ALTICE LABS WHITEPAPER

Hotspot 2.0 and ANDSF for Smart Mobile User Connectivity

May 2014

altice labs

Altice Labs
Rua Eng. José Ferreira Pinto Basto
3810-106 Aveiro – Portugal
http://www.alticelabs.com
Tel: +351 234 403 200
Fax: +351 234 424 723

Contents

Summary

This white paper presents the base technological aspects of Hotspot 2.0 and illustrates the benefits of its combination with the Access Network Discovery and Selection Function (ANDSF) offloading framework. Both technologies empower the mobile user terminal with the capability for discovering the best access network taking into consideration different aspects such as user preferences and policies, where the provision of enhanced user experiences over the current complex network deployment environment is expected.

We present a set of different use cases showcasing the synergy capabilities achieved through the combination of these two technologies and analyse the technical requirements based on the current standards. From this work, we conclude with a future prospect regarding smart mobile user connectivity.

1. Introduction

With the data explosion in mobile access to a rich plethora of on-line services and multimedia, mobile operators are seeing their access network resources stretching thin. Evolving the network to face these challenges goes beyond normal capacity increases, due to overwhelming resource and spectrum starvation, and requires the adoption of novel deployment solutions that, more than just facing the increasing demand, actually boost connectivity scenarios. Under that aspect, offloading strategies have been considered as a prime response to these issues, leveraging the capabilities of WLAN as a complementing technology.

Raising the capability above simple uncoordinated access, the Wi-Fi alliance has been enhancing the access technology to a new level, integrating into its infrastructure the support of authentication and roaming procedures, similar to the ones we witness in mobile network accesses. This set of extended connectivity mechanisms, known as Hotspot (HS) 2.0 and standardized by the W-Fi Alliance, is actually able to tap-in to the authentication procedures of 3GPP, allowing SIM/USIM based authentication and empowering roaming scenarios. With the 3GPP's own contribution to offloading solutions, such as the Access Network Discovery and Selection Function (ANDSF), also addressing WLAN policies and mechanisms, there is an overlap between some parts of both technologies, providing ample synergy space.

The contribution of this whitepaper is twofold. On one hand, it provides a detailed description of the Hotspot 2.0 Wi-Fi Alliance standard, emphasizing its contributions as an offloading solution to mobile operators, based on its Release 2, which is under final stages in standardization. On the other, it provides a set of scenarios and considerations where Hotspot 2.0 interacts with ANDSF, in producing new optimized scenarios and solutions.

The remainder of this article is structured as follows. Hotspot 2.0 is described in Section 2, followed by the illustration of a set of specific utilization scenarios in Section 3. In Section 4, different alternative mobile operator offloading mechanisms are highlighted, presenting and focusing on Hotspot 2.0 and ANDSF integrated scenarios, and policy harmonization principles. Finally, the whitepaper concludes in Section 5.

2. Hotspot 2.0

Hotspot 2.0 enables a secure and automatic Wi-Fi access without the user intervention and thereby facilitates easier roaming between public Wi-Fi networks. Hotspot 2.0 leverages on the IEEE 802.11u standard [1], providing the discovery of supported roaming partners and the capabilities about individual Wi-Fi access networks. Such a Wi-Fi assisted technology leads to a vitalization of utilizing Wi-Fi networks, thus contributing to the offloading of mobile operator networks. In this section, we provide the basic technical aspects of Hotspot 2.0, such as its architecture, required components, and extended elements in detail, based on the standard operations and procedures specified in the Wi-Fi Alliance Hotspot 2.0 [4].

2.1 An Architecture, Components, and Requirements

The Hotspot 2.0 service architecture broadly consists of three main groups : Hotspot Operator, 3GPP/Mobile Service Provider (SP) and Mobile Device. An example of the Hotspot 2.0 architecture is shown on figure 1.

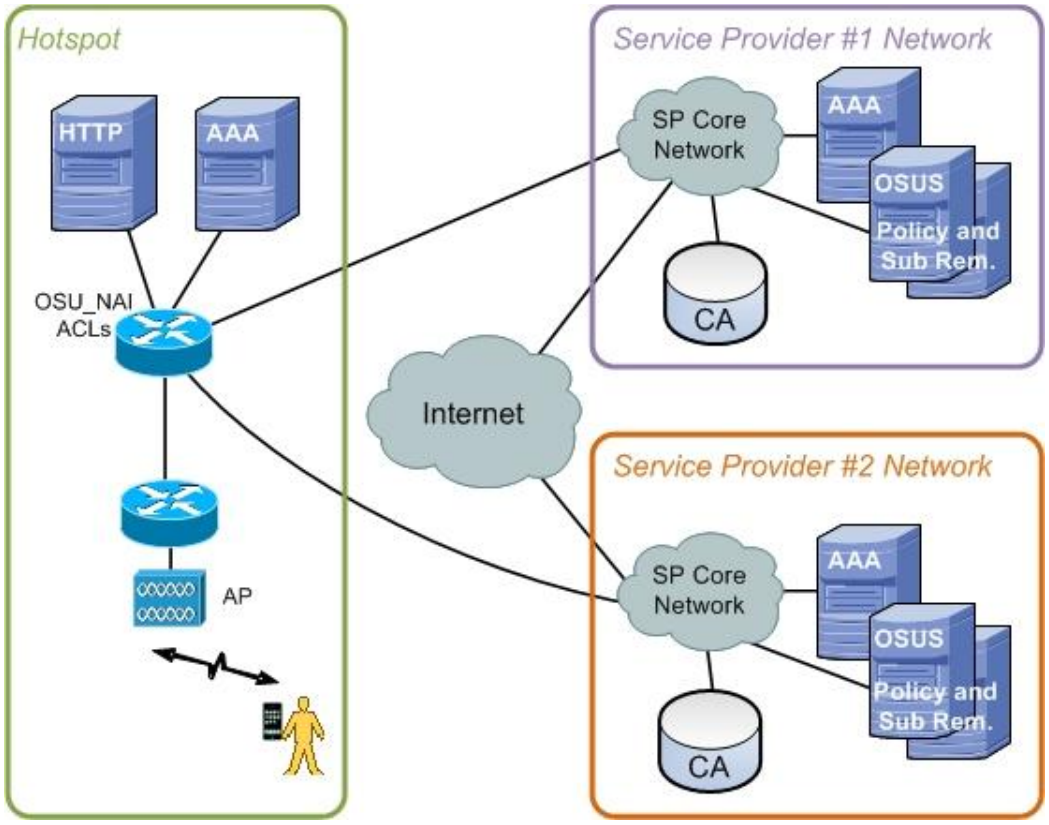

Figure 1 - Hotspot 2.0 Architecture

The following subsections detail the different components of the Hotspot 2.0 architecture, present in the figure.

2.1.1 Service Provider

The Service Provider (SP) is an entity that offers network services (from the perspective of the Hotspot Operator), which can be identified by the Network Access Identifier (NAI) Realm, 3GPP Cellular Network (in the form of a list of Public Land Mobile Network Identifiers, PLMN IDs) or Roaming Consortium Access Network Query Protocol (ANQP) elements. With the ANQP protocol, Mobile Devices can get extra information from the Hotspot APs, like the elements mentioned, before proceeding to the authentication or association processes.. More details about the ANQP elements available in Hotspot 2.0 can be found in sections 2.6 and 2.7.

The components of SPs may run over the same server (component) or different servers (components) in a distributed way. These are composed by (1) the Online Sign Up (OSU) Server, (2) the AAA Server, (3) the Policy Server and (4) the Subscription Remediation Server.

- **OSU Server**: it is the entity that handles the OSU process with the user, and is described in details in section 2.4;
- **AAA Server**: it is the entity responsible for authenticating the user credentials and grants Internet access to the user when they are valid;
- **Policy Server**: it can deliver policies to the user, guiding him through the Hotspot Discovery and Selection process. These policies are provided to the user in the form of Management Objects (MOs). More details about these policies are provided in section 2.8, specific to the Management Objects content;
- **Subscription Remediation (Sub Rem) Server**: it provides subscription parameters to the user, through the usage of Management Objects. The delivery of subscription parameters to the user is part of the OSU process and more information about it can be found in sections 2.4 and 2.8;

2.1.2 Hotspot Operator

The Hotspot Operator is the entity that is responsible for the operation of the Wi-Fi hotspot. The components and respective requirements are described as follows.

The **Access Point (AP)** composes the network termination point. When an AP indicates support for HS2.0, it shall support the following capabilities:

- WPA2-Enterprise Security protocol: In an AP that indicates support for HS2.0, TKIP and WEP shall not be used;
- 802.11u beacons: the management frames used by a Wi-Fi AP for announcing its presence and advertised information about the access network (detailed in section 2.5);
- ANQP Elements: the information elements used to discover the capabilities of the access network supporting IEEE 802.11u [1] (detailed in section 2.6);
- HS2.0 ANQP Elements: the information elements extended from ANQP elements [1], to discover the capabilities of the access network supporting Hotspot 2.0 [4] (detailed in section 2.7);
- Proxy ARP service: It serves two purposes:
  1. Enabling mobile devices to remain in power save mode for longer periods of time;
  2. Protecting against malicious behaviours of an associated mobile device.
- Hotspot procedures: According to Hotspot processes (detailed in section 2.2);
- Capability to disable P2P cross connect ([3]): a security consideration to prohibit a potential security threat by peer-to-peer (P2P) traffic. It is enabled by advertising the P2P Manageability attribute with the Cross Connection Permitted field set to 0.

The **AAA Server** of the hotspot can act as an AAA proxy to relay messages to the AAA Server of supported SPs. If it is a free public hotspot, the Hotspot AAA Server acts as an AAA Server (as described in section 2.1.1) for its own customers.

The **HTTP Server** handles the communication, such as all registration, remediation, terms and conditions data exchange, between Mobile Device and Hotspot Operator/Services Providers, executed over HTTPS.

The **Sub Rem** and **OSU Servers**, in the case of free public Wi-Fi hotspots, are required by the Wi-Fi hotspot operator and act the same way as their Service Provider counterparts (section 2.1.1).

2.1.3 Mobile Device

When a mobile device associates to a BSS and includes the HS2.0 support element in the association (or re-association) request frame, the mobile device shall support the following capabilities:

- WPA2-Enterprise: When a mobile device indicates support for HS2.0, TKIP and WEP shall not be used;
- 802.11u beacons: the management frames used by a Wi-Fi AP for announcing its presence and advertised information about the access network (detailed in section 2.5);
- ANQP Elements: the information elements used to discover the capabilities of the access network supporting IEEE 802.11u [1] (detailed in section 2.6);
- HS2.0 ANQP Elements: the information elements extended from ANQP elements [1], to discover the capabilities of the access network supporting Hotspot 2.0 [4] (detailed in section 2.7);
- Online Sign Up (section 2.4) and subscription provisioning using both the OMA-DM and SOAP-XML protocols; this includes support for the PerProviderSubscription MO (detailed in section 2.8);
- The mobile device procedures: Defined in section 2.3;
- The capability to determine time: In order to validate certificate time and date requirements.

2.2 Hotspot Procedures

Hotspot 2.0 is implemented with the intention of being used in public places and available for all type of users. Normally, this kind of scenarios increases the probability that the users may be exposed to local users, third party attackers or towards the Internet. The following Hotspot procedures have the aim to prevent these types of attacks and increase Hotspot security.

- L2 Traffic Inspection and Filtering: Prevents frames exchanged between two mobile devices from being delivered by the Wi-Fi Access Network (AN), without first being inspected and filtered in either the Hotspot operator network or the SP core network.
- Forwarding of Group-Addressed (Multicast/Broadcast) Frames: Hotspot operators can set if the forwarding of group-addressed frames is allowed. Some group-addressed frames may need to be converted to individually-addressed frames (e.g. DHCP packets).
- Proxy ARP Service: A HS2.0 AP shall support the Proxy ARP service, and when enabled (mandatory when the forwarding of group-addressed frames is enabled, optional when disabled) the AP shall maintain a Hardware Address (MAC) to Internet Address (IP) mapping for each associated station, and shall update the mapping when the Internet Address of the associated station changes.

Hotspots offering OSU shall employ the SSID configuration procedures and provide two Extended Service Sets (ESSs), namely an ESS that supports OSU and a production ESS that provides network access to the authenticated mobile device.

Hotspot operators can use the HS 2.0 OSU mechanism, which could give a simple solution for users to access free public Wi-Fi hotspot service, without relying on any service provider, by utilizing OSU subscription and integrated AAA mechanisms. In this this case, the process is as follows:

1. The user in a Free Public Hotspot initiates the OSU registration process with the Free Public Hotspot's OSU server.
2. During the registration protocol (REP) exchange, the OSU server presents the terms and conditions to the user, such as Internet access regulations depending on regions or allowed/blocked capabilities and privacy.
3. If the user accepts the terms and conditions, the OSU server issues a credential; if the user refuses, no credential is provisioned.
4. When the user/mobile device returns to the same Free Public Hotspot, the previously provisioned credentials are used to automatically connect the access..
5. If the terms and conditions change, then the user is taken though a subscription remediation process during which the new terms and conditions are presented. If the user accepts the changed terms and conditions, then a new credential is provisioned.

An example of this process is shown on the next figure.

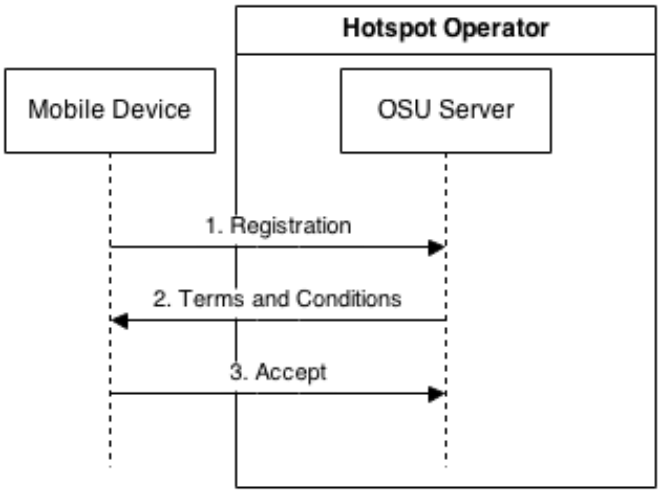

Figure 2 - Accept example of Free Public Hotspot process

More details about hotspot procedures can be found on section 5 of [4].

2.3 Mobile Device Procedures

This section describes the procedures that are applicable when a mobile device is joining or is associated to a HS2.0-compliant network. Procedures are separated by states (Discovery, Registration, Provisioning and Access), following the flowchart described in the next figure.

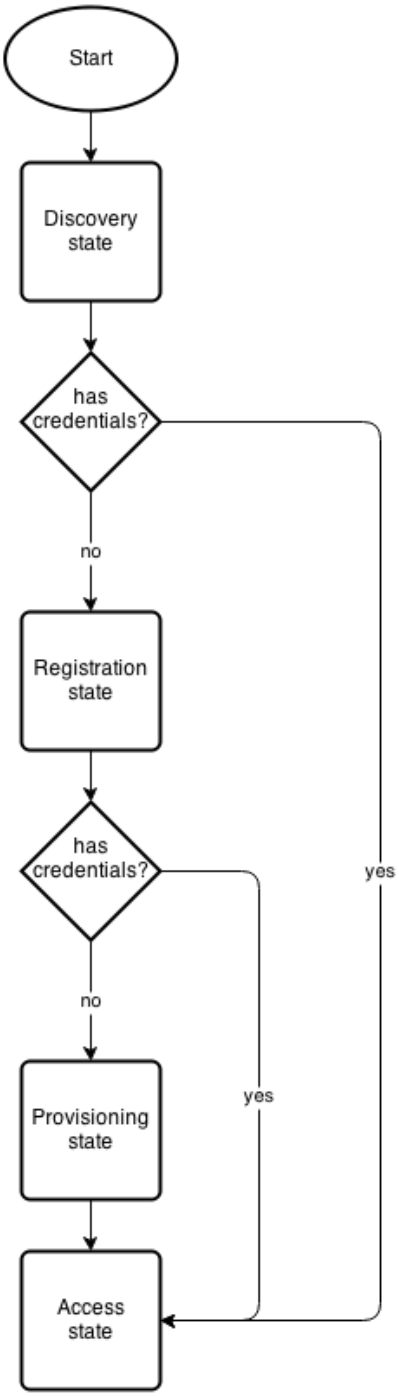

Figure 3 - Mobile Device Procedures State Machine

In the next sections, the processes in each state are described.

2.3.1 Discovery State

During the Discovery state, the mobile device scans for HS2.0 capable networks and performs an ANQP-element exchange to know the capabilities of these networks prior to the IEEE 802.11 association process. HS2.0 capable networks are identified by the presence of the HS2.0 indication in

the AP's Beacon and Probe Response frames. Also, mobile devices may use the ANQP Domain ID in the Hotspot 2.0 Indication element, as well as implementation-specific methods, to reduce the number of Generic Advertisement Service (GAS) requests in order to more efficiently use the medium.

Next, the mobile device determines if it has one or more credentials (stored in or referenced by the PerProviderSubscription MO) that it can use to access to any of the available HS2.0 networks. If multiple networks are available, including non-HS2.0 ones, the mobile device may select the network based on the overall priority or other possible heuristic, such as the signal strength, and automatically proceed to the Access state.

If HS2.0 networks are available but the user does not have the respective credentials, the mobile device may allow the user to manually select a HS2.0 network from a list of available options on a User Interface (UI) for OSU. Once the user selects a network from the OSU list, the mobile device proceeds to the Registration state.

An example selection flowchart is shown in the next figure.

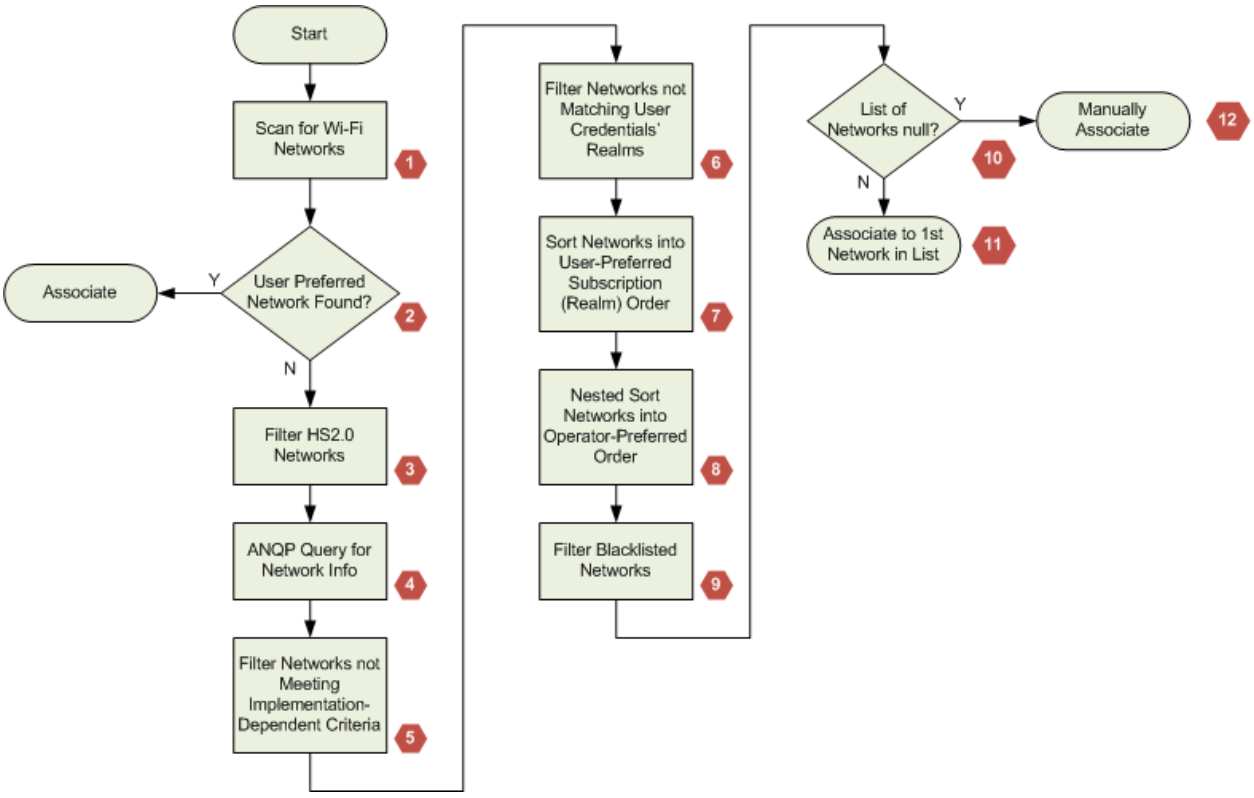

Figure 4 - Selection Procedure Steps

1. The CM (connection manager on the mobile device) kicks off the network selection process with an active or passive scan for Wi-Fi ANs;
2. The CM compares discovered networks with a list of preferred networks that the user has previously configured on the mobile device and causes the mobile device to associate with the Wi-Fi AN having the highest user preference (if a match is found);
3. If no user-preferred network is found, the list of discovered networks in step 1 is filtered from HS2.0 networks (i.e., non-HS2.0 networks are deleted from the list). Note that network selection for legacy networks is outside the scope of this example;

4. For HS2.0 networks not having a cached profile, ANQP queries are performed as needed, for example, a query for the NAI Realm and/or 3GPP Cellular Network information;
5. The discovered network list is filtered based on implementation dependent criteria. Examples include minimum RSSI level, protocols/ports blocked by hotspot firewall, PLMNs, etc.;
6. The discovered network list is filtered for realms matching the user's credentials. Wi-Fi ANs whose NAI Realm or 3GPP Cellular Network do not match user credentials (optionally including credential types) are filtered;
7. When the user has more than one Wi-Fi subscription, the remaining Wi-Fi ANs in the list are sorted by subscription preference which the user has previously configured;
8. Then the Wi-Fi ANs in the list go through a second level sort (i.e., nested sort) in which the networks are ordered by the subscription preference (step 7) and by operator preference;
9. The sorted list is then filtered for blacklisted networks;
10. If the filtered and sorted list of networks has one or more remaining networks:
    a. Then, the CM causes the mobile device to associate to the first entry (highest sorted network) in the list;
    b. Else, the CM can optionally request the user to decide whether to associate with a Wi-Fi AN.

2.3.2 Registration State

The Registration state is entered after the mobile device has associated to an OSU ESS to perform online sign-up for an account with a service provider. If the mobile device already has credentials for the current HS2.0 network, the registration state is not entered and the mobile device proceeds to the Access state.

During the OSU procedure, the mobile device sends the information such as contact information and payment method to the OSU server, as required by the SP to obtain an account. The mobile device could provide this data in an automated manner or the user could manually enter the information during the OSU process. Credentials and related metadata provisioned in the next state (Provisioning state) are bound to this account.

2.3.3 Provisioning State

The Provisioning state is entered after the mobile device and the OSU server have exited the Registration state.

The following actions occur in the Provisioning state:

- Installing the trust anchor CA certificate(s) on the mobile device,used to validate the SP's AAA server certificate, the Subscription Remediation server certificate and the Policy server certificate received during the authentication process.
- Installing an EAP-TLS (x.509v3) client certificate on the mobile device used for access to HS2.0 networks (if required). For the support of other credential types in the mobile device, installing the security mechanism fitting to the relevant EAP method is required.

- Installing the PerProviderSubscription MO on the mobile device with credentials or credential metadata, WLAN security settings and other metadata for access to HS2.0 networks. Note that the PerProviderSubscription MO can contain a username/password credential.

Some operators may have other methods of provisioning policy (e.g., re-distribution of SIM cards) that are out of scope of the specification. In this case, the Policy node within the PerProviderSubscription MO is not present. Once the provisioning process is successfully completed, the mobile device disassociates from the OSU ESS, exits the Provisioning state and proceeds directly to the Access state.

2.3.4 Access State

The Access state is entered when the mobile device has associated to a network for which it has login credentials and WLAN security settings and has successfully authenticated to that network. For HS2.0 networks, these settings were previously configured on the mobile device, either in the Provisioning state or via other means.

In the Access state, the mobile device mutually authenticates with the SP's AAA server using one of the EAP methods described in Table 1.

Table 1 - EAP Method per Credential Type (from HS2.0 Specification)

Credential Type	EAP Method
Certificate	EAP-TLS
SIM/USIM	EAP-SIM , EAP-AKA, EAP-AKA'
Username/Password (with server side certificates)	EAP-TTLS with MSCHAPv2

If the authentication with the AAA server is successful, the mobile device receives full access to the Wi-Fi hotspot network.

If the user subscription/policy expires (more details about expiration parameters in section 2.8) during the Access state, Mobile Device should return to the Registration state to update them, or even select other Hotspot.

A mobile device may fail to successfully authenticate/associate to a Hotspot 2.0 AP. Failure may be due to a variety of reasons, however, authentication/association failure does not necessarily mean there is a problem with a credential or subscription, the credential may still be valid with other APs. Therefore, in the both cases, the mobile device should not disable a credential from being used with other BSSs and, in case of authentication failure, the mobile device shall not attempt more than 10 consecutive authentications that result in authentication failures at the same ESS using a given credential within a 10-minute interval. The authentication process may restart after the expiration of the 10-minute time interval.

2.4 Online Sign Up (OSU)

Online Sign Up (OSU) is a process to obtain credentials from an operator/service provider. This feature gives a simple and clear way of providing end user device configuration provisioning, resolving a difficulty in Hotspot 2.0 release 1 that is focused on network discovery and selection.

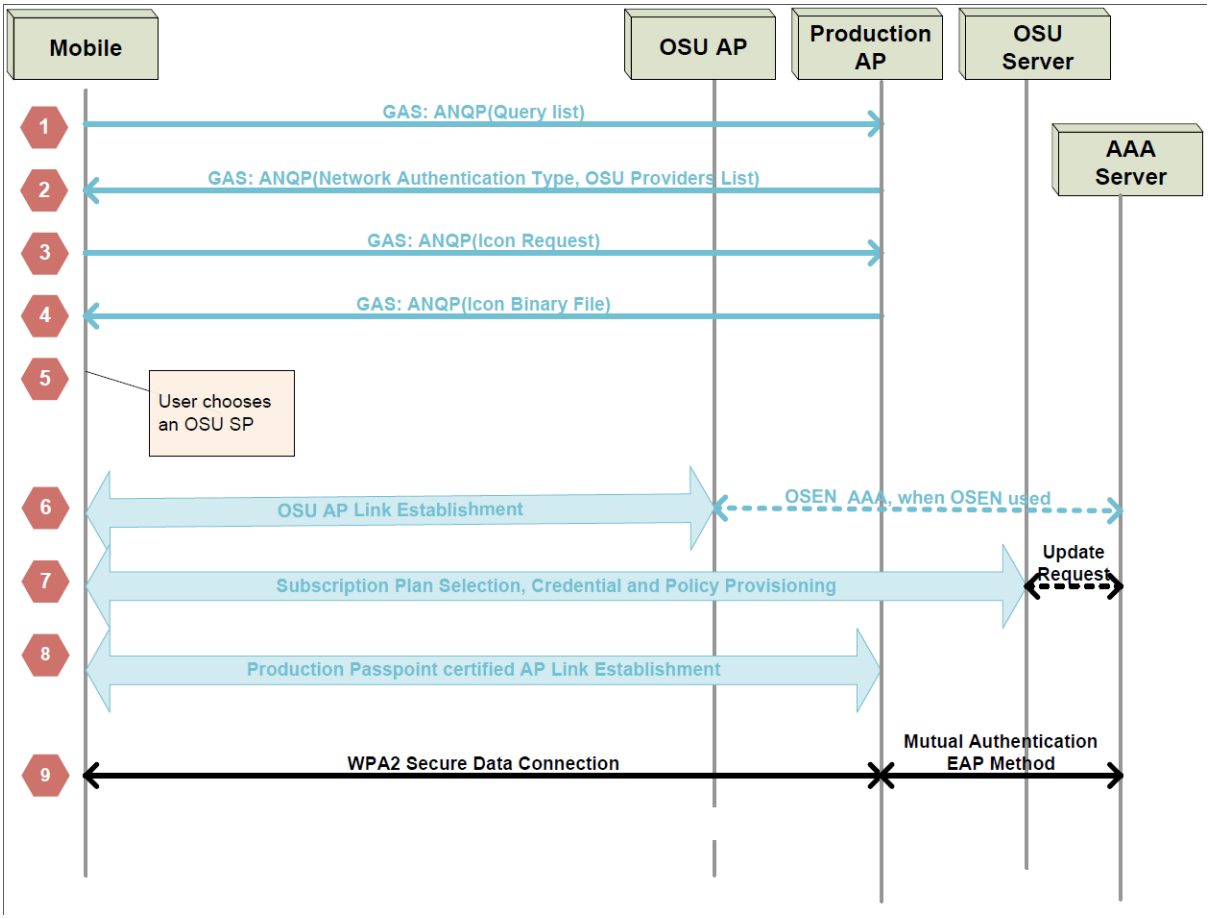

Figure 5 - OSU Signalling Flow

The OSU signalling flow presented in the previous figure, is composed by the following steps:

1. The mobile device issues an ANQP Query for the Network Authentication Type and OSU Provider information;
2. The AP returns the Network Authentication Type and OSU Providers List elements to the mobile device. If the Network Authentication Type message indicates that OSU is available, then the OSU Providers List element contains the OSU SSID and at least one online sign-up provider.
3. The mobile device may request an OSU Provider Icon of the desired size in pixels using the Icon Request HS2.0 ANQP-element. Note that in this example exchange, an icon is requested by the client device. Also, the request of the icon is optional.
4. If an icon was requested, the AP returns the Icon Binary File for the requested icon. If the OSU Providers List element contains more than one OSU provider, steps 3 and 4 can be repeated for each provider.

5. The mobile device displays on its UI a list of available OSU provider icon(s) and/or friendly name(s). If the user selects an icon and/or friendly name, indicating that online sign up for a subscription is desired, the mobile device continues with Step 6.
6. The client device connects to the user-selected OSU ESS.
7. The user provides the information needed by the SP to sign up for a subscription. Credentials (certificate, SIM or username/password) and optionally network-selection policy are provisioned on the mobile device. When credentials are provisioned, the OSU server sends an update request to the AAA Server with the mobile device's provisioned credential using a mechanism which is outside the scope of the specification.
8. The mobile device disassociates from the OSU ESS and associates to an AP in the production ESS using the newly provisioned credentials.
9. The mobile device and AP establish a WPA2-Enterprise security association and the user is granted full access privileges according to their subscription.

2.5 Beacon Elements

In 802.11u, many new elements were added to the beacon frames. For Hotspot 2.0 AP, the elements required are the following:

- Interworking element (Venue Info and HESSID fields must be included): This element provides the following information about the interworking service capabilities:
  - Access Network Type: Is set by the AP to advertise its access network type in the beacons. Can be used also to indicate the desired access network type, e.g. a private network or chargeable public network in an active scan;
  - Indication if connection to the Internet is available;
  - Indication if (unauthenticated) emergency services are reachable;
  - Venue Info (optional in 802.11u, required by HS2.0): Composed by Venue Group and Venue Type providing extra information about the hotspot context (e.g. Business, Educational, Residential, etc.) and building description (e.g. Stadium, Library, Museum, Bar, etc.) respectively;
  - HESSID (optional in 802.11u, required by HS2.0): Identifier for a homogeneous ESS. It is a globally unique identifier that, in conjunction with the SSID, may be used to provide network identification for a Subscription Service Provider Network (SSPN) (e.g. 02:03:04:05:06:07).
  - Roaming Consortium element: Identify the roaming consortium and/or Subscription Service Provider (SSP) whose security credentials can be used to authenticate with the AP (e.g. 2233445566).
- BSS Load element: provides information about population and traffic levels in the BSS (e.g. stations count, channel utilization and available capacity).
- Country information element: two-digit ISO 3166-1 country code shall be set to the value for the country in which the hotspot is located and the Country information element shall be configured to be included in Beacon and Probe response frames unless prohibited by regulatory rules or the hotspot's location is unknown (e.g., the hotspot is on an airplane).

More details about all these elements can be found in [1].

2.6 ANQP Elements

ANQP allows Mobile Devices to get extra information from Wi-Fi AP's without the need of any association or authentication. With ANQP, Mobile Devices can get more details about the Hotspots that could help in the selection process when Beacons information isn't enough.

The following sub-sections describe the ANQP Elements (defined by IEEE) that are required for Hotspot 2.0 (more details of each element can be found in [1]).

2.6.1 Venue Name

The Venue Name ANQP-element provides zero or more venue names associated with the BSS. The Venue Name ANQP-element may be used to provide additional metadata on the BSS. For example, the information may be used to assist a user in selecting the appropriate BSS with which to associate (e.g. "Midtown Shopping Center"). Zero or more Venue Name fields may be included in the same or different languages.

2.6.2 Network Authentication type

The Network Authentication Type ANQP-element provides a list of authentication types supported. These authentication types could be acceptance of terms and conditions, on-line enrolment (OSU), http/https redirection and/or DNS redirection.

2.6.3 Roaming Consortium

The Roaming Consortium ANQP-element provides a list of information about the Roaming Consortium and/or SSPs whose networks are accessible via the AP. Each Roaming Consortium is identified by an OI (Organization Identifier, e.g. 0x0050C24A4,)

2.6.4 IP Address Type Availability

The IP Address Type Availability ANQP-element provides the information about the availability of IP address type, i.e. IPv4 or IPv6 that could be allocated to the Mobile Device after successful association.

2.6.5 NAI Realm

The NAI Realm ANQP-element provides a list of network access identifier (NAI) realms corresponding to SSPs or other entities whose networks or services are accessible via the AP. Each NAI realm may optionally include a list of one or more EAP Method subfields used for authentication (e.g. example.org [EAP-SIM, EAP-TLS]).

2.6.6 3GPP Cellular Network

The 3GPP Cellular Network ANQP-element contains cellular information, such as network advertisement information, e.g. mobile network codes (MNC) and mobile country codes (MCC) to assist a Mobile Device in selecting an AP to access 3GPP networks.

2.6.7 Domain Name

The Domain Name ANQP-element provides a list of one or more domain names of the entity operating the IEEE 802.11 access network (Hotspot Operator) (e.g. example.com or another.example.com.

2.7 HS2.0 ANQP Elements

The following sub-sections describe the extended Hotspot 2.0 ANQP Elements (defined by the Wi-Fi Alliance), providing additional functionalities to IEEE 802.11 ANQP-elements supporting HS2.0 features. These elements are formatted as defined by the ANQP vendor-specific element (more details of each element can be found in section 4 of [4]).

2.7.1 HS Query List

The HS Query list provides a list of identifiers of HS2.0 ANQP-elements for which the requesting mobile device is querying in a HS ANQP Query. The HS Query List shall be used in a GAS Query Request to request HS2.0 ANQP-elements. Both the ANQP Query List and the HS2.0 Query List can be included in single GAS Query Request.

2.7.2 HS Capability List

The HS Capability list provides a list of information/capabilities that has been configured on an AP. The HS Capability list element is returned in response to a GAS Query Request.

2.7.3 Operator Friendly Name

The Operator Friendly Name element provides zero or more operator names for the Hotspot Operator. If more than one operator names are included, they shall represent the same operator name in different human languages.

2.7.4 WAN Metrics

The WAN Metrics element provides information about the WAN link connecting an IEEE 802.11 AN and the Internet. The main information that this element provides is the following:

- Link status (up, down or in test state): the element used to reflect the status of the WAN link;
- At Capacity: the element used whether the WAN link is at capacity and no additional mobile devices will be allowed to associate to the AP;
- Current downlink/uplink speed: the element used to represent the estimated WAN Backhaul link for current downlink/uplink speed in kilobits per second;
- Downlink/uplink load: the element used to represent current percentage loading of the downlink/uplink connection, as measured over an interval the duration of which is reported in Load Measurement Duration;
- LMD (Load Measurement Duration): the duration over which the downlink/uplink load has been measured.

2.7.5 Connection Capability

The Connection Capability facilitates protocol filtering, allowing or restricting traffic on some protocols and ports. For example, a firewall on upstream to the access network may allow communication on certain IP protocols and ports, while blocking communication on others.

2.7.6 NAI Home Realm Query

The NAI Home Realm Query element is used by a requesting mobile device to determine if the NAI realms for which it has security credentials are realms corresponding to SPs, or other entities whose networks or services are accessible via the BSS. The requesting mobile device includes in the NAI Home Realm Query only the NAI Home Realm Name(s) for which it has credentials. In response to the NAI Home Realm Query, a responding AP returns a NAI Realm ANQP-element.

2.7.7 Operating Class Indication (optional)

The Operating Class Indication element provides information on the groups of channels in the frequency band(s) the Wi-Fi AN is using. This element reports the operating classes of APs in the same ESS as the AP transmitting this element. A mobile device supporting more than one frequency band (e.g., 2.4GHz and 5GHz) may use this element for BSS selection purposes.

2.7.8 OSU Providers List

The OSU Providers List element provides information for one or more entities offering Online Sign Up service. For each OSU provider, the following information is provided: the friendly name (in one or more human languages), the NAI used to authenticate to the OSU ESS if configured for OSU Server-Only Authenticated L2 Encryption Network (OSEN) that is used for OSU access only by considering the operators have existing hotspot deployments with an open SSID and captive portal for authentication, the Icon(s) and the URI of the OSU Server.

2.7.9 Icon Request

The Icon Request element provides a filename for which a mobile device is requesting download. The Icon Filename is one of the filenames included in the OSU Providers List element.

2.7.10 Icon Binary File

The Icon Binary File element provides the binary contents of an OSU Provider icon. The Icon Binary File HS2.0 ANQP-element is provided in response to an Icon Request ANQP-element.

2.8 HS2.0 Management Objects (MO)

The Hotspot 2.0 management objects (MO) are composed by the main node (PerProviderSubscription) that contains the information about policies, subscription and credentials provided by a Service Provider. Mobile devices may have multiple independent PerProviderSubscription nodes, one per each Service Provider.

2.8.1 PerProviderSubscription

This node is the root node of the Hotspot 2.0 management objects tree and is used for the Service Providers delivery policies, subscription and credential parameters to the mobile devices. The direct sub-nodes of PerPrividerSubscrition node are described in the following sections. For more details about Hotspot 2.0 Management Objects, see section 9 of [4].

The full tree specification is shown in the next two figures.

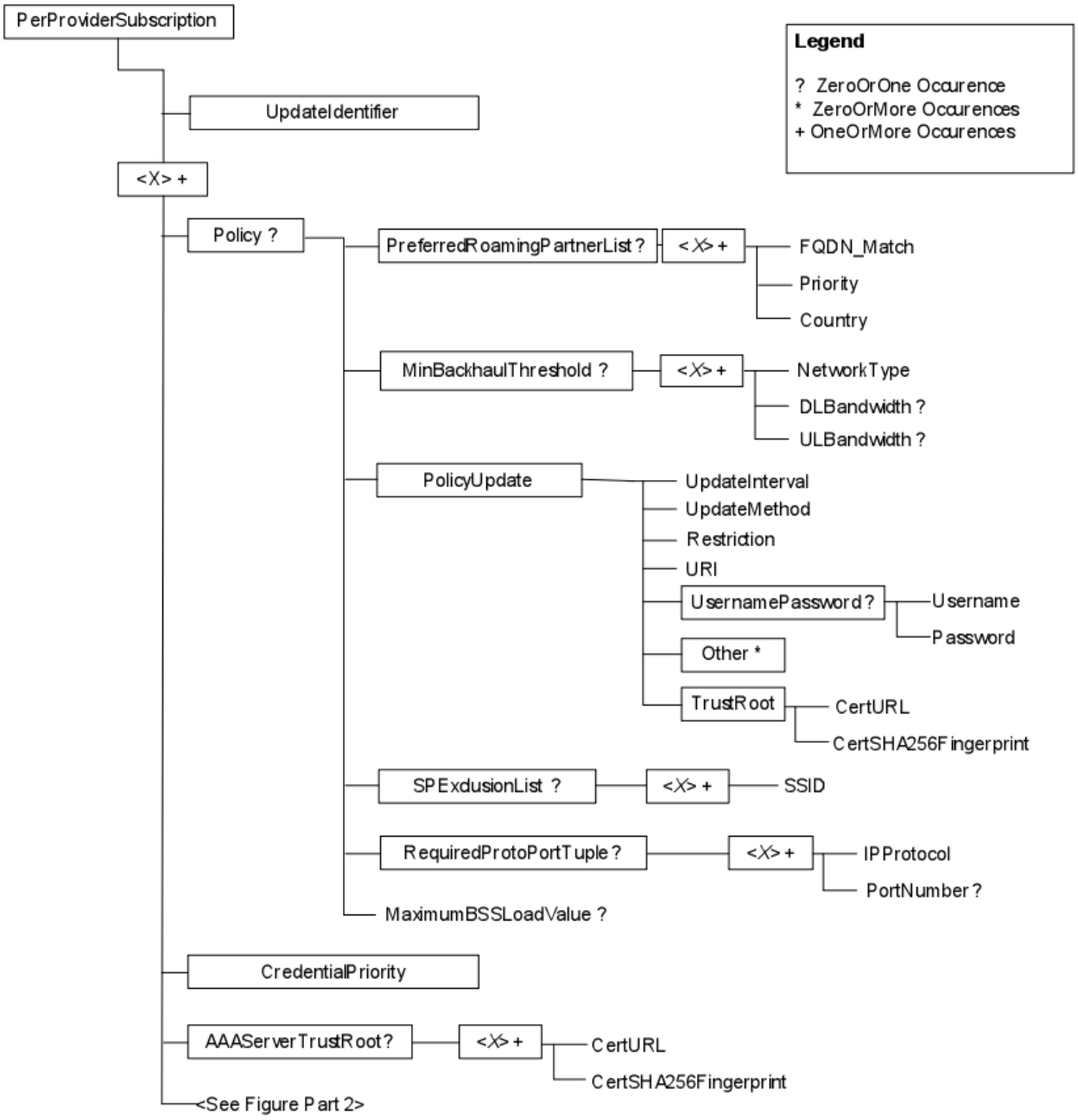

Figure 6 - PerProviderSubscription MO Tree (Part 1) from [4]

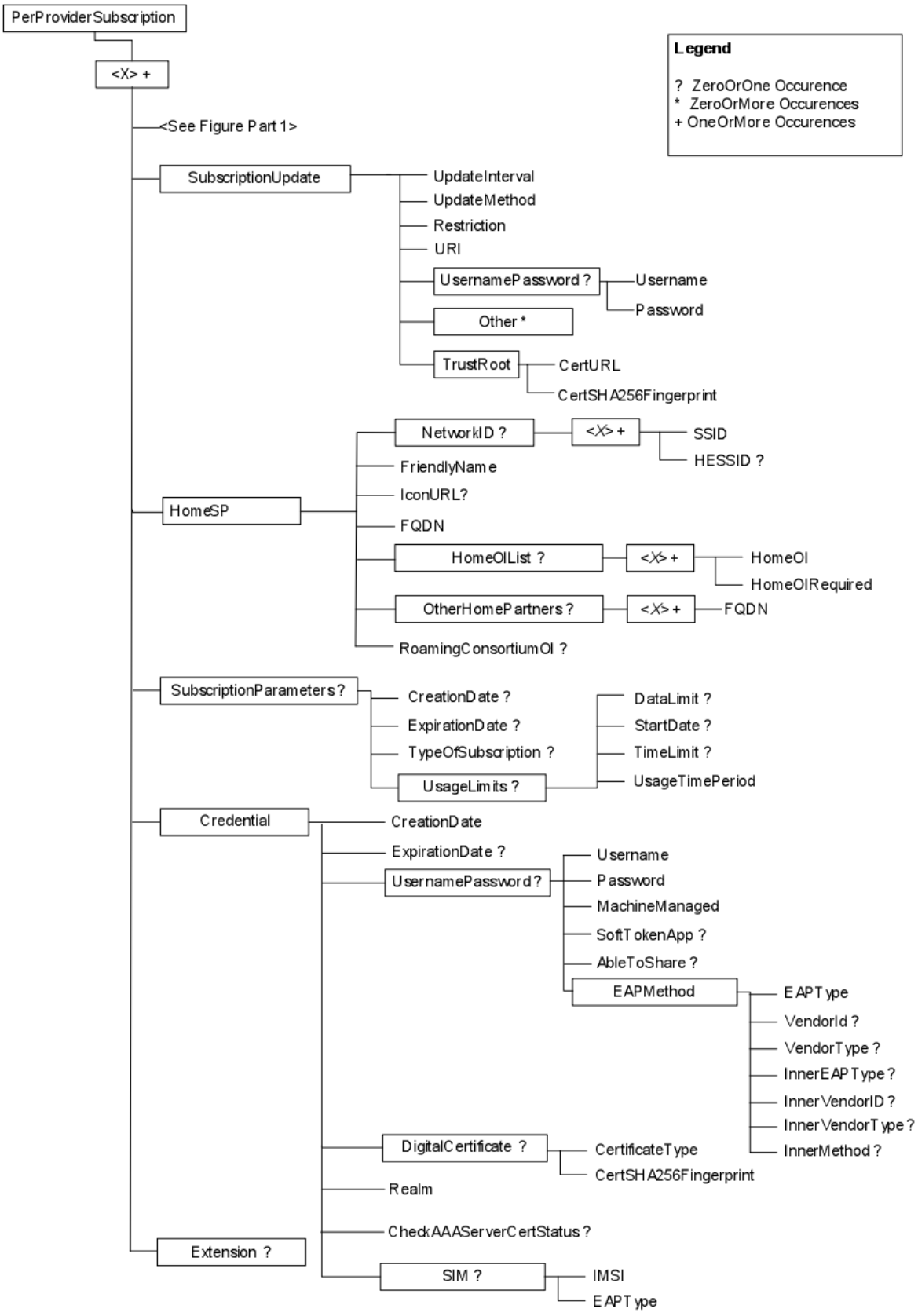

Figure 7 - PerProviderSubscription MO Tree (Part 2) from [4]

2.8.1.1 UpdateIdentifier

This node specifies the Update Identifier for the PerProviderSubscription MO. The UpdateIdentifier is an unsigned, 16-bit integer set by a Subscription Server. Subscription servers should change the value of the UpdateIdentifier every time any node in the PerProviderSubscription MO is added, deleted or modified. The default value of this leaf node is zero, meaning un-provisioned values in the MO.

2.8.1.2 Policy

This node contains the policies provided by the Service Provider for helping mobile devices on hotspot selection.

In this node, Services Providers can specify policies using the following child nodes:

- PreferredRoamingPartnerList: Allows the user to identify priorities among the roaming partners. Any roaming partner not included in this list has a default priority.
- MinBackhaulThreshold: Specifies the minimum uplink bandwidth, downlink bandwidth or both for the hotspot selection. The available bandwidth of an Hotspot can be measured by SPEED * (1 – LOAD / 255), where the SPEED and LOAD parameters are obtained from the HS2.0 ANQP WAN Metrics element (section 2.7.4) at the hotspot
- PolicyUpdate: Indicates when and how the mobile device should update these policies.
- SPExclusionList: Contains the SP exclusion list, which is a list of SSIDs that the mobile device shall not autonomously select. However the user may manually select such a network.
- RequiredProtoPortTuple: Indicates IP protocol and port number required by the SP for the purpose of network security and management, which must be present in the HS2.0 ANQP Connection Capability element (section 2.7.5).
- MaximumBSSLoadValue: Specifies the maximum acceptable BSS Load for the hotspot selection. The BSS Load can be obtained from the hotspot beacons (section 2.5) and if the mobile device cannot find an AP with channel utilization less than the defined MaximumBSSLoadValue, or if BSSLoad is not available, this policy is ignored.

2.8.1.3 CredentialPriority

This node indicates the priority of the credential, when multiple credentials are included in a single PerProviderSubscription MO instance.

2.8.1.4 AAAServerTrustRoot

This node provides the HTTPS URL at which the mobile device can retrieve AAA Server trust root(s) and the respective SHA-256 fingerprint(s). This trust root is used by the mobile device to validate the AAA Server's identity when performing EAP authentication.

2.8.1.5 SubscriptionUpdate

This node identifies the subscription server and when the user should update the subscription parameters.

2.8.1.6 HomeSP

This node provides information about the Home SP for this subscription like SSID/HSSID, Friendly Name, IconURL, FQDN, Roaming Consortium, Organizational Identifiers and Partners List.

2.8.1.7 SubscriptionParameters

This node contains the user subscription information, with the following parameters:

- Creation date: Date and time (UTC) that the PerProviderSubscription MO was initially provisioned to the mobile device;
- Expiration data: Date and time (UTC) that the subscription will expire.
- Type of subscription: Specifies the type of subscription associated with the account. Subscription types are defined by the Home SP (example values are "Gold", "Silver" and "Bronze").
- Usage limits: Specifies usage limits of this subscription by:
  - Data limit;
  - Start date;
  - Time limit;
  - Time period;

2.8.1.8 Credential

This node provides the credentials of this subscription to the user get access to the hotspot network. The Subscription Server shall ensure that exactly one of the EAP methods ("UsernamePassword", "DigitalCertificate" or "SIM") is used.

2.8.1.9 Extension

This node is used to include additional information that is not present in the PerProviderSubscription MO specification.

2.9 Technical example

This section provides a generic technical example of Hotspot 2.0 utilization. The first stage of the mobile device under the Hotspot 2.0 scope is the discovery process where the mobile device listens for the beacons of the AP's in the area and selects only the AP's with Hotspot 2.0 support. With the information obtained from the beacons, the mobile device can already exclude some Hotspots using the Roaming Consortium or BSS load fields (section 2.5). After that, mobile devices can retrieve more information from the Hotspot AP's using the ANQP protocol to get the native ANQP elements (section 2.6) or the Hotspot 2.0 extended elements (section 2.7). The mobile device can use this information to further filter the Hotspot list, like described in the section 2.3.1, and after selecting a Hotspot, the mobile device connects to the OSU ESS (section 2.2.4) to get credentials from OSU, or connects directly to the production ESS if already has valid credentials.

The next diagram describes the flow of this Hotspot connection process, with each step detailed in the following points:

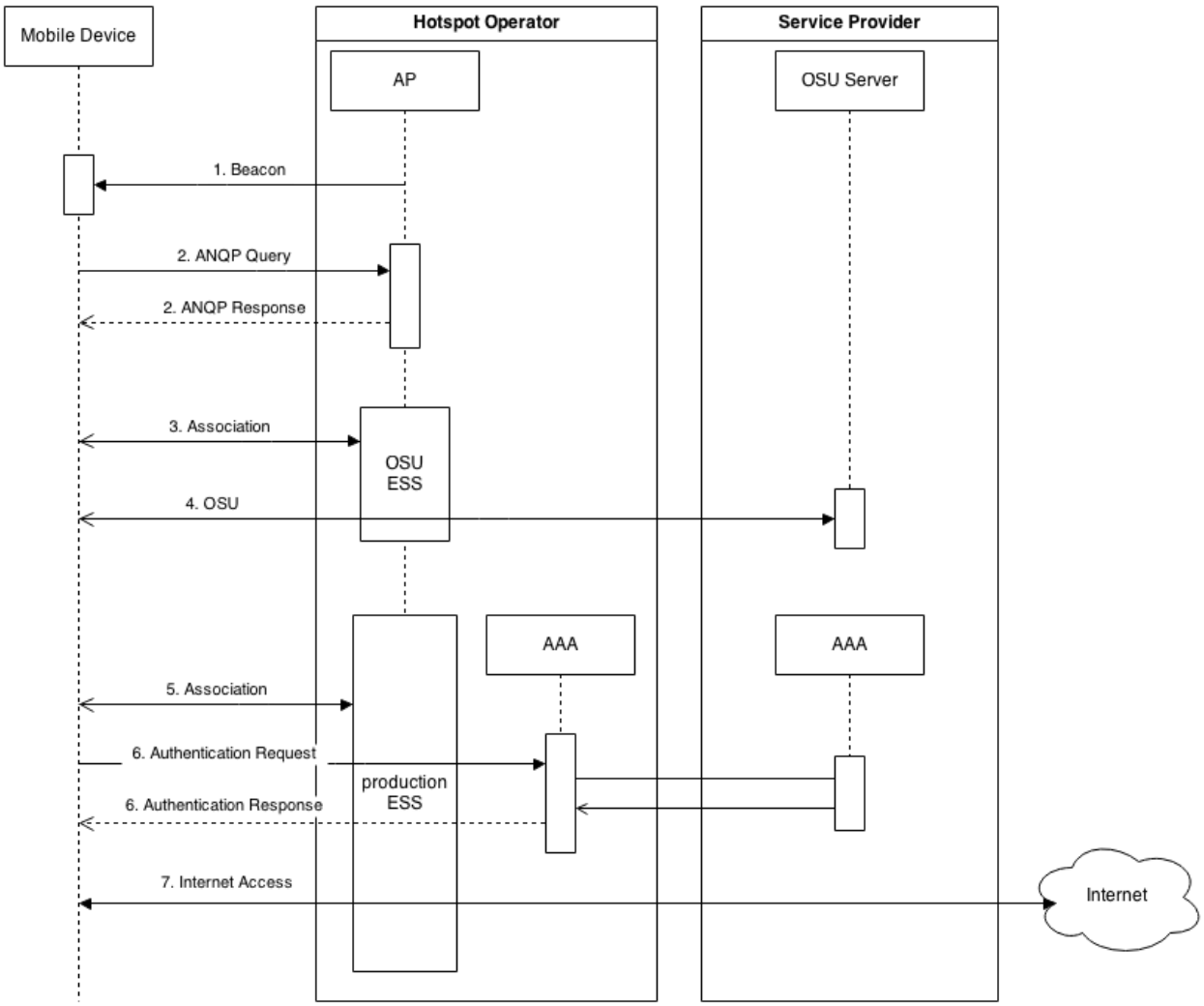

Figure 8 - Example of Hotspot 2.0 Connection Flow

1. Mobile device receives the beacons from Hotspot AP's in the area;
2. After excluding some AP's, and if the Mobile Device still has multiple choices, it tries to get more information from AP's through an ANQP Query procedure, i.e. Connection Capability, WAN Metrics, etc.;
3. If the Mobile Device does not have credentials for the selected Hotspot, it associates with OSU ESS to get them from the Online Sign Up process. Else it passes directly to step 5;
4. The Mobile Device gets credentials from the Service Provider through Online Sign Up process (see section 2.4);
5. The Mobile Device associates with production ESS;
6. The Mobile Device performs the authentication with credentials obtained from the OSU process, following 3GPP AAA procedure specified in TS 24.234.
7. If the authentication process was successful (step 6), Mobile Devices gets access to the Internet (or any other target network).

3. Hotspot 2.0 Use Cases

In this section, we show a selection of Hotspot 2.0 use cases (section 3.1) and an example how mobile devices get access to the Internet through Hotspot 2.0 (section 3.2), with message exchanges and procedures.

3.1 Scenario Examples

The following sections describe two scenarios, based on the Wi-Fi Alliance Hotspot 2.0 standard, where the usage of Hotspot 2.0 can directly be applied.

3.1.1 Airport Scenario

For travellers waiting for their connecting flights in an airport, with the Hotspot 2.0 service, users can access the Internet. In this case, users can pay for this access through the OSU process of the Hotspot 2.0 and continue having Internet access with priority on the user's preferred list in another airport as long as a Hotspot 2.0 supported by the same Service Provider is available and the user subscription is not expired. In another way, with Hotspot 2.0, it is possible to buy access to the Internet and use it in many different countries/airports under the roaming consortium where the user is leveraging on.

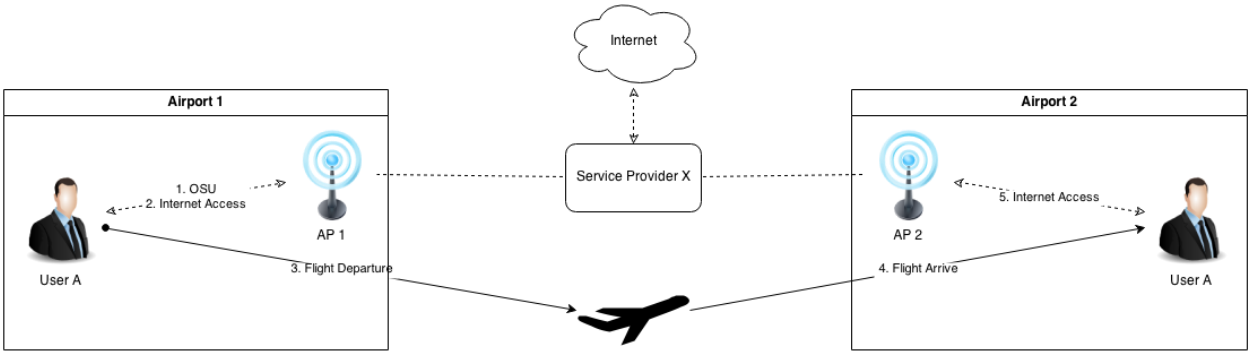

Figure 9 - Airport scenario example

3.1.2 Shopping Scenario

In shopping centres, there are many Wi-Fi APs with different SSID which make the network selection process complex. Hotspot 2.0 can help to provide an easier Internet access to their customers. In this scenario, mobile devices can automatically search for a Hotspot 2.0 with their SIM credentials to select an available Wi-Fi connection. Users can have better Wi-Fi Internet access without their manual intervention, based on the obtained information through ANQP and HS2.0 query/response.

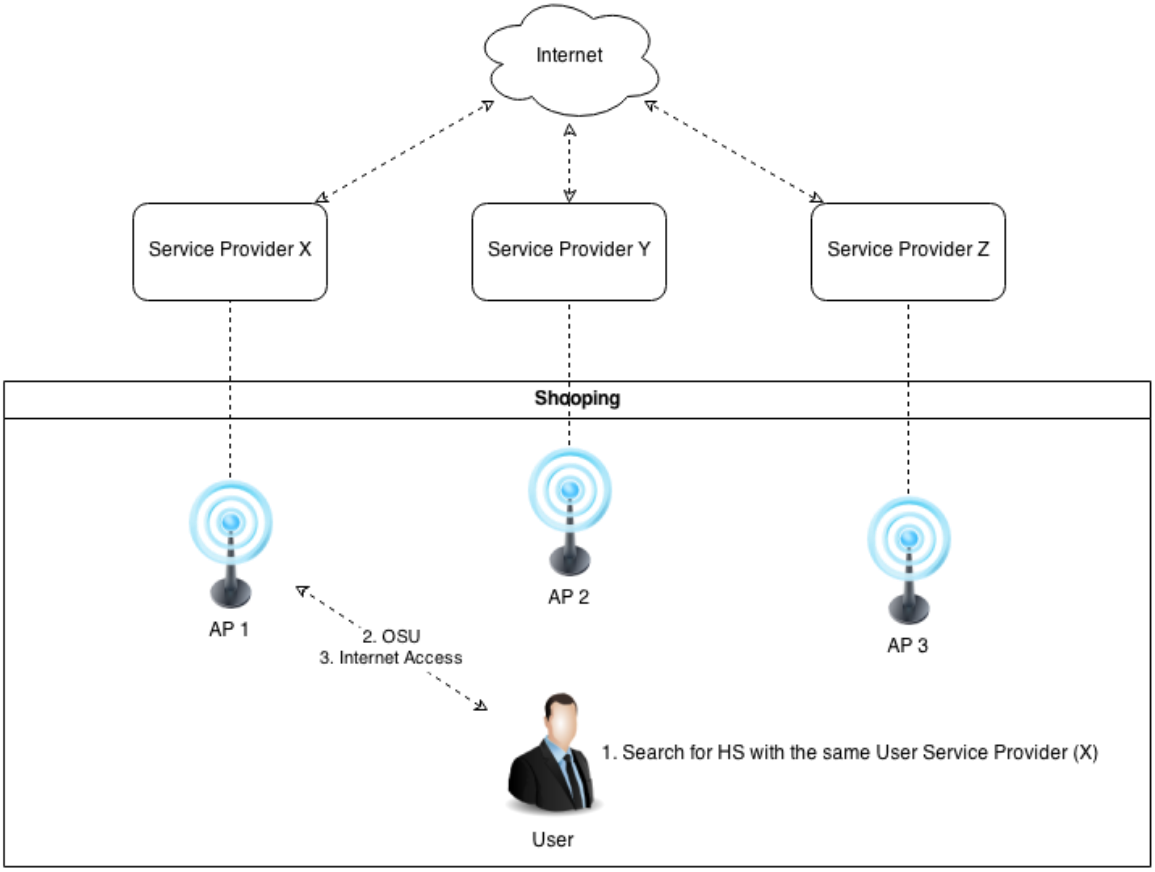

Figure 10 - Shopping scenario example

4. A combination of Hotspot 2.0 and ANDSF

Access Network Discovery and Selection Function (ANDSF) is a 3GPP cellular standard technology that provides a list of access networks and policies, based on different aspects, such as the current user location. Looking at the supported features of the two technologies – ANDSF and Hotspot 2.0, they have complementary aspects that can fill up individual shortcomings, thus their combination is expected to be a stronger enabler, highly enhancing the user experience and inducing more users towards the Wi-Fi networks. Therefore, in this section, we first describe ANDSF concisely and analyse combined ANDSF and HS2.0 use cases representing the synergy effects. In addition, we also provide guidelines towards the harmonization of a joint policy behaviour between both technologies.

4.1 4.1 ANDSF

The ANDSF is standardised by the 3GPP in TS 23.402 [6], as a network function in the Evolved Packet Core, capable of being queried by a mobile terminal using an OMA-DM based interface, named S14, standardised in TS 24.302 [7]. Through it, a client counterpart located in the mobile terminal is able to query the ANDSF about Access Network Discovery information, Inter-System Mobility and Inter-System Routing policies. The first one allows the terminal to collect information about available access networks belonging to specific geographical areas, considering 3GPP, 3GPP2, WiMAX, or WLAN technologies, among others. The Inter-System Mobility Policy (ISMP) allows the terminal to obtain information about link selection according to a specific area, time of the day and priority. Finally, the Inter-System Routing Policy (ISRP) goes one step further and allows for traffic distribution based on IP flows, or services.

The information exchanged between the ANDSF and the querying terminal is expressed in 3GPP Management Objects (MOs), standardized in TS 24.312 [6]. This type of information structure is very similar to the one provided through HS2.0. In fact, considerations can be raised regarding the impact that two different sets of policies can exercise over the mobile terminal decision process. Under this aspect, and focusing strictly on the WLAN aspect, mobile operators interacting with WLAN aspects are interested in addressing information that goes beyond expressing SSIDs, as in the case of ANDSF, but rather expressing peer roaming agreements. As such, not only in order to address possible interference, but rather identifying complementary benefits, the 3GPP is analysing different HS2.0 scenarios in TR 23.865 [7].

4.2 Combined Use Cases and Analysis

4.2.1 Use Cases

4.2.1.1 Energy Saving on a Terminal

One of the main advantages of combining ANDSF and HS2.0 is that it can reduce battery consumption on terminals. Both technologies pursue a seamless access network discovery and selection while the terminals, on the move, meet available accesses.

The ANDSF server can deliver Hotspot/AP lists and policy information based on the UE's specific location. However, it is hard to know the exact information about restricted capabilities and dynamically changed backhaul status on the given lists. HS2.0 enables the UEs to obtain detailed information of the given AP, i.e. restricted connection capability, backhaul speed, congestion, etc., by using ANQP signalling exchange between the UE and AP. However, it may run out of battery to find the best-suited AP amongst many APs in the list. ANDSF provides the AP lists based on the terminal's location to confine the lists of APs the terminal needs to perform ANQP signalling, thus

reducing the number of ANQP signalling trials, avoiding quick battery consumption, and providing fast decision process for Wi-Fi association of the terminal.

For technical requirements, the following are required;

- The terminal should support S14 (ANDSF) and HS2.0.
- The terminal should send ANQP requests and receive ANQP responses in the preferred list provided by ANDSF response.
- More requirements are subject to intended applications.

4.2.1.2 Obtaining Capability of Provided APs in Specific Locations

In some area providing limited Internet connection like a campus or a securely managed company, there is a user who wants to get an Internet connection suited to his purpose among even same SSID-named APs – one is freely accessed whereas the other is limited with port blocking. ANDSF provides available Wi-Fi AP lists based on the terminal location. In the list, the terminal performs ANQP signalling with the two APs having the same SSID and obtains the connection capability information. In densely populated places having many and similar APs, HS2.0 is helpful for a user to select the best-suited AP by considering its Internet use.

For technical requirements, the followings are required.

- The terminal supports S14 (ANDSF) and HS2.0.
- The terminal sends information about its location in the S14 signaling.
- The terminal should send ANQP requests and receives ANQP responses with APs having the same SSID and their Connection Capabilities.

4.2.1.3 Discovering Purpose-Served Wi-Fi AP, based on User's Intention

When a terminal enters into a particular Wi-Fi area, it receives information that the app should be redirected towards the Wi-Fi AP – having a particular SSID or BSSID – provided by a shop supporting the app for value-added services. When there exists APs with the same or similar SSID outside the store or place and it is overlapped with the AP installed within the area, especially with "Venue Name" provided by ANQP response, it can provide more accurate information for the user to select the best-suited AP to its use.

For technical requirements, the followings are required.

- The terminal supports S14 (ANDSF) and HS2.0.
- The terminal sends information about its location in the S14 signalling.
- The terminal should send ANQP requests and receives ANQP responses to APs having same SSID and their Venue Names.

4.3 Harmonizing Policies from ANDSF and HOTSPOT2.0

When both Wi-Fi-assisted technologies are used at the same time, two policies, coming from ANDSF and HS2.0, may bring coordination or harmonization issues. How those policies can be transferred and how some conflicted policies should be handled is an interesting issue.

A 3GPP TR 23.865 [8] presents several ways of how ANDSF policies can be extended to include HS2.0 policies. Based on the standardized vision from TR 23.865, three principles can be highlighted, addressing how to extend the ANDSF MO with policies related to HS2.0.

4.3.1 Providing both HS2.0 MO and ANDSF MO to the UE

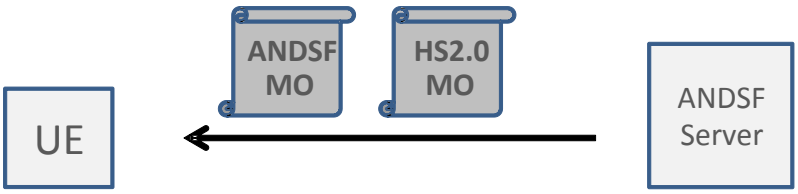

Figure 11 – A way of providing both HS2.0 MO and ANDSF MO to the UE

In this case, a 3GPP operator provides both the ANDSF policies and HS2.0 policies to a 3GPP UE. Both ANDSF MO and HS2.0 MO may be provided by the ANDSF Server as illustrated in Figure 11. Moreover, only the relevant subset of the HS2.0 MO would be used.

- On receiving those policies from the ANDSF Server, the UE evaluates the rule priority and prioritized access from the received policy. If the highest priority access technology is Wi-Fi, the UE selects an AP satisfying the HS2.0 policies.
- The ANDSF MO need to be extended to include additional policies related to HS2.0 parameters.

Advantages:

- No dependency between 3GPP ANDSF work and Wi-Fi Alliance HS2.0 work.

Disadvantages:

- Since HS2.0 policies are “global”, it is not possible to have HS2.0 with validity conditions (e.g. time-of-day and validity area) defined by ANDSF to make more “intelligent” Wi-Fi network selection. To add the validity conditions to the HS2.0 MO, 3GPP needs to work with Wi-Fi Alliance for enhancing HS2.0 to support validity conditions.

4.3.2 ANDSF MO Enhanced with Policies related to Elements HS2.0 (Rel. 1)

In this case, the ANDSF MO is enhanced with policies related to information elements available in HS2.0 Release 1,, providing additional functionality, including policy delivery from additional HS 2.0 releases with a different policy format.

- 3GPP extends the existing ANDSF policies with new policy elements based on HS2.0 Release 1 information. This is decoupled from the policies defined by Wi-Fi Alliance for HS2.0 Release 2.
- To include HS2.0 MOs, 3GPP may choose to simply copy-paste the definition into ANDSF MO, simplifying UE implementation since each policy is defined in the same way in both HS2.0 MO and ANDSF MO.
- Or, 3GPP may add different policies than those contained in HS2.0 and may also use different definitions compared to what Wi-Fi Alliance uses in HS2.0 MOs.

Advantages:

- Full flexibility in 3GPP to define Wi-Fi selection policies.
- Possible to make use of ANDSF validity conditions, priorities, etc. also for policies related to HS2.0 capabilities.

Disadvantages:

- It will be bound to any future extensions from Wi-Fi Alliance. HS2.0 MO policies further extended will not automatically be applicable to 3GPP scenarios, so this may conflict with HS2.0-related policies already defined by 3GPP.
- If the UE implementation is intended to fulfil both HS2.0 and ANDSF specifications, then different policy definitions will cause increased implementation complexity.

4.3.3 ANDSF MO Included with Relevant Parts of HS2.0 MO

In this case, the ANDSF MO is enhanced to include relevant parts of HS2.0 MOs. So, instances of the HS2.0 policies (in the format defined by HS2.0) are included (copy-and-pasted) into the ANDSF MO.

- Instances can be extended in ISRP and ISMP, or included in a new sub-tree in the ANDSF MO. Such a sub-tree would be dedicated for selecting Wi-Fi access network. For the definition in a new sub-tree, validity conditions should be added to that sub-tree to define under certain conditions that the HS2.0 policies are applicable to allow a more “intelligent” Wi-Fi network selection.

Advantages:

- There is a minimal dependency between 3GPP ANDSF and Wi-Fi Alliance HS2.0 work.
- Policies defined by any future extensions of HS2.0 Release 2.0 MO in Wi-Fi Alliance can easily be applicable to 3GPP scenarios as well.
- It is possible to make use of ANDSF validity conditions, priorities, etc. also for policies related to HS2.0 capabilities.

Disadvantages:

- If 3GPP desires to include anything not covered by HS2.0 Release 2 (e.g. policies for venue type information), it needs to define how to integrate such information elements directly into the ANDSF MO, or work in Wi-Fi Alliance to extend the HS2.0 MOs.

5. Concluding Remark

This paper described the technical aspects of Hotspot 2.0, as a powerful enabler able to bring better user experience over deployed Wi-Fi access networks. Concretely, the principles and technical aspects of Hotspot 2.0 were addressed, comprehensively including its architecture, procedures, and supported capabilities specified by the Wi-Fi Alliance. In addition, a set of the most prominent use cases realized by Hotspot 2.0 were provided.

This paper also addressed the basic technological aspects of ANDSF, which is a standard cellular technology providing the capability for mobile terminals to select the best access network suited to their purposes and preferences. These aspects become increasingly important in terms of applicability and usability over the evolving mobile operator network accommodating non-3GPP accesses. Such a novel feature provides ample synergic capabilities with Hotspot 2.0, since they both aim to support the selection of the best access, even though they are based on different access technologies standards. With this vision, we therefore provided jointly combined use cases and briefly analysed the technical requirements for each one, and presented the ways of delivering ANDSF and Hotspot 2.0 policies, under a 3GPP standard perspective.

In the current existing standardized descriptions and proposals, we have identified that ANDSF and Hotspot 2.0 will be highly required and extensively utilized as supportive mechanisms for an optimized, seamless and enhanced Internet access, as those are becoming essential in the current complex network deployment environments that involve various network policies.

Since the Wi-Fi Alliance and 3GPP standards have been progressing on each technology, it is also expected to see more enhanced capabilities along the evolution of the current network and its deployment, and even more integration issues.

6. References

[1] IEEE 802.11-2012, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[2] Marketing Requirements Document for Hotspot 2.0: Wi-Fi CERTIFIED PassPoint™ Certification Amendment, December 2011.

[3] Wi-Fi Peer-to-Peer (P2P) Technical Specification, Version 1.1, October 2010, https://www.wi-fi.org/knowledge-center/published-specification

[4] Wi-Fi Hotspot 2.0 Technical Specification R2 V4.00

[5] 3GPP TR 23.865, “Study on Wireless Local Area Network (WLAN) network selection for 3GPP terminals,” v12.1.0, Dec. 2013.

[6] 3GPP TS 23.402, “Architecture enhancements for non-3GPP accesses,” v12.4.0, Mar. 2014.

[7] 3GPP TS 24.302, “Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks,” v12.4.0, Mar. 2014.

3GPP TS 24.312, “Access Network Discovery and Selection Function (ANDSF) Management Object (MO),” v12.4.0, Mar. 2014.

Rua Eng. José Ferreira Pinto Basto
3810-106 Aveiro
Portugal

Tel.: +351 234 403 200
Fax: +351 234 424 723

www.alticelabs.com