspots in any number of ways. One method might be governmental recognition of Passpointhotspot networks, such as on governmental webpages, including tourism pages. In addition, the government might from time to time convene workshops or conferences for Passpointhotspot operators bringing in experts to brief them to new technology developments and business model opportunities.

Once a robust Passpointhotspot netwokris in place, there are a range of business models and services that are enabled by it – advertising supported connectivity, content services, specialized business services, capacity leasing, etc. But the key to the development of an ecosystem is pervasiveness of Wi-Fi, which requires capital investment, particularly for backhaul capability. That investment will be made for any number of reasons – service providers use Wi-Fi to retain subscribers, businesses use Wi-Fi to entice customers to their premises, customers themselves are willing to pay fees to access Wi-Fi, particularly if they are traveling, or governments to provide for better community access to communications .In our view, wide deployment of Wi-Fi CERTIFIED Passpointin India will increase the value of Wi-Fi and attract more investment in it.

Q2. Would you like to suggest any alternate model?

See response to Q1

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 – reselling capacity and bandwidth is possible and should be allowed. Typically, the term "resale" applies to a network provider who is reselling capacity to another provider. An example: a Wi-Fi provider, operating a Wi-Fi network at an airport, resells capacity on its Wi-Fi to a retail establishment inside the airport so that the retail establishment can in turn offer Wi-Fi using its specific SSID to its end customers visiting its store or restaurant.

Yes, light touch regulation is preferred. A simplified registration system would appear to support the government's interest in understanding who is providing services, while minimizing unnecessary burdens on these businesses for whom Wi-Fi is not their central focus.

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

No regulatory intervention is necessary unless problems emerge later. In fact, enabling maximum flexibility based on the use of Wi-Fi CERTIFIED Passpoint is the preferred choice, given the variety of networks and business models that will likely emerge.

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

As discussed in response to Q1, Wi-Fi CERTIFIED Passpoint solves the security problem. All public hot spot operators should be encouraged to offer Passpointfunctionality. For small shopkeepers who may not implementPasspoint, resale of Wi-Fi access to end customers should not be open and unprotected. At a minimum, these providers should be encouraged to use WPA2-Personal security and to create a log of who is utilizing the shop's access point. That said, the reality is that publicly accessible Wi-Fi hotspots can always be established without any security. The onus should be on the end-user when using such hotspots to be conscious that they are using an open and unsecured communication link and that personal data should not be transmitted – particularly bank information or credit card information. Acceptable Use Policies that users need to click through (often without reading them) will probably exclude any potential civil liability issues of the hotspot provider.

Government can play two roles in addition to encouraging Passpoint use. First, general computer crime and fraud related laws should be available to address any malicious activities that are criminal in nature.Those laws should be adopted and enforced. Second, government can help educate the public about the risks of using open, unsecured access.

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?

Market forces are the best method of determining what business models will work best in India. Wireless is one of the most dynamic, fast-changing sectors - from adoption rates, utilization of data, business models and technology. It would be virtually impossible for government to impose a static cost sharing and revenue sharing regime that would support the growth demanded by the Digital India goals. We believe the best approach is to rely on Wi-Fi CERTIFIED Passpoint to provide a flexible infrastructure that allows a multitude of business models that will change and refine as public Wi-Fi is deployed over time.