Nationwide Interoperable Public Wi-Fi

Creating a "PDO" Revolution for WiFi Hotspots

Arvind Kumar

ITU-TRAI International Training Program 2017

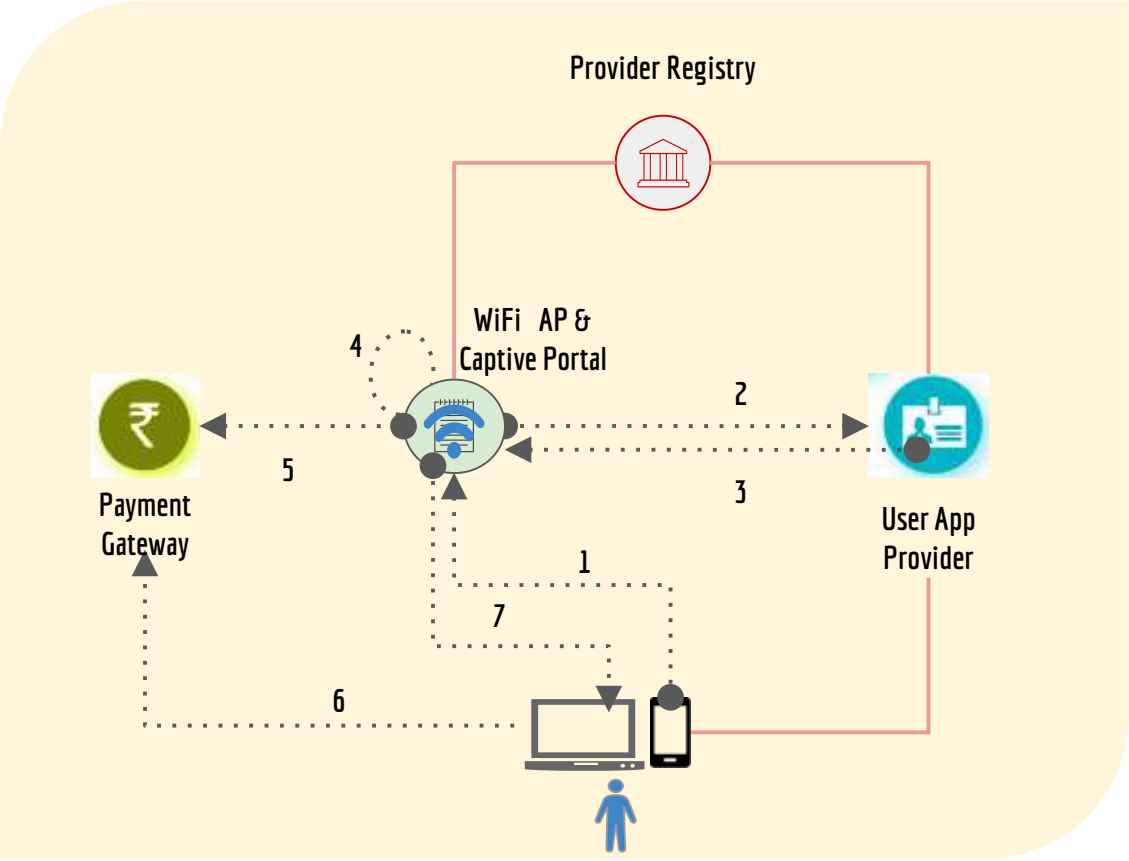
WANI Mission

- Establish an Open Architecture based WiFi Access Network Interface (WANI), such that;
  - Any entity should easily be able to setup a paid public WiFi AP. The Experience for a small entrepreneur to purchase, self-register, set-up and operate a PDO must be simple, low-touch and maintenance-free.
  - Users should be able to easily discover WANI compliant SSIDs, do one click authentication and payment, and connect one or more devices in single session.
  - Providers are unbundled to eliminate silos and closed systems. This allows multiple parties in the ecosystem to come together and enable large scale adoption.

Players in the ecosystem

- PDO/PDOA
  - Any Indian entity wanting to run one or more WANI compliant WiFi hotspots to public using either free or paid model.
- Hotspot HW/SW provider
  - Any provider who is providing necessary software, hardware, services, and/or support for PDOs/PDOAs to setup WANI compliant WiFi hotspot.
- User application provider
  - Any company providing a consumer software application and backend authentication infrastructure for users to signup, discover WANI compliant WiFi hotspots, and do single-click connect from within their app
- Central registry of providers
  - A central registry containing information about the providers

High level flow



Registration

- PDO/PDOA completes Self-Registration with Provider Registry using their public certificate (for signature validation). They also register their WiFi APs, SSIDs, and locations.
- User App provider is also registered with Provider Registry along with their authentication URL and public certificate (to validate their digital signature).
- User completes one time KYC with App Provider through their App. User App caches trusted SSIDs from Provider Registry from time to time.

Usage

1. User opens the App and browses for nearby WANI compliant SSIDs and then chooses one SSID to connect to.

2. WiFi Captive Portal of the PDO initiates user authentication with App provider backend using the token passed from the app.

3. App provider backend returns a signed user profile token back to WiFi Captive Portal.

Usage

4. WiFi Captive Portal displays data packs available with their charges. User selects desired data packs, click to confirm.

5. WiFi Captive Portal sends request for payment through their payment gateway.

6. User completes payment.

7. PDO activates <u>all device MAC-IDs</u> that were part of the signed profile and allows them to connect to the session without additional authentication.

8. User can begin browsing.

User app and signup

- Users are expected to use some software application (mobile/desktop/etc.) provided by the “App Provider” for user signup, KYC, and profile management.
- User App should provide the following key features during user signup and profile management:
  - App MUST do mobile number verification.
  - App also allows creation of mandatory “**username**” (unique username assigned to user within the app provider domain). This is shared with WiFi provider during authentication and used for audit and traceability.

User app and signup

- Features (contd…):
  - App should allow user to set up profile with additional optional attributes:
    - **Email** – user should be able to optionally set up email for getting alerts, etc.
    - **Preferred payment address** – This is ONLY for capturing preferred payment instrument

User app and signup

- Features (contd…):
  - App MUST also allow users to easily add/remove devices (MAC-ID and a name) which they want to connect to various Wi-Fi hotspots.
    - This allows the user to have more than one device to be connected to WiFi hotspots within same session.
    - This is critical to allow various devices used by user to also connect using the common app and authentication. For example, by connecting the mobile phone to the WiFi network, user may also connect his/her laptop or connected car or other future devices.
    - Optionally app may also provide “device group” profiles.

Hotspot discovery

- User App should allow users to discover nearby WANI compliant Access Points by detecting nearby SSIDs and verifying the MAC-IDs against the SSID Registry.

- In addition, optionally user App can provide location specific searches and allow users to discover “nearby” WiFi hotspots without being the WiFi range. SSID registry can be cached locally by app smartly for doing location level searches.

- App should also optionally allow users to save “favorites”, “most recent”, etc. for easy selection of regular connections.

- In addition, ideally App may also provide easy sorting and selection of access points based on the “Tag” attributes such as when AP is available, average speed, rating, etc. This allows users to select best AP within available selections.

- App must provide a mechanism for users to rate the access points and providers.

Authenticating user

- Whenever users want to connect to public WiFi hotspot using this scheme, they can open their App, browse WANI compliant Wi-Fi hotspots and click connect.
- App creates a token which needs to be passed to WiFi Captive Portal.

Benefits

- Unified architecture for user KYC and authentication
- User can use any preferred app for discovering and connecting to any WANI compliant hotspots with single-click
- Allows user to pay cash or any valid electronic payment mechanisms including upcoming UPI e-mandates
- Allows any entrepreneur to create "WiFi in a box" software/hardware stack
- Allows any SME or local entities to set up public paid WiFi hotspots using the WiFi in a box package
- Allows last mile connectivity to be bridged in India

Thank You!

arvind@gov.in