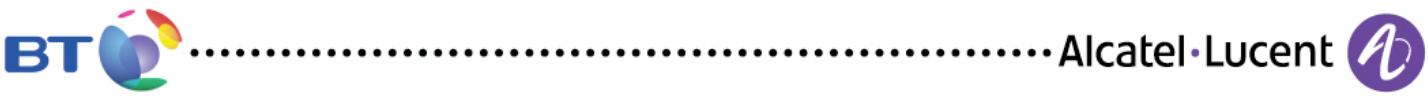
# WI-FI ROAMING – BUILDING ON ANDSF AND HOTSPOT2.0



# EXECUTIVE SUMMARY

This research collaboration paper between Alcatel-Lucent and BT describes the need for Heterogeneous Network Policies in a multi-operator environment. It analyses how new standards like the 3GPP Access Network Discovery and Selection Function (ANDSF) and the Hotspot2.0 initiative can complement each other to meet those needs whilst identifying a number of use-case scenarios where further standards work is required.

ANDSF is a cellular technology standard which allows an operator to provide a list of preferred access networks with policies for their use up to the granularity of a single IP flow or all traffic for a given PDN network (APN). IEEE 80211u and WFA Hotspot2.0 are Wi-Fi technology standards that allow devices to more easily discover Wi-Fi roaming relationships, determine access point capabilities and loading conditions, and more easily connect to Wi-Fi networks securely.

The combination of ANDSF and Hotspot2.0 is a particularly powerful enabler for a pain-free user experience across Wi-Fi and cellular networks.

The analysis identifies some proposals for further discussion and outlines potential contributions to the relevant standard bodies that we believe could improve the user and operator experience of heterogeneous network.

# TABLE OF CONTENTS

# INTRODUCTION

## The Need for Heterogeneous Network Policies

Even with planned LTE network upgrades, mobile traffic demands are forecast to exceed network capacities in the short to medium term. Operators are addressing this capacity crunch in a number of ways:

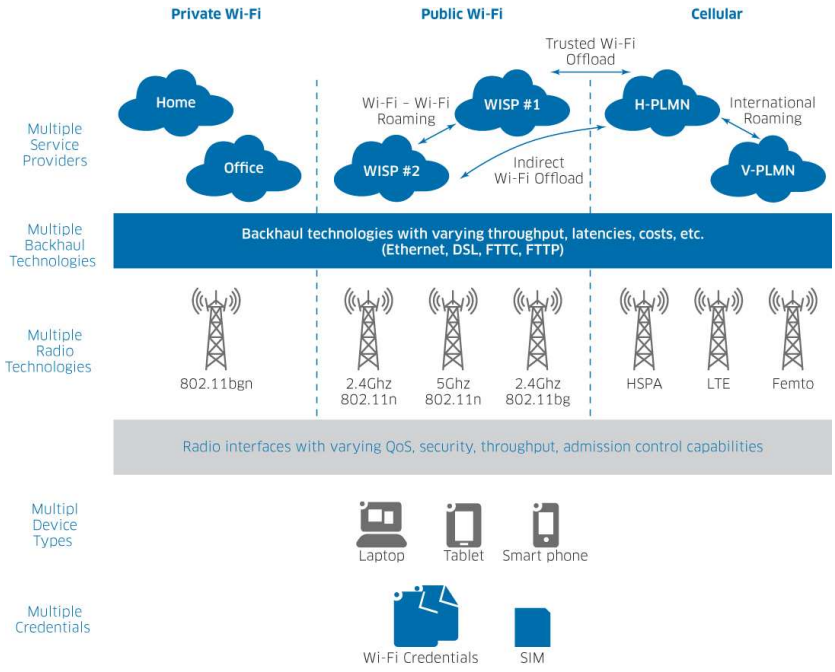
- Retreating from offering unlimited data bundle caps
- Improving policy control on existing networks
- Exploiting heterogeneous access networks, i.e. WLAN offload, femto cells

Policy controls typically enable network operators to manage current and future traffic demands whilst maintaining a decent customer experience by:

- Constraining traffic within the available network resources
- Responding effectively to changes in dynamic loading levels
- Offering differing levels of user subscriptions
- Prioritising QoS dependent services which require guaranteed connectivity; for example, VoIP, Internet TV, online gaming
- Blocking certain traffic types; for example, tariff caps, content blocking, age restrictions
- Exploiting routing efficiencies in backhaul networks; for example, selective IP traffic offload

Heterogeneous access networks allow mobile operators to move traffic from the macro cellular network, where the capacity constraints are most acute, to cheaper shorter range Wi-Fi and femto/picocell networks connected over a variety of backhaul connections. The environment for mobile connectivity is therefore becoming a more complex mix of technologies in both the air interface, backhaul and core which is further complicated by the more complex inter-operator roaming agreements enabled by emerging technologies such as Hotspot2.0 and non-3GPP access for EPC.

**Figure 1. Future heterogeneous environment**



To date, most network policy control infrastructures are applied within a homogeneous network scenario where a single network operator owns and controls the end-to-end network, for example, the LTE PCC architecture. As we move to a heterogeneous operator environment then the various networks may be owned by different operators and the various technologies may not always offer the same underlying policy enforcement mechanisms.

Delivering the effective policy control necessary for a good customer experience within heterogeneous environments faces a number of specific challenges:

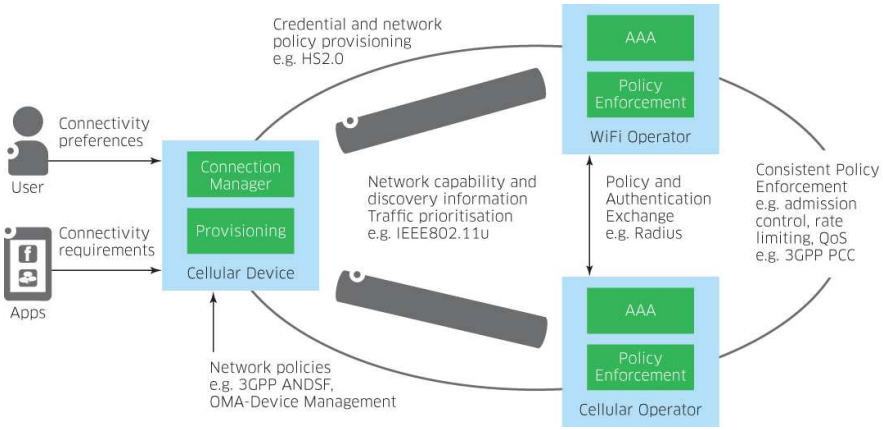
- Users may have multiple billing relationships with different access networks and so effectively multiple home operators. It is therefore no longer clear who owns the customer experience.
- Different access technologies are standardised by different standards bodies, therefore inevitable differences will occur in the policy control frameworks.
- Heterogeneous networks are exhibiting greater variability in their performance characteristics as new radio and backhaul technologies rollout: new flavours of Wi-Fi at 2.4 and 5 GHz, femtocells and a variety of backhaul and local loop technologies such as fibre to the cabinet and fibre to the premise.
- Public Wi-Fi coverage is increasing as fixed broadband operators see the advantages of community Wi-Fi schemes such as BT Fon, and as retailers and businesses see consumers demanding Wi-Fi access in shops, cafes, and hotels. This is creating greater overlap in Wi-Fi network coverage and a greater variety of Wi-Fi networks that users can connect to.
- New IP interconnection and roaming architectures such as trusted Wi-Fi offload and the Wi-Fi Alliance (WFA) Hotspot2.0/Wireless Broadband Alliance (WBA) Next Generation Hotspot (NGH) are emerging to enable cellular operators to meet the increasing traffic demands of mobile users. The trusted versus untrusted relationship adds a new dimension to the network selection and traffic routing policies, further complicating the decision process.
- Higher device costs and user investment in applications and content are driving SIM only contracts, with the result that the home cellular operator has less control over the device, and consequently, has less influence over the behaviour of device connection managers and device support for standards-based provisioning mechanisms.
- OEMs are taking more control of the user experience and are imposing their own network selection and traffic routing policies. It can be difficult to override this device behaviour and the diversity between OEMs on device policies can make it difficult to guarantee the user experience.

## Current Heterogeneous Policy Control

Today there is little consistency between the mechanisms used by Wi-Fi operators and those used by cellular operators to control, for example, network discovery, network selection, traffic prioritisation, user authentication, roaming capabilities and quality of service (QoS).

The user experience of heterogeneous networks is therefore very dependent on the device connection manager (and hence on the device vendor) which attempts to balance between the user preferences, various types of network policies and what it can discover about the available access networks to make the correct connectivity decision automatically on behalf of the user.

**Figure 2. Role of the connection manager**




However, Connection Manager (CM) behaviour varies significantly between OEMs/Operating system providers and it can often result in incorrect decisions or missed opportunities to connect to better networks. This leads to the user experiencing problems which are difficult to diagnose and fix. Some operators have attempted to overcome the behaviour of device connection managers with third-party applications. However, the ability of a third-party application to fix connectivity behaviour is limited, and one finds that even on devices where such an application is possible it is in a constant tug-of-war with the native connection manager. Even where appropriate standards do exist, the lack of device support for such standards makes it difficult or more expensive for operators to influence the behaviour of the device connection manager using network provided policies.

For heterogeneous environments, the current simplistic behaviour of device connection managers is inadequate. Lack of consistency of network traffic prioritisation and varying core network policy enforcement lead to a varying user experience. For example, not all services may be available on all networks or content filtering may be different across networks. This serves to break the seamless heterogeneous roaming that is the goal for operators.

In this paper we first consider the standards that are available to improve the customer experience of heterogeneous networks. We provide an overview of the two main standards involved: 3GPP ANDSF and Wi-Fi Alliance Hotspot 2.0. We then identify those use cases that are well covered by these and other relevant current standards activities and other use cases which are perhaps more challenging. For the latter, where we can, we identify the changes to the standards that would be necessary.

# 3GPP ANDSF

This section summarises the key features of the 3GPP Access Network Discovery and Selection Function (ANDSF) — a framework for specifying and delivering access network selection policy to mobile handsets.

## Key Definitions/Summary

In Release 8 the 3GPP partnership project has defined how a User Equipment (UE), or mobile device, can connect to the Evolved Packet Core (EPC) using a non-3GPP access (WLAN, WiMAX, CDMA2000). In the remainder of this document, only WLAN case will be considered.

In Release 10 this has evolved to support also the use cases where a same UE can connect simultaneously to both a 3GPP access (GERAN, UTRAN, e-UTRAN) and a non-3GPP access.

Simultaneous multi-access connectivity can be provided in several flavours:

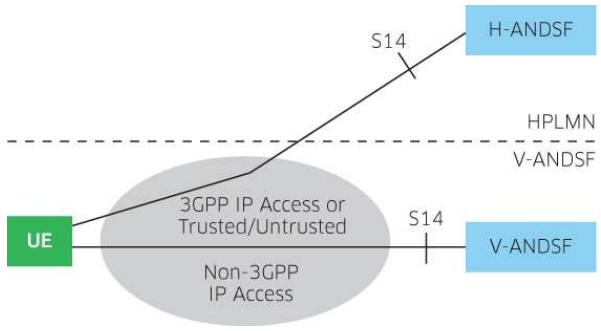
- **MAPCON –** Multi-Access PDN Connectivity: The ability to have one APN (one PDN connection) on a cellular access and another APN on a non-3GPP access.
- **IFOM –** IP Flow Mobility: The ability on a per IP flow basis to choose on which access each flow should be supported and to move them seamlessly between accesses.
- **Non-seamless Offload**: The ability on a per IP flow basis to choose on which access each flow should be supported, but assuming the flows over the non-3GPP access will not go through the 3GPP Enhanced Packet Core (hence without support for session continuity).

To allow mobile devices to know where, when and how to choose a non-3GPP access network, the TS 23.402 "Architecture enhancements for non-3GPP accesses" defines the ANDSF).

As illustrated in the figure below, the TS 23.402 defines a direct interface between a mobile device (UE) and an ANDSF server reachable through an IP network.

A UE that is roaming can access both the ANDSF server of its Home operator (H-ANDSF) and the ANDSF server of the visited network (V-ANDSF). (In case of a conflict, the V-ANDSF takes precedence.)

**Figure 4.8.1.1-2 from 23.402: Roaming Architecture for Access Network Discovery Support Functions**



According to the TR 21.905 definition, the Home Operator or Home PLMN (Public Land Mobile Network) is a PLMN where the MCC (Mobile Country Code) and MNC (Mobile Network Code) of the PLMN identity match the MCC and MNC of the IMSI (International Mobile Subscriber Identity). A Visited PLMN is a PLMN different from the HPLMN or from the Equivalent Home PLMN list.

It is worth noting that the Visited notion then doesn't relate to WLAN networks but just to cellular networks.

The ANDSF information is represented by the ANDSF Management Object described in 3GPP TS 24.312, an XML document compatible with OMA-DM standards.

This model specifies the following types of information:

- UE location
- Discovery information
- Inter-System Mobility Policies
- Inter-System Routing Policies

UE location: The UE may send his current location to the ANDSF server (this location can be based on geographical coordinates, a cellular cell or area, a WLAN location (HESSID, SSID, BSSID).

Discovery information may be sent by the ANDSF server and allows the mobile device to map from its current location to a list of alternative access networks that may also be available. For example, a list of Wi-Fi access networks within the current 3G cell or at the current mobile device geographical location can be provided by the ANDSF server.

Inter-System Mobility Policies (ISMP) may be sent by the ANDSF server and apply to UEs that do not support MAPCON, IFOM or non-seamless offload (or do not have these features enabled). They consist of a number of prioritised rules that control which network should be used. Each rule defines a location and/or a time when a particular access network can be used. For example, a particular Wi-Fi access network can be marked as valid when the mobile device is in a particular 3G cell between 9 a.m. and 5 p.m. The mobile device will use the access network which is valid and has the highest priority.

Inter-System Routing Policies (ISRP) may be sent by the ANDSF server and apply to UEs that support MAPCON, IFOM or non-seamless offload. Similarly to ISMP, they consist of a number of prioritised rules that control which network should be used on:

- Per APN basis for MAPCON
- Per IP flow basis for IFOM and non-seamless offload

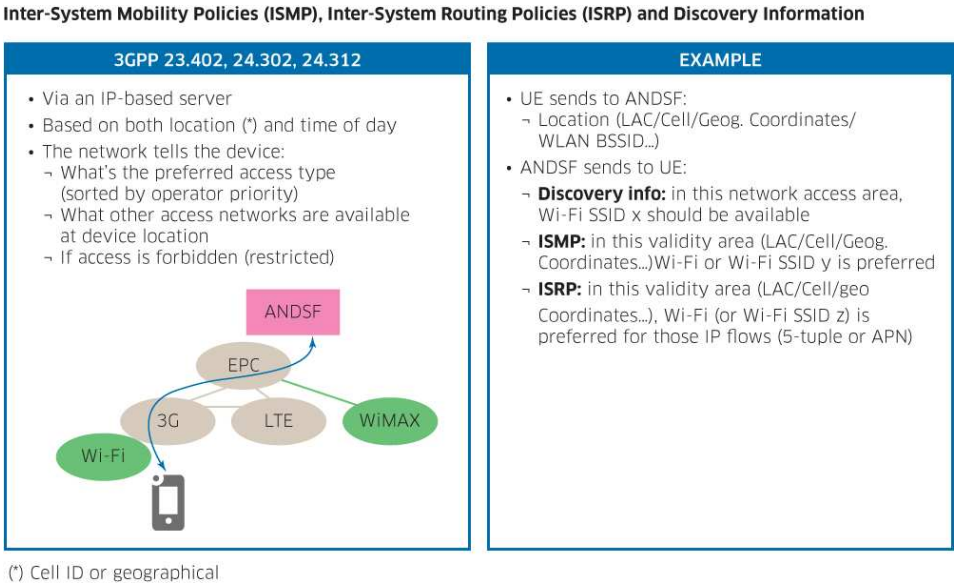
Both ISMP and ISRP also allow usage of some access networks to be restricted. Thus it is possible, for example, to specify which APN MAY be moved to non-3GPP access and which MUST remain over 3GPP coverage (for MAPCON), and which IP flows MAY be moved to non-3GPP access and which MUST remain over 3GPP coverage (for IFOM).

The frequency of the UE request as well as the size of the data sent to the UE (information sent to the UE = ANDSF data for a whole country/region/town and so on) are not defined by the 3GPP.

## Wi-Fi Network Identification in ANDSF

It is worth noting that in the ANDSF Managed Object (MO) model, Wi-Fi networks are identified using their SSID possibly coupled with HESSID. For location purposes the BSSID (the MAC address of the access point) is used (with or without SSID and/or HESSID). No other information is available to mention whether a given access network is public or private, belongs to the MNO or not, what kind of networks or services may be behind. (It thus differs from the information provided by Hotspot2.0. See Hotspot2.0 Description, p11.)

**Figure 3. ANDSF example 1**




(Note: The HESSID is defined in 802.11u and described in Hotspot2.0 Description, p11.)

## Usage Scenarios

ANDSF supports the following scenarios:

**A. Policy information download from any network and in-advance storage of policies/network maps**

- Providing information regarding non-3GPP access networks discovery and selection while a device is not connected to a WLAN network nor has its Wi-Fi interface switched on
- Providing information regarding non-3GPP access networks while a device is not connected to a WLAN network but has its Wi-Fi interface switched on
- Providing information while a device is connected to a WLAN network

| Device on: | ANDSF info available/delivered |
|---|---|
| Cellular only<br>(Wi-Fi interface off) | Yes |
| Cellular,<br>Wi-Fi interface ON | Yes |
| Attached to Wi-Fi | Yes |
| No network | Yes: Policies and discovery information may have been sent earlier and stored (and covering a far wider area than the one the device was previously on). |

**B. UE location reporting**

Reporting a device location based on one or several technologies at the same time:

- A 3GPP location (at least the PLMN but could be tracking/location areas or one/a set of cell identifiers)
- A geo-location (latitude, longitude)
- A WLAN location (at least BSSID, with/without SSID/HESSID)

**C. Tailored information based on both UE location and time of day**

Although discovery information and policies could be sent in advance and cover a very wide area (even a PLMN), thanks to the UE reporting its location when querying the ANDSF, the operator also has the choice to only send tailored information based on the UE location. Furthermore, time of day can also be used for validating when a given policy is to be applied.

**D. Available access networks list**

- Providing information on location of WLAN access networks (note that though implicitly it is assumed those networks allow to connect to the EPC, it is not necessarily so)

**E. Restricted/Preferred access networks list**

- Providing policies for restricted/preferred access networks

**F. Push/Pull mode**

The ANDSF may be queried by the UE (pull mode) but also supports a push mode to send network initiated updates to the device. Note though that ANDSF push interactions might not always be possible in all scenarios (for instance, via non-seamless WLAN offload).

# HOTSPOT2.0 DESCRIPTION

## Wi-Fi Alliance Hotspot2.0

The Wi-Fi Alliance has created a new standards activity, Hotspot2.0. Among the agreed requirements, HS2.0 will improve the ability of Wi-Fi devices to discover and securely connect to public Wi-Fi hotspots and thereby enable easier roaming between public Wi-Fi networks. The Hotspot2.0 work builds on the recently ratified IEEE 802.11u specification, which provides query mechanisms to enable devices to discover information about the roaming partners available and hence the type of credentials which may be used with the access point. It also incorporates the long ratified IEEE 802.11i based WPA2 Enterprise security specification which enables secure authentication and encryption for Wi-Fi data using a variety of user credentials including (U)SIM, digital certificates and username/passwords.

### IEEE 802.11i

IEEE 802.11i WPA2-Enterprise defines a standard for establishing secure, mutually authenticated channel between a Wi-Fi device and an access point *prior to* the establishment of any IP-based communications. 802.11i specifies authentication and data confidentially between the wireless client and the Access Point. Mutual authentication is performed using the Extensible Authentication Protocol over IEEE 802.1x, and data confidentiality (encryption) is provided using Counter Mode with Cipher Block Chaining Message (CCMP) which utilises 128-bit AES encryption and offers similar cryptographic strength to 3G cellular networks.

Multiple flavours of user credentials are supported within the 802.1x/EAP specifications and the device and access points can automatically negotiate which method will be used. The following user credentials are of most interest within next-generation public Wi-Fi networks.

- EAP-TLS RFC 5216 – uses public key infrastructure based client and server certificates. Appropriate for a fixed operator without HLR/HSS credential capability.
- EAP-TTLS RFC 5281 – allows legacy password-based authentication protocols to be used against existing authentication databases.
- EAP-SIM RFC 4186 – uses SIM card credentials and 2G network cryptographic algorithms for the challenge response.
- EAP-AKA RFC 4187 – uses SIM card credentials and 3G network cryptographic algorithms for the challenge response. This method is mandated within the 3GPP architecture for the S2a interface.

EAP-SIM/EAP-AKA are the most likely authentication choices for the MNOs because these methods utilise the same challenge-response authentication mechanism already used in the cellular network. EAP-TLS or EAP-TTLS are the most likely choice for pure Wi-Fi operators without a SIM based authentication infrastructure. EAP-TLS relies on the secure provisioning and storage of per user certificates on the mobile devices, whereas EAP-TTLS uses certificates to authenticate the server and username/password to authenticate the user.

Deployment of an IEEE 802.1x architecture introduces a number of new entities to the public Wi-Fi architecture:

- Supplicant: an entity within the mobile device for handling the client side of the 802.1x authentication. This is available on virtually all modern Wi-Fi enabled smartphones.
- Authenticator: an entity within the Wi-Fi access point for managing the 802.1x port access control and data encryption and for routing EAP requests to the AAA proxy or server.
- AAA proxy: an optional Radius AAA server in the access network responsible for forwarding EAP exchanges to other AAA servers (for example, Home AAA) based on the identity provided by the supplicant.
- AAA server: the Radius AAA server in the core network with which the user has a billing relationship. For MNOs this server may be responsible for providing the RADIUS/Diameter interface to the HSS.

The 802.1x/WPA2 authentication sequence is performed automatically whenever a device connects to an 802.1x enabled access point. It consists of 4 phases:

- **Scanning –** automatic detection of the availability of the access point and its 802.11i support
- **Association –** initial 802.11 association
- **Mutual Authentication –** 802.1x EAP authentication of the user and access point
- **Encryption Negotiation –** generation of a dynamic key for encryption of the air interface

IEEE 802.1x therefore provides a simple automatic and secure Wi-Fi connection and encryption mechanism able to utilise a variety of user credentials. Importantly for Hotspot2.0, an authentication exchange is performed between the device and an AAA server located potentially within the home service provider's core network. The authenticator or AAA proxy in the visited Wi-Fi network is able to determine to which service provider's AAA server the authentication should be forwarded, based on the NAI realm that the device provides as part of the Mutual Authentication phase.

#### IEEE 802.11u

IEEE 802.11u is an extension to the IEEE 802.11 standard to improve the ability of devices to discover, authenticate, and use nearby Wi-Fi access points.

**It introduces the concept of a Subscription Service Provider (SSP)**, which is the entity responsible for managing the user's subscription and associated credentials. Multiple SSPs will typically be accessible through a single access point, reflecting the various roaming relationships. The SSP concept is key to enabling easier Wi-Fi roaming as it breaks the relationship between the SSID and the access credentials. Instead, devices dynamically query which SSPs are accessible via the AP, irrespective of the SSID(s) that the AP is broadcasting. This allows devices to automatically discover roaming agreements on access points it has never previously connected to.

IEEE 802.11u defines changes to the Beacon and Probe messages as well as a new Public Action Frame based Generic Advertisement Service (GAS) that allows unauthenticated devices to query an access point capabilities and supported SSPs before associating. Changes to the beacon and probe messages allow access points to broadcast their support for 802.11u for example, as well as for some broad roaming information such as Roaming Consortium OUI. A roaming consortium is a group of subscription service providers (SSPs) having inter-SSP roaming agreements. GAS enables devices to perform more detailed queries.

## Homogeneous Extended Service Set ID (HESSID)

The HESSID is a new identifier introduced in IEEE 802.11u and is used to identify a set of access points (BSS) that belong to the same network and which consequently exhibit common networking behaviour. It is the identifier of the network behind the Layer 2 wireless route and it should be used in conjunction with SSID, which is the existing WLAN radio access identifier. Both HESSID and SSID are therefore used together to discover a specific WLAN and its network attachment. Coupled together, they provide a unique identifier for a WLAN access network. If the HESSID parameter is not available in the WLAN hotspot, then the SSID is used only, as with current implementations.

The HESSID is typically the value of the BSSID of one of the access points in that set. The HESSID is optionally present in the IEEE 802.11u beacon messages and so can be discovered prior to association.

However, this makes it vulnerable to spoofing and cannot be relied upon as a secure identification. Its primary aim is to allow subdivision of APs sharing a common SSID.

### Main Extensions to Beacon/Probe/Association Messages

The most relevant extensions to Beacon/Probe/Association messages are described here. A more detailed list is available in Hotspot2.0 Description, p11.

| Interworking | Indicates support of IEEE 802.11u based interworking service |
|---|---|
| Advertising Protocol | Contains information that identifies a particular advertisement protocol supported by the AP, for example, ANQP or IEEE 802.21 |
| Roaming Consortium | Contains information identifying the roaming consortium and/or SSP whose security credentials can be used to authenticate with the AP |
| QoS Map | Support for the QoS mapping service |
| SSPN interface | Indicates whether the AP supports an interface to SSPNs for the purpose of authenticating users and provisioning services |

### Access Network Query Protocol

GAS queries and responses can be formatted using a number of protocols; however, Access Network Query Protocol (ANQP) (defined as part of IEEE 802.11u) is likely to be the most commonly supported.

ANQP defines a number of standard Information Elements, which allow devices to query specific information such as location, cellular network roaming, emergency services support, authentication realms and so on. ANQP is also a two-way exchange enabling the device to provide its values for these information elements to the access point or to an ANQP server during the exchange.

As the beacon/probe messages may be limited in size, ANQP allows the mobile device to query a longer list of roaming consortium identifiers.

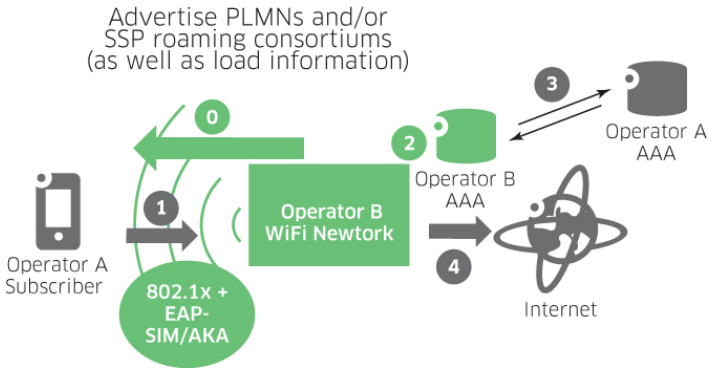
Thanks to the 3GPP Cellular Network Information Element, ANQP can also provide the list of PLMNs that can be accessed via the access point.

### QoS Enhancements

In addition to improving the ability of devices to discover compatible Wi-Fi networks, IEEE 802.11u also provides extensions to the basic IEEE 802.11e QoS mechanisms to improve the ability of the Wi-Fi network to manage traffic for multiple SSPs. A Wi-Fi network, as part of the roaming agreement, can be provided with a QoS Mapping from the SSP which determines how downlink IP traffic classes should be mapped to the over-the-air IEEE 802.11 QoS traffic classes.

In addition, a new QoS Action Frame message (QoS Map Configure) allows the AP to send this SSP specific QoS mapping definition to the device, thereby enabling the device to apply the QoS mapping to uplink IP traffic.

**Figure 4. Hotspot2.0 principle**



# ANDSF/HOTSPOT2.0 COMPLEMENTARITY

The list below is not exhaustive but summarizes network discovery and selection features provided by ANDSF and Hotspot2.0:

| Device on: | ANDSF info available | Hotspot2.0 info available |
|---|---|---|
| Cellular only<br>(Wi-Fi interface off) | Yes | No |
| Cellular,<br>Wi-Fi interface ON | Yes | Yes |
| Attached to Wi-Fi | Yes | Yes |
| No network | Yes: Policies and discovery information may have been sent earlier and stored (and covering a far wider area than the one the device was previously on). | No: Hotspot2.0 information can only be received on the spot (but still could be stored by the device). On the other hand, it provides more dynamic information than ANDSF which can be coupled with 802.11 broadcasted channel load. |

| Information | Provided by ANDSF | | Provided by Hotspot2.0 | |
|---|---|---|---|---|
| Location (*) of other WLAN networks | Yes | Part of Discovery Information | No | But an ANDSF server could be queried via ANQP or ANDSF could be another protocol advertised alongside ANQP or 802.21 |
| WLAN security type | Yes | Part of Discovery Information (AccessNetworkInformationRef) | Yes | Implied from the credentials |
| Run-time URI for EAP parameters | Yes | Part of Discovery Information (AccessNetworkInformationRef) | | |
| IP@ type handled | Yes | Part of Discovery Information (AccessNetworkInformationRef) (not necessarily relevant when device connects to EPC and gets an address assigned by the EPC) | Yes | 802.11u |
| List of restricted/preferred access networks | Yes | Identified by SSID with/without HESSID (doesn't go to BSSID granularity) | No | |
| Type of access network | No | | Yes | 802.11u Access Network Type (public/private/private with guest access, chargeable public network, free public network, personal device network, emergency only…) |
| Venue | No | | Yes | 802.11u<br>**Group** (residential, business…)<br>**Type** (convention centre, library, coffee shop…)<br>**Name** ("Starbucks"…)<br>The lists are very detailed. |
| Network authentication type | | | Yes | 802.11u (acceptance of terms, online enrollment, http/https redirection, DNS redirection) |
| Roaming consortium list | No | | Yes | 802.11u |
| NAI realm + EAP method | No | EAP-SIM/AKA assumed | Yes | 802.11u |
| Reachable PLMN list | No | H-PLMN or V-PLMN implicitly assumed | Yes | 802.11u + 24.234 Annex A |
| BSS load | No | | Yes | 802.11 |
| AP load-balancing | No | | No | |
| Report UE location | Yes | | No | |

(*) In ANDSF, all locations defined with one or several technologies (cellular, geo-location, WLAN [BSSID with/without SSID/HESSID]).

# SCENARIO ANALYSIS

In the sections below, we provide a summary of expected scenarios for network selection,provide a summary of expected scenarios for network selection, network authentication and routing/QoS, respectively, and the potential issues they can raise.

To better understand them it is important to describe first the various possible operator relationships and the expected behaviour of both device and network elements.

## Different Possible Operator Relationships

### Operator identification

While mobile operators are traditionally identified by their PLMN, the 802.11u also caters for Roaming Consortiums that are not necessarily related to mobile network operators.

Thus, thanks to 802.11u, a device may learn what PLMNs can be accessed but also receive the list of roaming consortiums identified by an Organization Identifier field which contains a public organizationally unique identifier assigned by the IEEE.

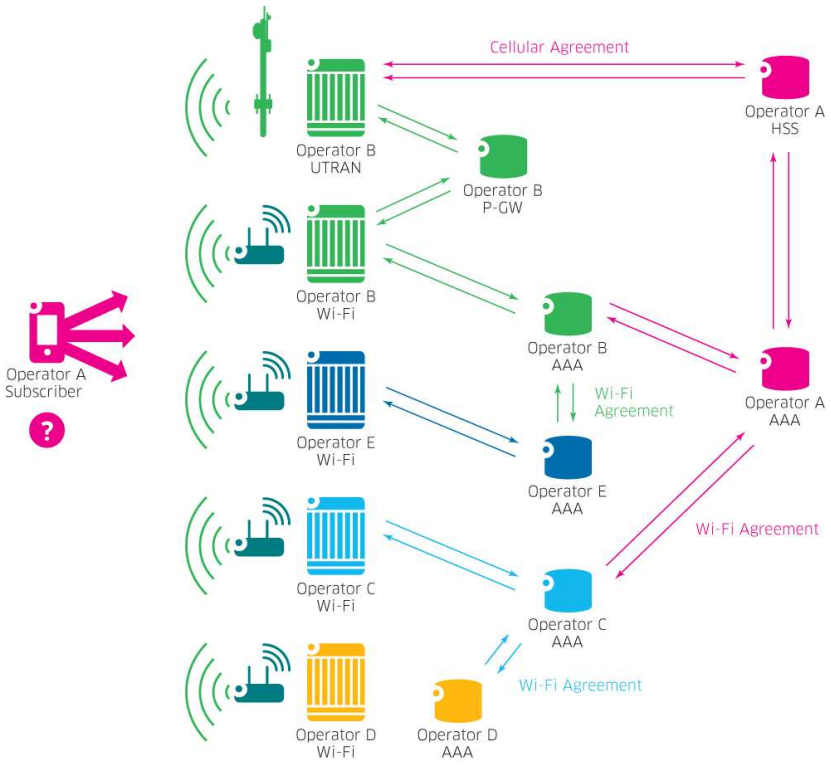
Figure 5 summarises the various operator relationships.

As an example, we see that a Mobile Network Operator A can have a cellular roaming relationship with MNO B that also owns a Wi-Fi estate.

B has also its own Wi-Fi agreement with E while A can have a direct agreement with C.

Note that C and E could be one and the same operator.

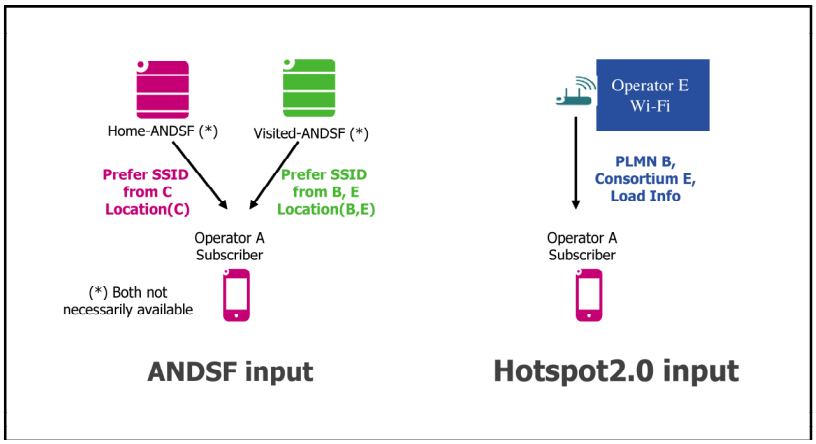
**Figure 5. Example of operator relationship**




## Expected Device and Network Behaviour for Support of the Scenarios Below

To perform network selection a device may benefit from the following inputs (all, some or none may be available to the device):

- its Home-ANDSF policies
- its Visited-ANDSF policies
- 802.11u list of PLMNs reachable via a Wi-Fi access network
- 802.11u list of roaming consortiums and/or SSP whose security credentials can be used to authenticate with the AP transmitting this element



In case of conflict between V-ANDSF and Home-ANDSF, V-ANDSF prevails (in particular to allow 3G to Wi-Fi session continuity support).

Note though that session continuity may not be an absolute requirement depending on operator choice or type of application the user is running.

In the example in Figure 6 below, thanks to both information received by the ANDSF and gathered using Hotspot2.0 mechanism, the UE knows it can connect with its credentials to any of the five access networks available.

The result of the network selection process in the UE will depend on actual content of the ANDSF policies as well as other local operating environment information like signal strength. How load information could be taken into account alongside ANDSF policies is unspecified, but the ANDSF Policies Delegation section (p31) offers a proposal to that effect.

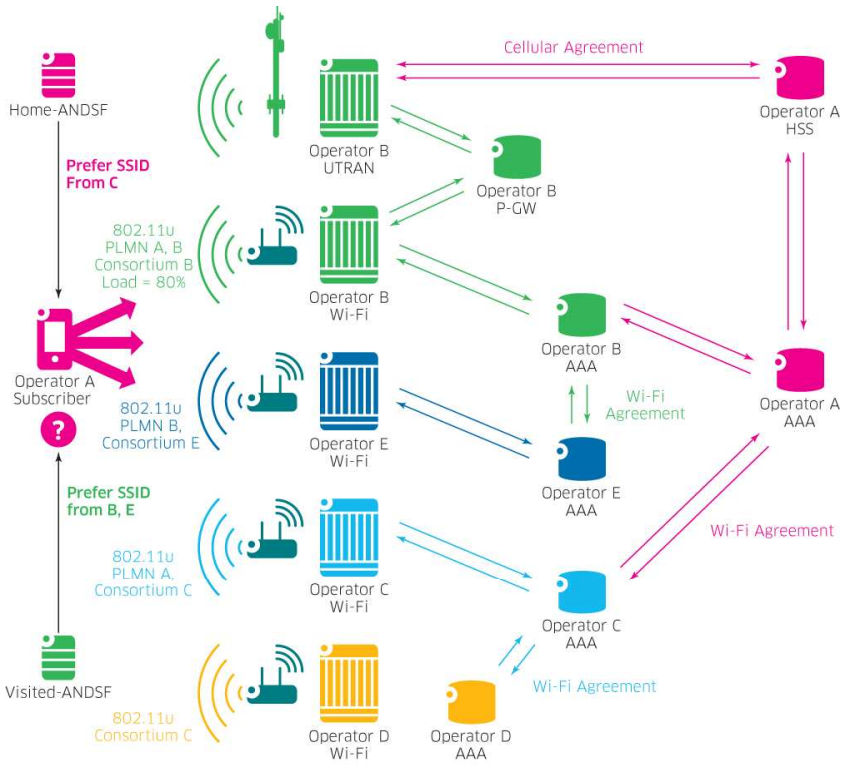
Assuming the selected network is Operator E Wi-Fi the device will build a decorated NAI (Network Access Identifier), as described in 3GPP TS 23.003, which will include its home realm as well as the registered PLMN as other realm.

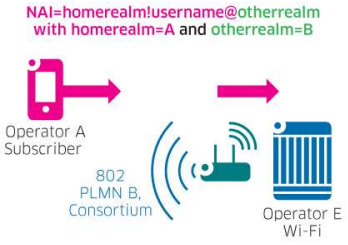
In our example based on the registered PLMN, the other realm is B so the authentication request will be forwarded by E to operator B AAA.

Should the network selection result have been for instance D, as home realm (A) and other realm (B) may not have been configured in D's network, the authentication may have to go through an AAA broker to reach Operator AAA.

Note though that this Home-MNO subscriber may not benefit from partnership with a WISP consortium if all SSIDs are not known in advance, as ANDSF identifies access networks rather than operators. Should additional roaming consortium be statically configured on the device, then there is no way to know how this would interact with ANDSF. The sections covering Network Selection Scenarios Summary (p20) and Addition of Roaming Consortium IDs in ANDSF Policies (p28) provide some suggestions for easing/solving this.

**Figure 6. Network selection example 1**




Building the decorated NAI

## Network Selection Scenarios Summary

These scenarios examine how current network selection policies can work.

### Subscriber with public Wi-Fi provided by cellular operator

| | Scenario description | Potential issues | Possible solutions | Comment |
|---|---|---|---|---|
| 1 | User has a cellular subscription from MNO1. MNO1 also owns Wi-Fi access. | | | This is a basic scenario supported both by 3GPP and Hotspot2.0. |
| 2 | User has a cellular subscription from MNO1. MNO1 has a Wi-Fi roaming agreement with WISP1. | | | This is a basic scenario supported both by 3GPP and Hotspot2.0. |
| 3 | User has a cellular subscription from MNO1. MNO1 has an international cellular roaming agreement with MNO2 and MNO2 has an in-country Wi-Fi roaming agreement with WISP2. | Because WISP2 does not have a roaming agreement with MNO1 it will not advertise support for MNO1 as an SSPN.<br><br>How will an HS2 device therefore discover that WISP2 can be used with MNO1 credentials?<br><br>How does the WISP2 know the roaming relationships between MNO1 and MNO2 as it must forward SIM credentials for MNO1 users to MNO2 AAA server? | V-ANDSF (from MNO2) will provide the relevant information to the device. The registered PLMN (MNO2) may also be detected by the device from the cellular network information in HS2.0.<br><br>Thanks to the NAI used by the device, WISP2 will know to send the authentication to MNO2 AAA. | |
| 4 | User has a cellular subscription from MNO1. MNO1 has an international cellular roaming agreement with MNO2 and MNO2 has an in-country Wi-Fi roaming agreement with WISP1.<br>MNO1 also has a Wi-Fi roaming agreement with WISP1. | The selected AP is the same; however, the AAA and traffic can be routed via MNO2 or direct to MNO1.<br><br>Session continuity for local breakout traffic (that is, PDN Gateway (PGW) in V-PLMN) can only be maintained if traffic goes through MNO2 core network.<br><br>The NAI built by the device will be in the form of MNO1realm!username@MNO2realm because the MNO2 is the registered PLMN.<br><br>It may be implementation dependent whether the direct connection to MNO1 would be used or connection to MNO2. | | (Device may get policies both from H-ANDSF and V-ANDSF. In this particular case, both would direct to the same access network.) |
| 5 | User has a cellular subscription from MNO1. MNO1 has an international cellular roaming agreement with MNO2 and MNO2 has an in-country Wi-Fi roaming agreement with WISP2.<br>MNO1 also has a Wi-Fi roaming agreement with WISP1. Both WISP1 and WISP2 provide coverage in the same area. | If the network selection process chooses WISP1 (for instance in absence of V-ANDSF guidance) then WISP1 may not know where to route the authentication as the NAI provided by the device will include the V-PLMN as "other realm." | Authentication may need to go through an AAA broker. | Session continuity for local breakout traffic (that is, PGW in V-PLMN) can only be maintained if traffic goes through MNO2 core network. Device may get policies both from H-ANDSF and V-ANDSF. The V-ANDSF would take precedence. Now WISP1 Hotspot2.0 would advertise the HPLMN, while WISP2 would advertise the VPLMN alias the registered PLMN. |

| | Scenario description | Potential issues | Possible solutions | Comment |
|---|---|---|---|---|
| 6 | The user is in range of both an HS2.0 AP advertising the MNO as a SSPN and a legacy AP with which the user has a private credentials; for example, home/office private Wi-Fi. | Should private networks take preference over Wi-Fi networks present in the ANDSF policy rules?<br><br>User access to private local network domain only possible if legacy AP is selected. | Provide policies per access network type (private, public, corporate…) | Stage 2&3 in 3GPP are not completely consistent. In Stage 3 user preferences override ANDSF policies. |
| 7 | The user is associated to an HS2.0 AP and a private AP becomes available. | Should the device remain associated to the current HS2.0 AP or switch to the private AP?<br><br>User access to private local network domain only possible if legacy AP is selected but only the HS2.0 AP may be able to offer QoS support for specific applications such as IMS voice over Wi-Fi. | Provide policies per access network type (private, public, corporate…) | Depends on the priority given by ANDSF between both APs. This could be a good use case to couple 802.11u information for reporting by the UE of the type of access point and for ANDSF to provide policies per AP type as described in "Addition of access network type in ANDSF policies" section. |
| 8 | User has a subscription with MNO1 which has roaming with WISP1. WISP1 has a roaming agreement with WISP2. | Because WISP2 does not have a roaming agreement with MNO1 it will not advertise the MNO1 SSPN. | WISP1 and WISP2 could belong to the same roaming consortium and hence the device could receive the information from Hotspot2.0.<br>That information could be made available via ANDSF using an extension of the policies to specify roaming consortium IDs. | See proposal in sections entitled "Addition of roaming consortium IDs in ANDSF policies" and "Greater Standardisation of SSPN interface". Indirect relationships would only be supported within consortiums agreements. |
| 9 | MNO1 has a roaming agreement with WISP1; however, WISP1 has Wi-Fi hotspots in multiple countries. MNO1 wants to restrict use of WISP1 to access points in a limited set of countries for certain groups of subscribers. | How does the home MNO operator know the location of the access point that the subscriber is connecting to in order to reject authentication?<br><br>How does the device know that access has been refused only for that country and that service from this WISP is still valid in other countries? | AP location could be supplied as an additional Radius/Diameter attribute by WISP1 in the AAA exchange. | |

### Subscriber with public Wi-Fi provided by WISP

| | Scenario description | Potential issues | Possible solutions | Comment |
|---|---|---|---|---|
| 10 | User has a Wi-Fi subscription from WISP1 and is in range of two HS2.0 APs owned by WISP2 and WISP3 both of which supports roaming with WISP1. WISP1 prefers to roam via WISP3, but the AP belonging to WISP2 has the best RSSI. | How does WISP1 indicate that WISP3 is the preferred roaming partner?<br><br>For a user without any ANDSF prioritisation there is no means to prioritise visited WISP in the HS2.0.<br><br>In addition, any solution needs to work for Wi-Fi only devices such as tablets where ANDSF function may not be available.<br><br>The user may not be aware of the commercial difference between WISP2 and WISP3 and so cannot be expected to make the decision as to which to use. | HS2.0 Phase 2 is discussing possible prioritisation mechanisms as part of the online sign-up mechanisms<br><br>A roaming partner preference list is required. | |
| 11 | User has a Wi-Fi subscription from WISP1 and buys temporary access from WISP2. The user is in range of an AP with roaming agreements with both WISP1 and WISP2, which SSPN should be used. | Currently no means to prioritise SSPNs relative to each other. | Prompt the user to select the SSPN from the list of valid ones at this time. | |
| 12 | User has a Wi-Fi only subscription (no SIM card) provided by an MNO that owns a Wi-Fi network. | | | MNO may wish to sell services to Wi-Fi only devices (iPad…) and connect them to its EPC.<br>Similar to basic Hotspot2.0 case? |

### Subscriber with both cellular and WISP Wi-Fi subscriptions

| | Scenario description | Questions | Possible solutions | Comment |
|---|---|---|---|---|
| 13 | User is in range of a Hotspot2.0 AP which advertises support for the cellular operator. | | | Same as in "Subscriber with public Wi-Fi provided by Cellular Operator" section. |
| 14 | User is in range of a Hotspot2.0 AP which advertises support for the WISP. | | | Same as in "Subscriber with both Cellular and WISP Wi-Fi subscriptions" section. |
| 15 | User is in range of a Hotspot2.0 AP which advertises support for both the cellular and Wi-Fi SSPNs. | Which subscription should be used? | Add prioritisation of SSPNs.<br>Again, as there is no way to anticipate the difference in cost for the end user, manual user preferences may still be needed. | |
| 16 | User is in range of a Hotspot2.0 AP which advertises support for the cellular SSPN and whose home SSPN is the Wi-Fi SSPN. | Should the device use the credentials associated with the home SSPN or not? | With prioritisation of SSPNs, the device would at least know which credentials to use. | Again, as there is no way to anticipate the difference in cost for the end user, manual user preferences may still be needed. |
| 17 | User is in range of 2 different Hotspot2.0 APs, AP1 advertises support for the cellular SSPN and AP2 advertises support for the Wi-Fi SSPN. | Which subscription and hence which AP should be connected to? | The ANDSF provided by the cellular SSPN will direct the device to AP1. | Decision may be overridden by user manual preferences. |
| 18 | User is in range of 2 different Hotspot2.0 APs with different SSIDs. Both advertise support for the cellular SSPN, but one is indicating WAN congestion via the HS2.0 extensions. | How does SSID prioritisation in ANDSF interact with HS2.0 congestion discovery? | Add a congestion criterion to the ANDSF rules. This could be achieved by use of a Local-ANDSF instance: ANDSF delegates policies to a local instance, that local instance is allowed to override ANDSF policies during an operator-defined time period based on congestion or load criteria. | The Local-ANDSF (L-ANDSF) and policy delegation proposal is an extension to current specifications described in "ANDSF Policies Delegation" section. |
| 19 | The device has received from ANDSF policy to always use Wi-Fi in a given area. Whilst connected on Wi-Fi, congestion (or any other problem) occurs and the device is disconnected due to a BSS Transition Request or Disassociate message for example. After switching to cellular the ANDSF policy forces the device to reconnect to the (still) available Wi-Fi network. | How long should a network policy that has failed to be applied be left before trying again?<br><br>Could result in repeated failed authentications and load on the WISP AAA infrastructure. | With an L-ANDSF instance, congestion would trigger a switch to cellular. The hysteresis value described in ANDSF Policies Delegation section (p31) would prevent failed attempts to reconnect immediately to Wi-Fi. | |
| 20 | Device is in range of two APs both supporting the cellular SSPN one of which provides trusted access to the cellular core, the other does not. | How does the device determine which AP provides trusted access?<br><br>When does the trusted access feature become more important than RF metrics such as RSSI? | | |

| | Scenario description | Questions | Possible solutions | Comment |
|---|---|---|---|---|
| 21 | In all the scenarios above what happens if the device is already connected to an AP and a better one becomes available? | When are network selection policies re-evaluated?<br><br>How important is staying with the current SSID, for example, to maintain session continuity versus changing SSID which may lead to improved services or better QoS? | | Depends on the priority given by ANDSF to the second SSID.<br>Quoting 23.402: "If the UE has access network discovery information, inter-system mobility policies or inter-system routing policies valid for its present location, which indicate that there is an access network in its vicinity with higher priority than the currently selected access network(s), the UE should perform procedures for discovering and reselecting the higher priority access network, if this is allowed by user preferences. |

**Subscriber with residential + public Wi-Fi + cellular subscriptions provided by the same operator**

This use case may be seen as a subset of use case 1 but with a dedicated focus for the home access. In such a case it would be particularly beneficial for the operator to steer the UE to the residential private network (even if a public SSID from same operator is available on the subscribers' box or access point). As the private SSID chosen by the subscriber is not known to the operator, current ANDSF specifications do not allow to give preference to that access. The Addition of Access Network Type in ANDSF Policies section (p29) is a proposal to couple 802.11u information made available from Hotspot2.0 to an ANDSF policy per access type.

**Specific case: Wi-Fi only devices**

It may not be expected that a Wi-Fi only device (for instance a tablet) will follow accurately 3GPP specifications as it may not even know that service is provided to him through an EPC core network. Hence the need to ensure behaviour of such a device, for example, building an NAI as suggested in the Improvements to Device Authentication Behaviour Section (p34).

Furthermore, such a HS2.0 device would still need some equivalent of ANDSF for network prioritisation as described in the Support for Multiple Network Policies on Devices Section (p36).

## Network Authentication Scenarios

The use of IEEE 802.1x based EAP authentication combined with interoperator roaming agreements means that devices may attempt to authenticate to a wider range of networks with potentially less reliable interconnects. This raises a number of possible scenarios where user authentication may fail or where the credentials may be valid but access is not allowed. Examples include:

1. Rogue APs advertising support for roaming partners
2. Wi-Fi networks using admission control to limit the number of users from roaming partners
3. Roaming networks where home operators wish to provide access for subsets of their users, for example, gold subscribers only
4. Temporary failures in network routing within visited operators or roaming hubs due to AAA outage

5. Overloading of AAA servers

In all these cases the behaviour of the WPA supplicant should be such as to *avoid*:

- incorrectly invalidating device credentials or network settings (and preventing the device from attempting to connect to a valid AP in future)
- generating a flood of re-requests by the supplicant to the same AP for which it was denied access

To date, the behaviour of the supplicant is device specific. Some devices will mark any network for which an EAP-Failure is received as disabled requiring the user to manually reconfigure the network settings. If a network silently discards authentication attempts, then a device may repeatedly try to connect to the same network rather than try an alternative available network. Ideally, we would want some way for the 802.1x/EAP authentication to be able to differentiate between the different types of authentication/authorisation failures such that a device can act in the correct way. For example:

1. 802.1x authentication failed due to invalid user credentials
   Device should not attempt to connect to this network with these credentials again
2. Failed due to invalid AAA server
   Device should not attempt to connect to this rogue network
3. Temporary failure to contact AAA server
   Device should retry a number of times
4. Valid user credentials but access not authorised at this location
   Device should not retry at this particular AP

Currently, the EAP authentication standard RFC 3748 specifies EAP-SUCCESS (code 3) or EAP-FAILURE (code 4) as the result of an EAP authentication exchange. Alternatively, the AAA server may simply choose not to respond and terminate an authentication exchange silently. In either case, for an EAP-FAILURE or a silent termination, there is no means for the device to determine the reason for failure and hence what its subsequent behaviour should be.

EAP methods may also send EAP Notification messages which can be used to implement result indications and which can be sent prior to a Failure message. In RFC 3748 EAP Notifications are defined as providing a textual string to be displayed to the user; however, EAP Notifications may be redefined by particular EAP methods. In EAP-AKA/SIM (RFC 4186/RFC 4187) Notifications are used to pass result indications to the client to indicate why an EAP-SIM authentication failed; for example, missing attributes or unsupported versions. EAP SIM/AKA Notifications include a notification code which is a 16-bit number. The most significant bit is called the Success bit (S bit). The S bit specifies whether the EAP Notification relates to a failed authentication. The code values with the S bit set to zero (notification code values 0...32767) are used in unsuccessful cases. The receipt of a notification code from this range implies a failed EAP exchange, so the peer can use the notification as a failure indication. After receiving an EAP-Response/SIM/Notification for these notification codes, the server MUST send the EAP-Failure packet.

Some of the notification codes are authorization related, and hence, are not usually considered part of the responsibility of an EAP method. However, they are included as part of EAP-SIM because there are currently no other ways to convey this information to the user in a localizable way, and the information is potentially useful for the user. Examples of the failure notification codes are shown below:

0 General failure after authentication (implies failure, used after successful authentication)
1026 User has been temporarily denied access to the requested service (implies failure, used after successful authentication)
1031 User has not subscribed to the requested service (implies failure, used after successful authentication)
16384 General failure (implies failure, used before authentication)

EAP-TLS RFC 5216 encapsulates the TLS protocol within an EAP exchange as EAP Request/Response message pairs. Whilst EAP-TLS does not use the EAP Notifications in the way of EAP-SIM, it does allow for TLS-Alert messages to be sent from the server to the client using an EAP-Request message.

RFC 5216 states:
*The EAP server SHOULD send a TLS alert message immediately terminating the conversation so as to allow the peer to inform the user or log the cause of the failure and possibly allow for a restart of the conversation.*

The TLS alert message could be used to convey additional information about the reason for a Wi-Fi authentication failure prior to EAP-Failure. The TLS alert message types are defined in RFC 2246 and allow for issues such as certificate error, certificate revoked, access denied etc to be indicated to the client together with an alert level that indicates whether the alert is fatal to the authentication.

We can see that whilst some of the underlying EAP methods provide some means which could be used to indicate different types of 802.1x authentication or authorisation failure, there is no current explicit mechanism which would allow a device to differentiate reliably between the use cases identified above.

In particular, the difference between an authentication failure and an authorisation failure, that is, where a user's credentials are valid but they are not authorised to use this particular access point or network.

Interestingly, IEEE 802.11u introduces a number of new disassociation reason codes specifically to address the need to indicate:

a. User does not have a valid subscription
b. User is not allowed access at this location

The intention seems to be that an SSPN can indicate to the Wi-Fi access network that either of these cases apply during the authentication exchange. The Wi-Fi network will then send a disassociate message to the client station with one of the reason codes above. Note this is separate from the EAPOL authentication exchange and it is not specified whether an EAP-Failure is sent in these cases. The ability to indicate these use cases between the SSPN and Wi-Fi access network also depends on the ability for the authentication interface to provide the appropriate indicators/flags through, for example, custom RADIUS attributes. This interface is outside the scope of IEEE 802.11u and needs to be defined by another standards body such as perhaps Wi-Fi Alliance or the Wireless Broadband Alliance.

Note also that EAP is typically transported between operators encapsulated within Radius or Diameter protocols. Both of these protocols define standard message attributes which could also be reused to provide additional authentication/authorisation information above and beyond that defined within the EAP methods themselves,

| | Scenario description | Potential issues | Potential solutions |
|---|---|---|---|
| 22 | Device uses a roaming SSPN credential to authenticate to the AP but authentication fails due to:<br><br>Network error can't contact home AAA<br>Home AAA reject invalid credentials<br>Home AAA reject exceeded usage limit<br>Rogue AP<br>Visited AAA temporary no resource/capacity<br>Visited AAA network failure | No definition of correct device behaviour in these cases<br><br>Device may make unnecessary repeated attempts to connect causing load on the AP and AAA.<br><br>Device may invalidate credentials permanently due to a temporary network issue.<br><br>Poor device behaviour would make it more difficult to use authentication rejection to impose subscription usage limits. | Modifications to EAP reason codes and corresponding changes to 3GPP Sta/SWa interfaces |
| 23 | Device is in range of a rogue AP advertises itself as an HS2.0 AP supporting various SSPNs but rejects all authentication requests | This could result in devices removing user subscription credentials/settings resulting in the user no longer being able to connect to valid APs | |
| 24 | The user runs out of credit during a Wi-Fi session on one subscription, but has other subscriptions which are also valid on this AP. | How should the session be terminated, with a disassociation?<br><br>If so, how does the AP indicate that the device should not attempt to reattach with the same credentials?<br><br>How should the device switch to using another subscription? | |
| 25 | An access point decides to terminate the Wi-Fi session and sends a disassociate message; however, the device is still in range of this AP. | Should the device try the next best AP in range?<br><br>If no other APs in range, should it disable Wi-Fi and switch to cellular or should it wait and try and reassociate? | With an L-ANDSF or policy delegation: timing before reassociation would be provided (as how long it is allowed to override ANDSF policies). |

### Routing and QoS Scenarios

| | Scenario description | Issue | Potential solutions |
|---|---|---|---|
| 26 | How is 802.11u QoS mapping applied when serving multiple SSPNs at the same AP? | Should the AP apply all the QoS MAPs equally.<br>There are only 4 traffic classes over the air so there is no scope to have greater granularity in traffic classes. | |
| 27 | A device requires an access point that supports QoS mapping service to support VoIP. It is in an area with overlapping coverage some of which supports QoS mapping and some of which does not. | How is the QoS mapping service indicator included in the network selection rules?<br><br>At what point should AP functionality, for example QoS mapping support override RF metrics such as SNR? How would the criteria be specified? | |

# CONVERGENCE PROPOSALS/GUIDANCE/SUGGESTIONS

This section contains proposals that could help to close some of the identified gaps in the use cases above.

These proposals are the result of a joint BT and Alcatel-Lucent study and will be the basis for contributions/discussion papers to the relevant standard bodies or fora: 3GPP, Wireless Broadband Alliance, GSMA, Wi-Fi Alliance.

### Addition of Roaming Consortium IDs in ANDSF Policies

To date the ANDSF MO defined in TS 24.312 defines a prioritised access list that identifies WLAN networks based on:

- Access technology (WLAN)
- Access ID(SSID)
- Secondary access ID(HESSID)

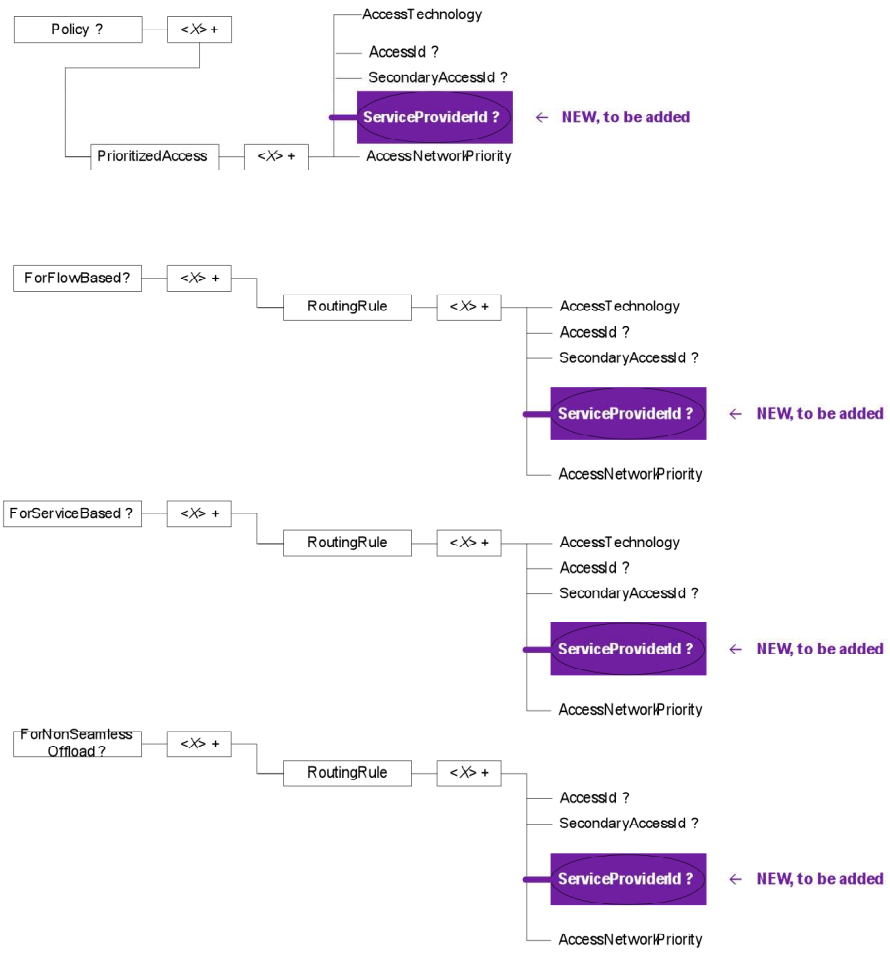
This differs greatly from Hotspot2.0 and 802.11u where what really matters is not the access identifier but the SSPN that can be reached through that access point.

As an MNO that has a partnership with a WISP roaming consortium may not know all SSIDs of that consortium and as commercial agreements may vary between different roaming consortiums, the following addition to the ANDSF MO in 24.312 would allow specifying policies such as:

- Priority 1: all Wi-Fi networks with SSID="Operator A SSID"
- Priority 2: any Wi-Fi network part of consortium C
- Priority 3: any Wi-Fi network part of consortium D

As illustrated in the figure below, a ServiceProviderId leaf can easily be added. This leaf can contain a roaming consortium Id as defined in 802.11u.

**Figure 7. Addition of Service Provider id in ANDSF MO**




This addresses scenario 8 in the section entitled “Subscriber with public Wi-Fi provided by Cellular Operator” (p20).

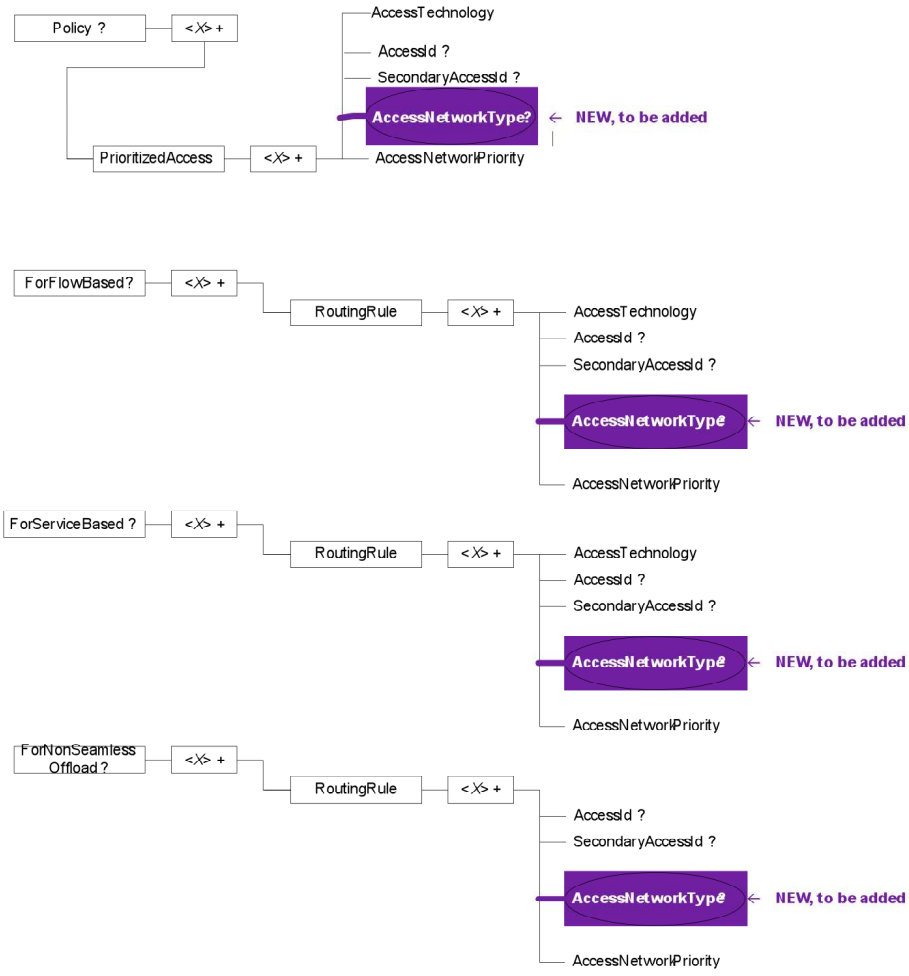
## Addition of Access Network Type in ANDSF Policies

An operator may need to distinguish policies for usage of residential Wi-Fi and for usage of hotspot or public Wi-Fi. Another use case for specific policies can also be the usage of Wi-Fi in corporate networks.

The current ANDSF MO does not allow for rules/policies that apply only to a given type of network. Furthermore, previously there was no automated way for the device to know that type. Now, thanks to information elements provided by 802.11u like Type of access network or Venue group/type, this information can be available in the device.

Hence the ANDSF MO could distinguish policies based on an access network type leaf that could, for instance, take the values “Residential”, “Carrier Hotspot”, “Enterprise”, “Public” or “Private”. A mapping with 802.11u Venue Group (Residential, Business etc.) could easily be defined in the Hotspot2.0 specification.

**Figure 8. Addition of access network type in ANDSF MO**



This addresses scenarios 6 and 7 in the section entitled “Subscriber with public Wi-Fi provided by Cellular Operator” (p20).

## ANDSF Policies Delegation

As detailed in the Network Selection Scenarios Summary Section (p20), the correct network selection choice may not only depend oncommercial agreements and/or availability of the network: QoS or load/congestion criteria may make a network more desirable than another.

This dynamic information can hardly be foreseen in advance within ANDSF policies. Were more dynamic information to be included in ANDSF, the sheer number of small Wi-Fi cells would pose scalability issues. It is unlikely to be beneficial for an operator to monitor the status of millions of access points from a centralised server, as policy updates would only be meaningful to a very small number of UEs (those located under the coverage of/nearby the access point) and because local conditions can change very fast based on interference, the number of users, etc.

A few additions to the ANDSF model could solve this, allowing ANDSF and Hotspot2.0 to complement each other for a solution that would both scale and allow the home operator to retain control over the device’s choice of network.

The proposal can be divided in two different flavours:

- Delegating some level of control to a local instance of ANDSF (ANDSF hierarchy) and/or
- Delegating authority to the roaming partner using the roaming partner protocol of choice.

The principle would be to allow the ANDSF to provide policies for the usage of a Local-ANDSF (L-ANDSF) or to delegate some level of authority to its WISP partner with parameters defining the scope of the delegation, how to avoid ping-pong effects and also to allow use of other protocols for fine tuning network selection decisions.

The ANDSF model defined in 3GPP TS 24.312 can be extended to provide the UE with instructions/policies of the operator regarding usage of a Local-ANDSF function.

The additional information to be added in the model could be:

1. Authorisation
2. Discovery/Addressing
3. Hysteresis to avoid too frequent inter-RAT handovers
4. Protocol

#### a. Authorisation

The authorisation information is provided by the ANDSF of the local PLMN to the UE and indicates to the UE whether usage of a Local-ANDSF or of another protocol provided by a roaming partner is allowed within a certain validity condition (place and time). When the validity conditions are met in such a case local policies provided by the L-ANDSF or by the roaming partner may override the usual ANDSF policies for the time specified in the hysteresis information.

This information could include which actions are allowed to be performed by the Local-ANDSF for example:

- barring the UE from the current access (or downgrading the priority of this current access)
- performing load-balancing between access points inside a same access network
- steering a UE from a non-3GPP network to a 3GPP network
- steering a UE from a non-3GPP network access to another non-3GPP access

**b. Discovery/Addressing**

This information indicates to the UE how it will find the Local-ANDSF if one is available and allowed.

It may correspond to:

- the FQDN or IP @ of the L-ANDSF
- or an indication on how this FQDN or IP @ may be fetched by the UE (for example, via 802.11u)
- or whether the L-ANDSF can be directly advertised by 802.11u (for instance, if based on 802.21 protocol)

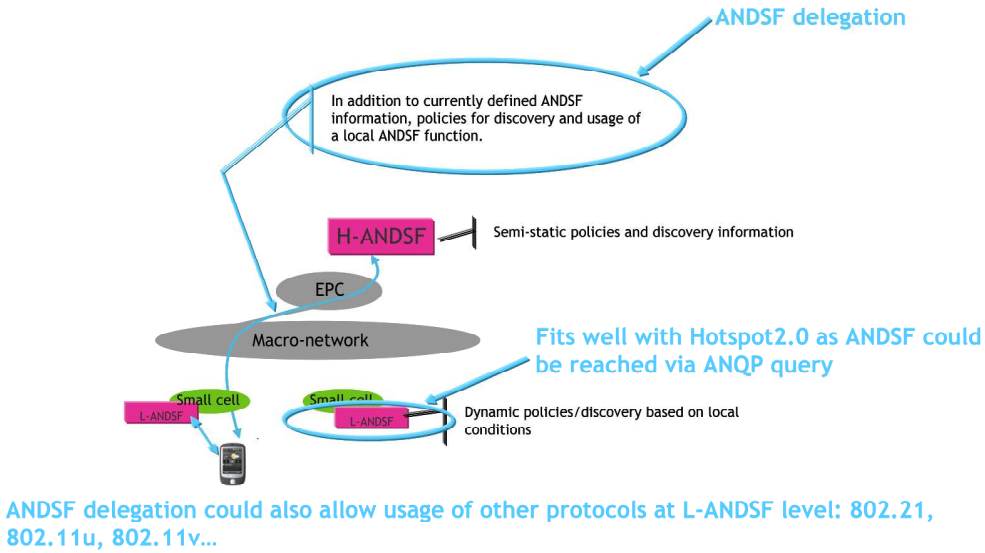
**c. Hysteresis**

Hysteresis information is provided by the ANDSF and allows avoiding the ping-pong effect of conflicting rules sent by the ANDSF and the L-ANDSF or the delegated authority. Hysteresis information gives limits to the time where the Local-ANDSF policy/delegated authority takes precedence over the global ANDSF policy.

**d. Protocol**

For cases where the WLAN network provider is different from the MNO and eventually provides roaming/offload to several different MNOs, it may be easier to rely on availability of other protocols (as ensured by Hotspot2.0 certification for instance) for access network discovery and selection. Depending on operator choices, the Local-ANDSF instance could be reachable via ANQP and use the current ANDSF MO or use similar functionality provided by other protocols like 802.21 or 802.11v (BSS transition mechanisms).

**Figure 9. ANDSF delegation to a local instance**




An example scenario out of many could be as follows:

MNO A has a Wi-Fi roaming partnership with WISP B. WISP B has deployed a Hotspot2.0 compliant Wi-Fi network.

MNO A ANDSF provides the UE with a policy to prefer B's Wi-Fi network but to also follow 802.11v indications of load when on B's network. Hence the delegation policy would be to use the Wi-Fi network only when load is below 70 percent as well as follow 802.11v-based load-balancing (BSS transition)

This addresses scenarios 18 and 19 in the section entitled "Subscriber with residential + public Wi-Fi + cellular subscriptions provided by the same operator" (p24), and scenario 25 in the Network Authentication Scenarios Section (p24).

**Figure 10. Example of ANDSF policy delegation**

- ISMP: Wifi preferred with SSID = MyPartnerHotspot
- Delegation policy
  - Allowed where SSID = MyPartnerHotspot
  - Addressing = L2
  - Protocol = 802.11v
  - Criteria = Load < 70%
  - Hysteresis = 20mn

## Improvements to Device Authentication Behaviour

We have seen in the Network Authentication Scenarios Section (p24) that whilst some of the underlying EAP methods providemechanisms to indicate different types of 802.1x authentication or authorisation failure, there is no current explicit mechanism which would allow a device to differentiate reliably between the use cases identified in this same section. In particular, the difference between an authentication failure and an authorisation failure, that is, where a user's credentials are valid but they are not authorised to use this particular access point or network. IEEE 802.11u defines new disassociation reason codes to differentiate these use cases but it is not clear how these disassociation messages relate to the EAP Success/Failure messages. It is also not clear whether devices are required to change their behaviour with respect to the disassociation reason codes.

More clarity in the expected device behaviour when confronted with a failed authentication due to either a rogue AP or a temporary loss of connectivity to the AAA server is needed. For example, we would suggest that a device should reattempt an authentication that silently fails but not reattempt when there is an explicit EAP-Failure response unless for example the HESSID is different.

In addition, at time of authentication clarification of how a device needs to build its NAI is required, particularly for Wi-Fi only devices that will not follow 3GPP TS 23.003 guidance on the topic.

This addresses scenario 22 in the Network Authentication Scenarios Section (p24).

## Greater Standardisation of SSPN Interface

IEEE 802.11u specification implies but does not define (that is, out of scope) an interface between a Wi-Fi access network and a home SSPN. This interface is used to convey a range of information between the Wi-Fi network and an SSPN, such as:

- User identification and authentication
- Accounting information
- Service authorisation, for example, credit limits, location restrictions, subscription service categories, access point location
- Advertising configuration and roaming information, for example, MNC/MCC, roaming consortium IDs realm
- Traffic policy enforcement, for example, quality of service configuration, gating control, traffic shaping rules

Indeed, IEEE 802.11u Appenex A identifies a number of specific information items that can be sent via the AAA protocol between the Wi-Fi access network and the home AAA server to aid in delivering per user service control. However, there is no formal mapping to either existing or new RADIUS/DIAMETER attributes and so no current means for this information to be exchanged in a standard way.

Authentication and accounting are typically already covered by existing WBA roaming protocols and similar protocols such as the STa interface defined in 3GPP TS 23.402. However, the remaining points require additional standards work to define how this information is transported between the Wi-Fi access network and the home AAA server via, for example, RADIUS/DIAMETER attributes.

There has been some standards work in this space already. For example, the QoS-Capability AVP defined by IETF RFC 5777 allows the transport of traffic classification filters and associated actions to enable the application of quality of service (QoS) rules. APN-Configuration Diameter attribute defined in 3GPP TS 29.272 allows the transport of service configuration information including:

- APN
- Authorized 3GPP QoS profile
- Statically allocated User IP Address (IPv4 and/or IPv6)
- Allowed PDN types (IPv4, IPv6, IPv4v6, IPv4_OR_IPv6)
- PDN GW identity
- PDN GW allocation type
- VPLMN Dynamic Address Allowed
- APN-AMBR

The Wi-Fi Alliance has defined Vendor Specific Attributes such as WISPr-LocationID that allow for the exchange of location information between Wi-Fi roaming partners.

As we can see, there are a variety of standards activities to extend the AAA protocols to enable service policies and configuration information to be exchanged between roaming partners, but greater consistency is required.

This addresses scenario 8 in the section entitled “Subscriber with public Wi-Fi provided by Cellular Operator” (p20).

## QoS Enabled Networks

IEEE 802.11u describes how a SSPN can define a QoS Mapping for IP QoS flags to be mapped into Wi-Fi Layer 2 QoS Flags on a per SSPN basis. This enables Wi-Fi devices and networks to more easily support services requiring guaranteed bandwidth or latency. For cellular service providers this QoS mapping mechanism potentially would allow the extension of 3GPP policies to the Wi-Fi access networks.

Unfortunately, the definition of how the SSPN should provide this information to a Wi-Fi access network is out-of-scope for IEEE 802.11u. In addition, there is no definition of how a Wi-Fi access network should handle Wi-Fi QoS mappings for multiple simultaneous SSPN on the same access point. It is unclear, for example, whether a SSPN would have a single QoS map for all subscribers or be able to provide per user QoS mappings. Wi-Fi admission control mechanisms will also interact with the SSPN requirement.

There is also an ongoing collaboration between the Broadband Forum and 3GPP which is also looking at the exchange of QoS policy information between network operators and again may provide a useful starting point for defining this aspect of the SSPN interface.

Whilst QoS Mapping support is a feature advertised by 802.11u enabled access points, there is no means currently within ANDSF to enable connection prioritisation of Wi-Fi access points with advanced QoS support over ones without it. This is an example of the need to be able to prioritise access networks by the functionality they provide.

This addresses scenarios 26 and 27 in the Routing and Qos Scenarios Section (p28).

## Support for Multiple Network Policies on Devices

In many of the use cases we considered, there may be multiple Wi-Fi subscriptions on the device, and in many cases, the device may not have been provided nor managed by any of the currently available network operators/SSPNs. Each SSPN may have a different roaming relationships and a different view of the relative priorities of the various roaming partners based on their own commercial imperatives. In these cases it is not clear that there is a single operator responsible for defining the network selection rules.

Current mechanisms for network prioritisation such as ones provided by ANDSF, assume a single operator, single subscription, and consequently, a single ANDSF policy. Clearly a Wi-Fi subscription provided independently of a cellular subscription will have different roaming priorities. Currently, at the Wi-Fi Alliance HS2.0 phase 1 specification there is no mechanism for the Wi-Fi subscription to define these priorities and no mechanism for multiple subscription network priorities to be reconciled into a single network selection decision. Phase 2 may deal with policy and priority but most likely will not address the reconciliation of multiple network priorities.

We propose that Wi-Fi SSPNs and cellular SSPNs adopt a consistent mechanism for the definition of network selection policies via, for example ANDSF ISMP, and that the user is able to define the relative priority of their network subscriptions, and consequently, the relative priorities of the ANDSF policies. A consistent mechanism such as ANDSF ISMP allows independent policies to be merged in a sensible way, supports the delegation of ANDSF proposed in the L-ANDSF model and allows OEMs to implement predictable network selection behaviour.

This addresses scenarios 15 and 16 in the section entitled "Subscriber with residential + public Wi-Fi + cellular subscriptions provided by the same operator" (p24).

## Importance of Device Certification Details

Key to the success of the Hotspot2.0 will be the ability for operators to rely on detailed certification of the device support for critical features like 802.1x, EAP authentication methods, the relevant 802.11u authentication features.

Particular attention should be given to the definition of the test scenarios and related use cases.

## Support for EAP-AKA' in Addition to EAP-AKA

From the list of credential types that need to be supported by devices that have SIM credentials (ANDSF Policies Delegation section – p31), the Hotspot2.0 is missing the EAP-AKA' (RFC 5448) which needs to be added.

## Conclusion

This paper has described the need for Heterogeneous Network Policies in a multi-operator environment. It has analysed how new standards like the 3GPP ANDSF function and the Hotspot2.0 initiative can complement each other to meet those needs whilst identifying a number of use-case scenarios where further standards work is required.

ANDSF is a cellular technology standard which allows an operator to provide a list of preferred access networks with policies for their use up to the granularity of a single IP flow or all traffic for a given PDN network (APN). IEEE 80211u and WFA Hotspot2.0 are Wi-Fi technology standards that allow devices to more easily discover Wi-Fi roaming relationships, determine access point capabilities and loading conditions, and more easily connect to Wi-Fi networks securely.

The combination of ANDSF and Hotspot2.0 is a particularly powerful enabler for a pain-free user experience across Wi-Fi and cellular networks. In particular, for cellular operators looking to offload data traffic onto roaming partner Wi-Fi networks, the improvements in Wi-Fi network selection and authentication offer significant improvements to the user experience and the ability of an operator to manage how different networks can be optimally used. However, as we show in this paper, there are many cases where enhancements to the current mechanisms will be required, for example, where there are Wi-Fi only operators or where the user has independent subscriptions from both a Wi-Fi operator and a cellular operator.

In our analysis we have identified some proposals for further discussion and outlined potential contributions to the relevant standard bodies that we believe could improve the user and operator experience of heterogeneous networks. Those proposals include:

- Improving consistency between Hotspot2.0 and ANDSF network naming and identification through the addition of Roaming Consortium IDs in ANDSF policies
- Enabling ANDSF policies to better exploit Hotspot2.0 information such as the access network type (residential, enterprise, public)
- Clarifications to Wi-Fi authentication mechanisms to differentiate between authentication and service authorisation failures, enabling devices to behave appropriately in failure conditions, and operators to provide differentiated subscriptions
- A new ANDSF policy delegation mechanism to enable the ANDSF infrastructure to refer devices to local ANDSF servers as a mechanism to cope with the increased range of networks and roaming partners that will be available in future

In these proposals we have attempted to build on the existing work within various standards bodies and attempt to identify opportunities for reuse and improved interoperability that will be required in a future multi-operator, multi-technology world.

# ANNEX A: 802.11U EXTENSIONS

## Extensions to Beacon Messages

A number of new optional information elements that may be added to the beacon messages are summarised below.

| | |
|---|---|
| Interworking | Information about the interworking service capabilities of an STA; for example, whether Internet access is available, whether ASRA is set and optionally includes the HESSID |
| Advertising Protocol | Contains information that identifies a particular advertisement protocol supported by the AP; for example, ANQP or IEEE 802.21 |
| Roaming Consortium | Contains information identifying the roaming consortium and/or SSP whose security credentials can be used to authenticate with the AP |
| Emergency Alert Identifier | Provides a hash to identify instances of the active Emergency Alert Service messages that are currently available from the network |

The existing Extended Capabilities Information Element is extended with new flags to indicate whether various IEEE 802.11u services are supported.

| | |
|---|---|
| Interworking | The Access Point supports IEEE 802.11u based interworking service |
| QoS Map | The station supports the QoS mapping service, see below |
| EBR | The station supports the Expedited Bandwidth Request service |
| SSPN interface | Indicates whether the AP supports an interface to SSPNs to allow user profiles, accounting information, traffic policies to be provisioned by the SSPN to the AP |
| MSGCF | Indicates whether the AP supports the IEEE 802.11u defined MAC State Generic Convergence Function. This function is responsible for collecting information from the MLME and SME to enable higher layer entities to manage mobility within an ESS. |

## (Re-)Association Message Changes

The Interworking Element is also added to the Association request message from a station to indicate its level of support for IEEE 802.11u. In addition a new

| | |
|---|---|
| QoS Map Set | Provides the mapping of the higher layer priority from the DSCP field used with the Internet Protocol to User Priority as defined by IEEE 802.11 |

## Access Network Query Protocol

GAS queries and responses can be formatted using a number of protocols. However, Access Network Query Protocol (ANQP) (defined as part of IEEE 802.11u) is likely to be the most commonly supported and is required for HS2.0 compliance.

ANQP defines a number of standard Information Elements which allow devices to query specific information such as location, cellular network roaming, emergency services support, authentication realms, etc. ANQP is also a two-way exchange enabling the device to provide its values for these information elements to the access point during the exchange.

| | |
|---|---|
| Query List/Capability List | Allows a device to determine the list of ANQP specific information elements that can be queried |
| Venue Name | Provides zero or more venue names associated with the AP |
| Emergency Call Number | A list of emergency phone numbers to an emergency responder (such as directed by a public safety answering point [PSAP]) that is used in a specific geographical area |
| Network Authentication Type | A list of authentication types when the Additional Step Required for Access flag is set to 1 |
| Roaming Consortium List | List of information about the Roaming Consortium and/or SSPs whose networks are accessible via this AP |
| IP Address Type | Information about the availability of<br>IP address version and type that could be allocated to the STA after successful association |
| NAI Realm List | A list of network access identifier (NAI) realms corresponding to SSPs or other entities whose networks or services are accessible via this AP |
| 3GPP Cellular Network Info | Cellular information such as network advertisement information, e.g., network codes and country codes to assist a 3GPP non-AP STA in selecting an AP to access 3GPP network |
| Geospatial Location | The AP's location in LCI format |
| Civic Location | The AP's location in Civic format |
| Location Identifier URI | An indirect reference to where the location information for the AP can be retrieved |
| Domain Name List | Provides a list of one or more domain names of the entity operating the IEEE 802.11 access network |
| Emergency Alert URI | Provides a URI for EAS message retrieval |
| Emergence NAI | A string, which can be used by a STA as its identity to indicate emergency access request |

## QoS Enhancements

In addition to improving the ability of devices to discover compatible Wi-Fi networks, IEEE 802.11u also provides extensions to the basic IEEE 802.11e QoS mechanisms to improve the ability of the Wi-Fi network to manage traffic for multiple SSPs. A Wi-Fi network as part of the roaming agreement can be provided with a QoS Mapping from the SSP which determines how downlink IP Traffic classes should be mapped to the over-the-air IEEE 802.11 QoS traffic classes.

In addition, a new QoS Action Frame message (QoS Map Configure) allows the AP to send this SSP specific QoS mapping definition to the device thereby enabling the device to apply the QoS mapping to uplink IP traffic.

# REFERENCES


1. IEEE Std 802.11™-2007
2. IEEE Std 802.11k™-2008 (Amendment 1: Radio Resource Measurement of Wireless LANs)
3. IEEE Std 802.11u™-2011 (Amendment 9: Interworking with External Networks)
4. IEEE Std 802.11v™-2011 (Amendment 8: IEEE 802.11 Wireless Network Management)
5. IEEE Std 802.21™-2008
6. 3GPP TR 21.905 Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications
7. 3GPP TS 23.003 Technical Specification Group Core Network and Terminals; Numbering, addressing and identification
8. 3GPP TS 23.402 Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses
9. 3GPP TS 24.302 Technical Specification Group Core Network and Terminals; Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3
10. 3GPP TS 24.312 Technical Specification Group Core Network and Terminals; Access Network Discovery and Selection Function (ANDSF) Management Object (MO)
11. 3GPP TS 29.272 Technical Specification Group Core Network and Terminals; Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol
12. 3GPP TS 33.402 Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses
13. Hotspot2.0 Specification v0.37
14. RFC 2246 The TLS Protocol
15. [RFC 3748 Extensible Authentication Protocol (EAP)
16. RFC 4186 Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)
17. RFC 4187 Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)
18. RFC 5216 The EAP-TLS Authentication Protocol
19. [RFC 5281 Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)
20. RFC 5448 Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')
21. RFC 5777 Traffic Classification and Quality of Service (QoS) Attributes for Diameter

# ABBREVIATIONS

| | |
|---|---|
| 3GPP | Third Generation Partnership Project |
| AAA | Authentication, Authorization and Accounting |
| Ack | Acknowledgement |
| ADSL | Asymmetric Digital Subscriber Line |
| AES | Advanced Encryption Standard |
| AN | Access Network |
| ANDSF | Access Network Discovery and Selection Function |
| ANQP | Access Network Query Protocol |
| AP | Access Point |
| API | Application Programming Interface |
| APN | Access Point Name |
| ASRA | Additional Step Required for Access |
| BS | Base Station |
| BSS | Basic Service Set |
| BSSID | Basic Service Set Identifier |
| CCMP | Counter Mode with Cipher Block Chaining Message |
| CM | Connection Manager |
| CMIP | Client MIP |
| CS | Circuit-Switched |
| DHCP | Dynamic Host Configuration Protocol |
| DL | Downlink |
| DNS | Domain Name System |
| DSCP | Differentiated Services Code Point |
| DSL | Digital Subscriber Line |
| EAP | Extensible Authentication Protocol |
| EAP-AKA | EAP-Authentication and Key Agreement |
| EAP-SIM | Extensible Authentication Protocol Method for GSM Subscriber Identity |
| EAP-TLS | EAP-Transport Layer Security |
| EAP-TTLS | EAP-Tunneled TLS |
| EAS | Emergency Alert System |
| EBR | Expedited Bandwidth Request |
| E-DCH | Enhanced Dedicated Channel |
| EDGE | Enhanced Data rates for GSM Evolution |
| EPC | Evolved Packet Core |
| ESS | Extended Service Set |
| e-UTRAN | Evolved-UTRAN |
| FA | Foreign Agent |
| FTTC | Fiber To The Curb |
| FTTP | Fiber To The Premises |
| GAS | Generic Advertisement Service |
| GERAN | GSM EDGE Radio Access Network |
| GGSN | Gateway GPRS Support Node |
| GPRS | General Packet Radio Service |
| GPS | Global Positioning System |
| GSM | Global System for Mobile communications |
| GTP | GPRS Tunneling Protocol |
| GTW | Gateway |

| | |
|---|---|
| HA | Home Agent |
| H-ANDSF | Home-ANDSF |
| HESSID | Homogenous Extended Service Set Identifier |
| HLR | Home Location Register |
| HO | Hand Over |
| HoA | Home Address |
| H-PLMN | Home Public Land Mobile Network |
| HS2.0 | Hotspot2.0 |
| HSDPA | High Speed Downlink Packet Access |
| HSPA | High Speed Packet Access |
| HSS | Home Subscriber Server |
| HTTP | Hyper Text Transfer Protocol |
| ICMP | Internet Control Message Protocol |
| IEEE | Institute of Electrical and Electronics Engineers |
| IFOM | IP Flow Mobility |
| IMSI | International Mobile Subscriber Identity |
| IP | Internet Protocol |
| ISDN | Integrated Services Digital Network |
| ISMP | Inter-System Mobility Policies |
| ISP | Internet Service Provider |
| ISRP | Inter-System Routing Policies |
| L2TP | Layer 2 Tunneling Protocol |
| L-ANDSF | Local-ANDSF |
| LAC | Location Area Code |
| LAN | Local Area Network |
| LB | Load-Balancing |
| LCI | Location Configuration Information |
| LTE | Long Term Evolution |
| MAC | Medium Access Control |
| MAG | Mobility Access Gateway |
| MAPCON | Multi-Access PDN Connectivity |
| MCC | Mobile Country Code |
| MIME | Multipurpose Internet Mail Extensions |
| MIP | Mobile IP |
| MLME | MAC sublayer Management Entity |
| MN | Mobile Node |
| MNC | Mobile Network Code |
| MNO | Mobile Network Operator |
| MO | Managed Object |
| MS-CHAP | Microsoft Challenge Handshake Authentication Protocol |
| MSGCF | MAC State Generic Convergence Function |
| MS-ISDN | Mobile Subscriber ISDN Number |
| MVNO | Mobile Virtual Network Operator |
| NAI | Network Access Identifier |
| NAT | Network Address Translation |
| NDIS | Network Driver Interface Specification |
| NGH | Next Generation Hotspot |
| NIC | Network Interface Card |
| OEM | Original Equipment Manufacturer |

| | |
|---|---|
| OMA-DM | Open Mobile Alliance – Device Management |
| OUI | Organizationally Unique Identifier |
| PAP/CHAP | PPP Authentication Protocol/Challenge-Handshake Authentication Protocol |
| PC | Personal Computer |
| PCC | Policy and Charging Control |
| PDN | Packet Data Network |
| PDP | Packet Data Protocol |
| PGW | PDN Gateway |
| PMIP | Proxy Mobile IP |
| PLMN | Public Land Mobile Network |
| PoA | Point of Attachment |
| PoS | Point of Service |
| PPP | Point-to-Point Protocol |
| PSAP | Public Safety Answering Point |
| QoS | Quality of Service |
| Radius | Remote Authentication Dial In User Service |
| RDF | Resource Description Format |
| RF | Radio Frequency |
| RFC | Request for Comments |
| RSSI | Receive Signal Strength Indicator |
| SCEP | Simple Certificate Enrollment Protocol |
| SCTP | Stream Control Transmission Protocol |
| SDO | Standards Development Organization |
| SGSN | Serving GPRS Support Node |
| SIM | GSM Subscriber Identity Module |
| SIP | Session Initiation Protocol |
| SNR | Signal to Noise Ratio |
| SSID | Service Set Identifier |
| SSL | Secure Sockets Layer |
| SME | Station Management Entity |
| SSP | Subscription Service Provider |
| SSPN | Subscription Service Provider Network |
| STA | Station |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| UE | User Equipment |
| UL | Uplink |
| UMTS | Universal Mobile Telecommunication System |
| URI | Uniform Resource Identifier |
| USIM | Universal Subscriber Identity Module |
| UTRAN | Universal Terrestrial Radio Access Network |
| V-ANDSF | Visited-ANDSF |
| VoIP | Voice over IP |
| V-PLMN | Visited Public Land Mobile Network |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WBA | Wireless Broadband Alliance |
| WiMAX | Worldwide Interoperability for Microwave Access |
| WISP | Wireless Internet Service Provider |

| | |
|---|---|
| WLAN | Wireless Local Area Network |
| WPA | Wi-Fi Protected Access |
| XML | eXtensible Markup Language |

For more information, please contact the authors by email at:

Barbara Orlandi, Alcatel-Lucent Bell Labs, barbara.orlandi@alcatel-lucent.com
Frank Scahill, BT Innovate and Design, frank.scahill@bt.com