Hotspot 2.0 / Passpoint

Seen from the Enterprise WLAN Engineer

aruba
a Hewlett Packard
Enterprise company

About me

- Herman Robers
- Background in network security engineering and consulting
- Joined WLAN industry: Aruba Networks in 2011
- Current: Aruba, a Hewlett Packard Enterprise company (the networking part of HPE)
- Twitter: @**hrwlan**
- ACCX, ACDX, CISSP certified
- Airheads community: Herman Robers
- Youtube: ABC Networking (youtube.com/c/ABCnetworking)
- Today: my personal opinion…

What is Hotspot 2.0 / Passpoint

Passpoint

GAS

802.11u

AQNP

EAP-AKA

OSU

OI

EAP-SIM

Hotspot 2.0

WisPr

HSS

HLR

SIM

uSIM

Evolution of Wi-Fi Hotspot Authentication Methods

2000 → 2012

Web Auth; UserName/ Password

Auto Portal (WISPr)

802.1X Auth (EAP-SIM, AKA, TLS, TTLS)

WPA2

UNTRUSTED Wi-Fi

TRUSTED Wi-Fi (Next Gen Hotspot)

Introduction of WISPr (2003)

- Wi-Fi Alliance (WFA) developed the **Wireless Internet Service Provider roaming (WISPr)** specification in 2003 to address the usability issues in Hotspots and automate the Hotspot login and authentication process
- WISPr was designed to be a “best practices recommendation” for authenticating to Wi-Fi hotspots using captive portal – and mechanisms to support roaming of users between different wireless internet service providers (WISPs)
- WISPr is not a standard – it was not advanced by WFA due to intellectual property rights infringement concerns
- Many public Wi-Fi hotspot providers continue to follow the WISPr specifications today despite some interoperability issues

DEAD

WISPr requires a software client that is customized by the SP

It uses an XML-file based login mechanism to improve usability for repeat users

WISPr defines the set of RADIUS attributes that must be supported by the operator

WFA Passpoint (Hotspot 2.0)

- In 2010 WFA began work on Hotspot 2.0 initiative with the goal of developing solutions for operators to leverage Wi-Fi to extend their network capabilities in a secure manner
- **Passpoint Objective**: Simplify access to public hotspot networks – making access more akin to roaming in cellular networks - while addressing the security and roaming issues between different operators
- Passpoint is the WFA program to implement Hotspot 2.0

WFA "Passpoint" certification available since mid 2012 - Based on Hotspot 2.0 specification

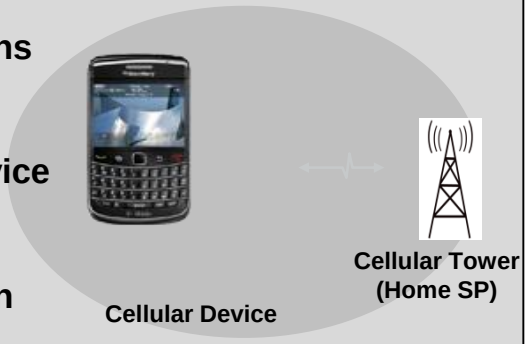
Passpoint– Making Wi-Fi Roaming Similar to Cellular Networks

Cellular Network

1. SP subscriber turns on his phone

2. Gets cellular service automatically

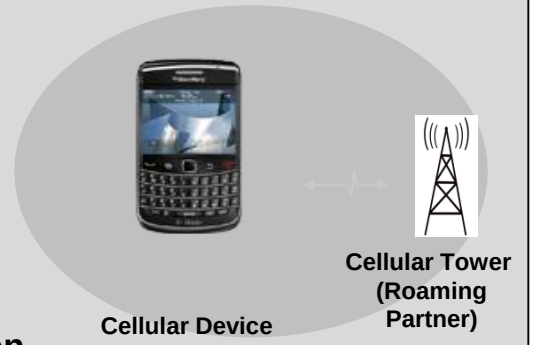
3. Secure connection



1. SP subscriber comes to roaming partner

2. Gets service automatically

3. Secure connection



Automatic and Secure

Wi-Fi Networks with Passpoint

1. Wi-Fi subscriber comes to AP of Home SP

2. Gets Wi-Fi service automatically

3. Secure connection

1. Wi-Fi subscriber comes to AP of Roaming Partner

2. Gets Wi-Fi service automatically

3. Secure connection

Automatic and Secure

Key Technology Elements in Passpoint Products

802.11u: Network Discovery and Selection

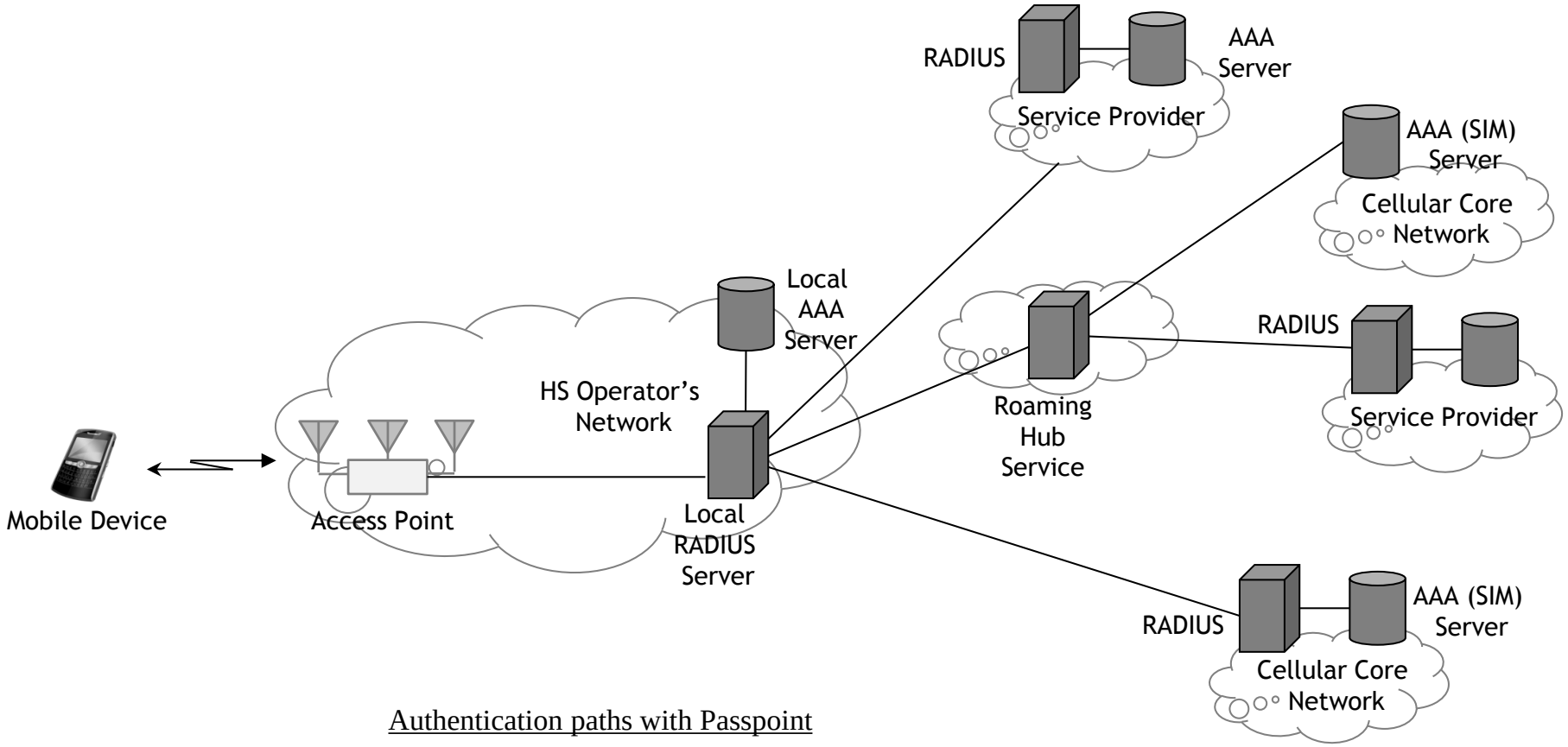
WPA2 - Enterprise ; Automated Login (SIM Cards); Strong Authentication (802.1X)

Automated Roaming accounting, Billing and Settlement

Pre-Association Presentation of Reachable Operators

WLAN Pro's don't typically care; Providers DO… Monetization of WiFi.

Authentication with Passpoint



Authentication paths with Passpoint

- WPA2-Enterprise is mandated with Passpoint and specifies 4 EAP types:
  - EAP-SIM
  - EAP-AKA
  - EAP-TLS
  - EAP-TTLS
- **The innovation in Passpoint is in allowing the mobile device to identify the service providers and capabilities of a hotspot before association and authentication, rather than the authentication itself**

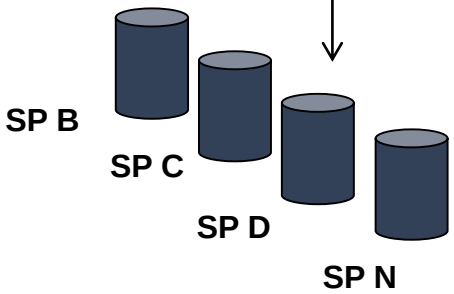
Hotspot 2.0 Sequence of Operation

Passpoint Mobile Device

Passpoint AP

Hotspot Operator Server (A)

Roaming Hubs



Network Discovery and Selection

Passpoint AP Advertises .11u support in Beacon; Provides Network Name via SSID element in Beacon

Device uses GAS to post ANQP query to AP for information on list of supported providers and access policies

AP provides HS Operator Domain Name and Network Access Identifier (NAI) Realm list (list of supported operators)

Automated Roaming

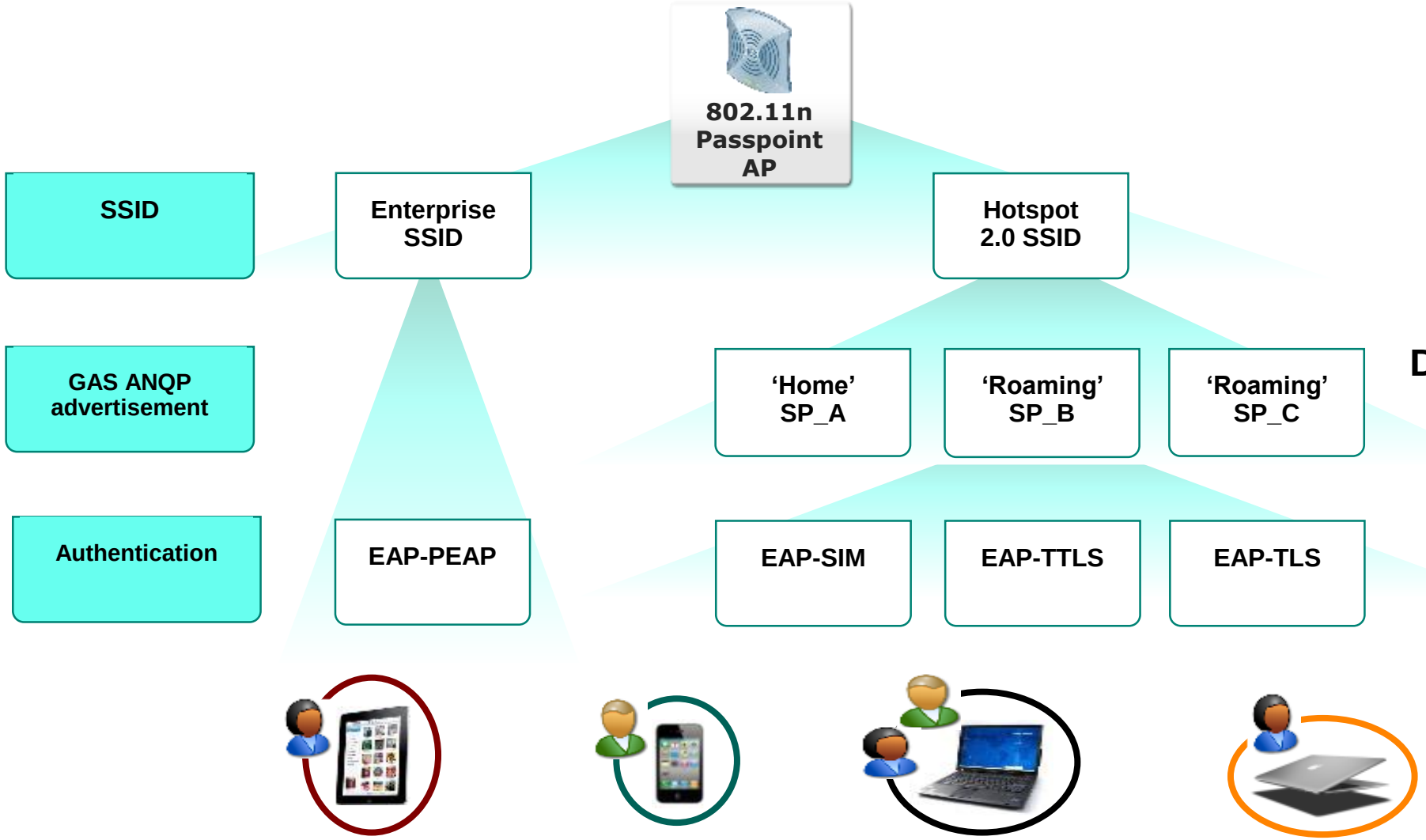
Device compares received Realm List with locally stored credential information to determine if it can authenticate to the network

Device uses operator policy (stored locally) to connect to the preferred network from an ordered list

Device authenticates to network using the credentials required by the selected operator (EAP-SIM, AKA, TLS, etc.)

WPA2 - Enterprise ; Automated Login (SIM Cards); Strong Authentication (802.1X)

HS2.0 Advertisement and Authentication

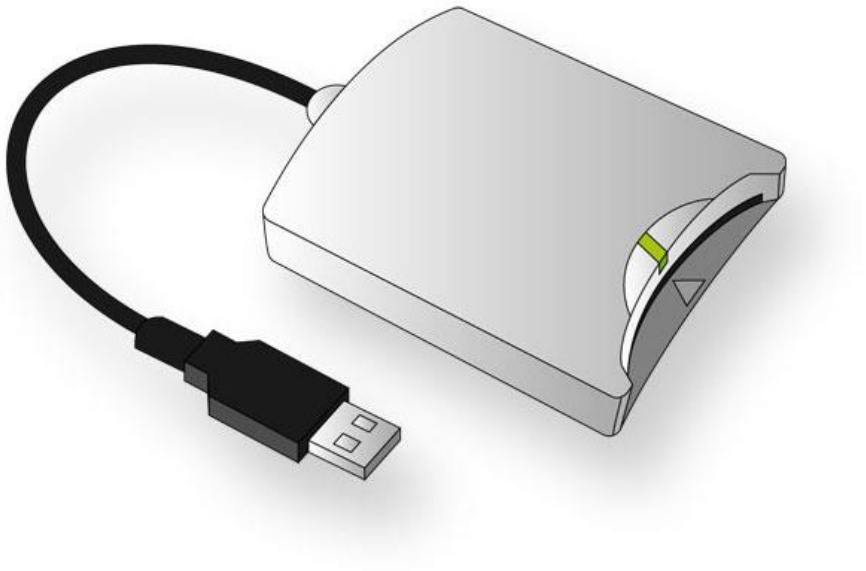


Decoupling the SSID and the services

EAP-SIM, EAP-AKA

– EAP-SIM = Authentication with a 3G SIM Card

– EAP-AKA = Authentication with a 4G uSIM Card



– You need to have access to the keys stored on the SIM in order to do an authentication (control the SIM)

– Those keys are in the provider HLR (Home Location Register)

– Only useful in provider environments!

– Not supported on all phones…

– … and not on non SIM devices like laptops, non 3G/4G tablets

– FreeRADIUS ‘supports’ EAP-SIM, however that is only when you have some challenge-responses from the SIM and it will do authentication only on those challenge-responses.

– I could not make my phones authenticate successfully with recent FreeRADIUS in lab. Followed: http://irq5.io/2013/12/23/implementing-eap-sim-at-home/

Roaming With Hotspot 2.0

- Similar to Cellular Roaming that provides access to subscribers outside of their home operator network, Wi-Fi Roaming allows operators to increase their coverage footprint by having roaming agreements with other Hotspot operators (partners)

- The framework for Wi-Fi Roaming reuses the network interfaces and business processes used for Cellular Roaming:
  - The subscriber is authenticated via the Home Operators subscriber database (HLR/HSS)
  - Using Data Clearinghouse / Hubs / Roaming Exchanges for billing
  - Using web portals to select and control roaming partners and monitor roaming usage

- **Roaming Consortium: has connections to many Home Operators**

Roaming Exchanges allow operators to easily connect with multiple roaming partners through a shared network

Mitigates the need for establishing direct connections with individual partners

Roaming Consortium Element

Element ID	Length	Number of ANQP OIs	OI #1 and #2 Lengths	OI #1	OI #2 (optional)	OI #3 (optional)

- Roaming Consortium Element is in Beacon and Probe Response frames
- The mobile device uses information in this element to determine if it has the required credentials for any of the available Wi-Fi networks
- The RC Element provides OI (**Organization Identifier**) for the Hotspot Owner and the top 2 Service Providers that have roaming agreements with the Hotspot Owner/ SP
- Other available SP information (beyond the top 3) is available through GAS-ANQP Query
  - The number of additional OI's available is indicated in the "Number of GAS-ANQP OI's" field
- If the mobile device recognizes the OI, it attempts association using security credentials that corresponds to that OI

Some practical issues with Passpoint (in the Enterprise)

– You need to pre-configure the device (phone) for Passpoint
  -> Only really in Cellular provider environments

– You need to have devices that support EAP-SIM/EAP-AKA
  -> In many countries, providers are locked to devices; in many European countries you can run any phone on your cellular subscription. For example my Nexus 5 does not support EAP-SIM; unsure about other devices.

– This resulted in less take-off than expected.

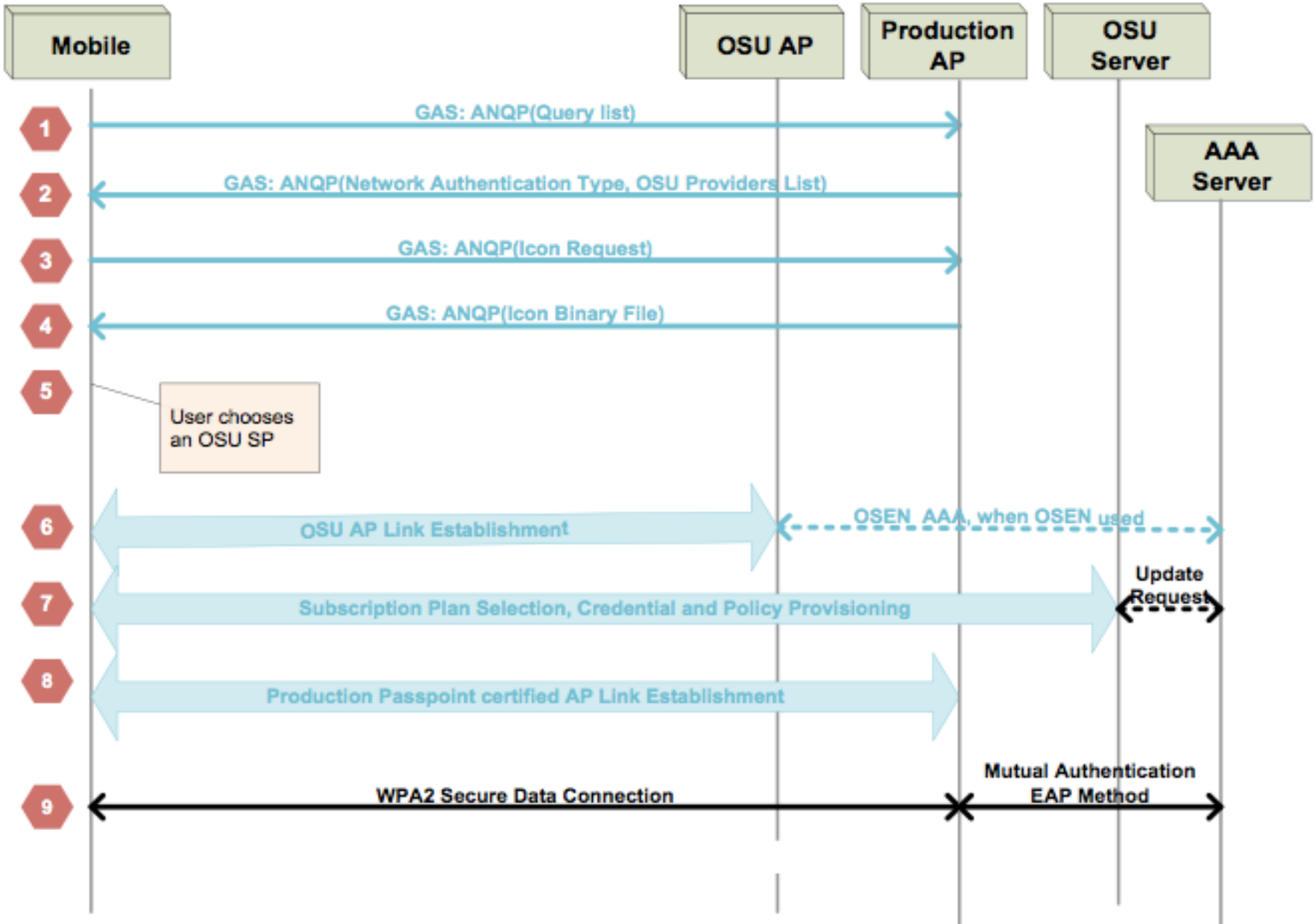
– Serice Provider focused.

Life is it better with PassPoint Release 2?

Addresses the provisioning nightmare:

- Provisioning – and standardizing - security credentials and network selection policies on mobile devices
- PassPoint Release 2 capable devices will have support for a UI that indicates availability of subscription service from a particular SP (and the provisioning of credentials)
- The credential provisioning sequence is launched when the user clicks on the SP icon
- Credentials can be:
  - User name / password (chosen by the user or provided by SP)
  - X.509v3 certificate provided by SP (issued at the PassPoint capable AP)
  - Pre-provisioned client cert (issued by the SP and installed using any out of band methods)
- The **Online Signup (OSU) Server** is a portal set up by the SP to facilitate the provisioning of credentials (and network selection policies)
  - Uses Open Mobile Alliance – Device Management (OMA-DM) Management Object (MO) to send the provisioning data to the connection manager on the device

HS 2.0 R2: OSU Message Exchange Flow



Summary

– Passpoint is WFA standard deploying HS2.0

– Automatic discovery (802.11u, GAP, ANQP)

– WPA2 Enterprise

– EAP-SIM = 3G SIM module authentication

– EAP-AKA = 4G SIM module authentication

– Device provisioning challenge

– Device support challenge

– Passpoint 2: OSU = Online Sign-up protocol

– Service provider…

– Useful in Enterprise? T.B.D.