Ruckus
Simply Better Wireless.

white paper

Hotspot 2.0 Release 2

ACCELERATING THE MOVE TO AUTOMATIC AND SECURE ROAMING WHEN USING WI-FI TECHNOLOGY

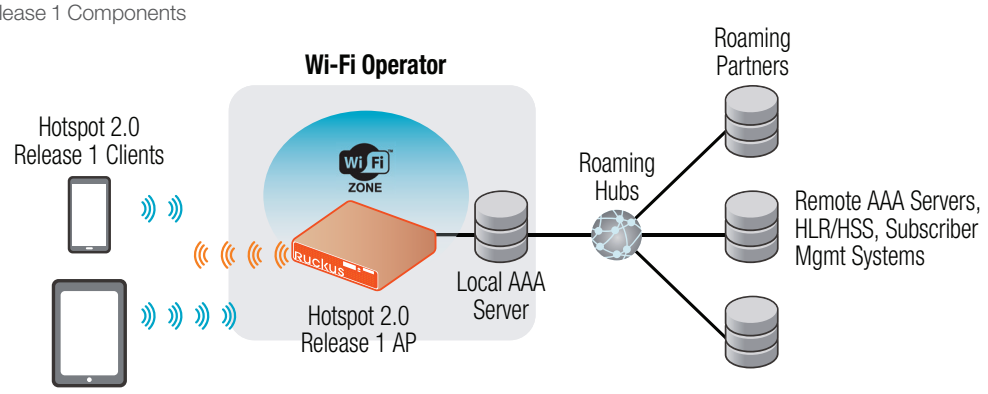
Introduction

Hotspot 2.0 Release 2 expands and improves upon the considerable innovations introduced with HS2.0 Release 1, which was based on the IEEE 802.11u standard. Release 1 introduced new capabilities for automatic Wi-Fi network discovery, selection, and 802.1X authentication all based on the Access Network Query Protocol (ANQP). With Hotspot 2.0, the client device and access point exchange information prior to association using ANQP. The access point advertises the "backend" service providers (SPs) who can process authentication requests that are reachable from this hotspot. The client than checks to see if it possesses a credential for one of those SPs, and if it does, it proceeds to associate and then authenticate to the AP using 802.1X and the provisioned credential. Supported client credentials include SIM cards, USIMs, X.509 certificates and username/password pairs. Each credential is associated with a specific EAP type. The primary benefits of Release 1 were automating the connection experience at hotspots where the client credential was accepted and providing a secure, encrypted airlink for public Wi-Fi. A secondary benefit is the ability to support multiple roaming partners over a single SSID, with SSID proliferation becoming a big issue for operators looking to expand their footprint through roaming relationships.

Hotspot 2.0
Release 2

ACCELERATING THE MOVE TO AUTOMATIC AND SECURE ROAMING WHEN USING WI-FI TECHNOLOGY

Figure 1: Hotspot 2.0 Release 1 Components



Release 2 is largely focused on standardizing the management of the credentials; how they are provisioned, how they are stored on the device, how they are used in network selection, how long they are good for, etc. Some of these capabilities aren't applicable to cellular credentials (SIM/USIM), as those are provisioned by the home mobile network operator (MNO) and are themselves the stored credential. But what about all those Wi-Fi only devices, how do we get them provisioned for service (and perhaps even linked to the subscriber's cellular data account)? And what if the service provider wants to apply some policy as to how its credential may be used (including the cellular credentials)? How do we expire a credential after a certain amount of time or usage? What do we do if a device submits a credential that has expired? And how can we do all of these things in a manner that preserves the security of the subscriber and their credential? Well, those were just the issues that the smart folks in the Wi-Fi Alliance's® Hotspot 2.0 Technical Task Group set out to address with Release 2.

We need to make SmartPhones smarter

Until Release 2 there was no standard format for managing a Hotspot 2.0 credential on a client device. Depending upon the OS or manufacturer, a text or XML file was typically used, but these might have different naming conventions, syntaxes, and locations within the file system. Release 2 leverages the Open Mobile Alliance's Device Management (OMA-DM) framework, which provides a standardized XML tree structure within which different kinds of information can be stored in a consistent manner. Release 2 specifies a new PerProviderSubscription Management Object (PPS-MO), which is one or more of the branches in the OMA-DM tree containing all of the information related to the Hotspot 2.0 credentials on the device. The credentials themselves may be stored in the PPS-MO (e.g. a username/password pair), or they may be located elsewhere on the device (e.g. a SIM or X.509 client certificate) and referenced within the PPS-MO. However, the PPS-MO doesn't just contain the credential information; it also standardizes the storage of some associated Release 1 parameters and introduces a whole range of new ones. Here are a few examples of the type of information stored within the PPS-MO for a given provider's credential:

Table 1: Release 1 standards and new introductions with release 2

TABLE 1

Release 1	Release 2
Credential (or Credential Pointer)	Preferred Roaming Partners
Home Provider Domain	SSID Blacklist for Autonomous Selection
Roaming Consortium OIs	Home Provider AAA Server Trust Root
NAI Realm and/or PLMN ID	Subscription Update Parameters
Required TCP and UDP Services/Ports	Usage Limits (Time or Data)

It's important to understand that the credential information and associated parameters for each provider are being stored in a separate branch of the PPS-MO tree. Further, only the provider who provisioned the credential is allowed to modify any of the parameters for that credential. So, a SIM credential branch from your cellular provider might contain preferred roaming partners and blacklisted SSIDs that apply when using EAP-SIM, while a username/password credential branch from your cable operator could contain a different set of policies to follow when using that credential with EAP-TTLS. Consistent with Release 1, Release 2 upholds the mobile user's preference as the ultimate decision maker for network selection, providing the ability for the user to prioritize multiple subscriptions/credentials.

Hotspot 2.0
Release 2

ACCELERATING THE MOVE TO AUTOMATIC AND SECURE ROAMING WHEN USING WI-FI TECHNOLOGY

We need a few New Backend Servers

With Release 1, the only supporting servers required were the AAA servers providing the client authentication, or perhaps acting as gateways to a mobile operator's Home Location Register (HLR) for EAP-SIM authentication. Release 2 adds a number of new server elements in order to support service registration, credential provisioning, credential management, and ensure the security of the client and credentials. Here's an overview of these new server elements:

- Online Signup (OSU) Server – used to register new users for service and provision them with a credential.
- Policy Server (PS) – used to provision network detection and selection policy criteria for the provider's issued credential.
- Subscription Remediation Server (SubRem) - used to correct any issues with the issued credential, policy or subscription, and also to renew prepaid type credentials.
- CA/PKI – used to generate and issue client certificates if TLS authentication will be used. All Release 2 clients receive Trust Roots that link to the Wi-Fi Alliance's® PKI, meaning that clients can validate all Release 2 server components, and even the provisioning WLAN itself, before they've been provisioned with a credential of their own.

Note that these are logical entities and could be implemented on separate platforms or in a single box, perhaps even combined with the AAA server.

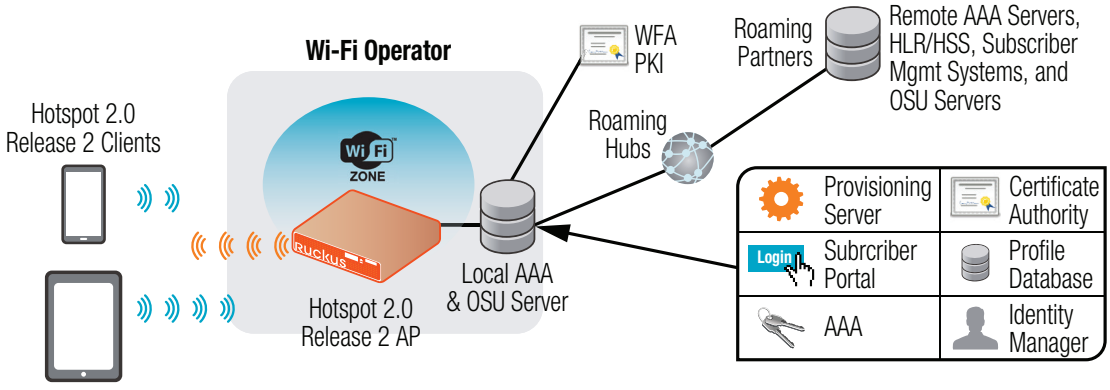
So how does it work?

A Release 2 client will see the Release 2 support in the Hotspot 2.0 indication element of the APs beacons and probe responses. The client then sends an ANQP query to the Release 2 AP. In the ANQP response, the AP indicates that Online Signup services are available and lists the OSU providers that are reachable from this hotspot. Since the client does not have a valid credential associated with this hotspot operator, or any of its roaming partners, it does not proceed to automatically associate and 802.1X authenticate. Instead, while it is still in the pre-association phase the user will be notified that Online Signup services are available. If the user elects to sign up, they will be presented with a list of the available Online Signup providers. The list is typically displayed as an icon, title, and description for each operator. The icon is actually embedded within certificate issued to the OSU server, thus ensuring that clients don't connect to "rogue" provisioning systems. Remember that everything described so far has happened while the client is not yet associated to any WLAN.

At this point, we should detour to discuss a new type of WLAN that is being introduced with Release 2. The OSU Server-only authenticated layer 2 Encryption Network (OSEN) is similar to the trusty old RSN, with the striking exception that OSENs only require authentication of the servers and expect that the client will remain anonymous during the session. OSEN is used exclusively as an option for the OSU WLAN, and is prohibited from being used in production WLANs. The other option for the OSU WLAN is to use Open Authentication. If OSEN is used, it is encrypted using Anonymous EAP-TLS, which again only authenticates the server/network and not the client using the PKR trusts. The intent is to ensure that the client is connecting to a valid/trusted OSU WLAN and that the registration and provisioning servers are authenticated. In order to accomplish this, there will be new Public Key Infrastructure (PKI) root trusts loaded into Release 2 clients. These will be used to validate OSU servers and the OSU WLAN if the OSEN option is used.

Once the user selects an OSU provider from the list, the connection manager on the device will connect to the OSU WLAN (Open or OSEN). It then triggers an HTTPS connection to the OSU server URI, which was received with the OSU providers list. The client validates the server certificate to ensure it is a trusted OSU server. At this point the client will be prompted to complete some

Figure 2: Hotspot 2.0 Release 2 Components



Hotspot 2.0
Release 2

ACCELERATING THE MOVE TO AUTOMATIC AND SECURE ROAMING WHEN USING WI-FI TECHNOLOGY

type of online registration through their browser – this could be anything from registering as an existing subscriber to purchasing prepaid access for a few hours. When they successfully complete the registration, they will be pushed a credential, associated parameters and, optionally, the policy to apply for that credential. Release 2 specifies that this secure communication between the provisioning servers and the clients can be accomplished with either SOAP-XML or OMA-DM messages over HTTPS. These messages map to the PPS-MO structure, and the information is stored in the management object on the client. Finally, now that the client has a valid credential for the production HS2.0 WLAN, it disassociates from the OSU WLAN and connects to the HS2.0 WLAN using the standard ANQP mechanisms. The connection manager also factors any configured policies into its selection decisions when utilizing the credential. From then on, the credential provider can use this framework to update the credential, policy or subscription of the device by indicating via RADIUS messaging that the client needs to contact one of the provisioning servers. Additionally, the client also can track parameters stored it its PPS-MO, such as update intervals, subscription expiration, or data usage limits, and automatically contact the appropriate subscription or policy server when an update or renewal is needed. The provisioning and management of credentials and policy is critical to ensure that Hotspot 2.0 services are available on all devices and that operators have

What's Next?

The Wi-Fi Alliance held a formal launch event for Release 2 in October of 2014 in conjunction with the Wireless Broadband Alliance's Wi-Fi Global Congress at the Palace Hotel in San Francisco. Ruckus was honored to perform the public demonstration of Release 2 at the launch event. The WFA also announced that Ruckus' OSU server suite is one of two selected for the Passpoint Release 2 Certification Testbed. Ruckus also issued a press release announcing the Release 2 certification of our SmartCell Gateway controller and ZoneFlex 7372 Access Point. On the client side, Samsung already has two models of the Galaxy S5 that have been certified, there are a number of certified chipset reference designs available from companies like MediaTek, Broadcom, Qualcomm Atheros, and Marvell, and Intel has also received certification for the 7260.HMWG adapter.

Figure 3: Hotspot 2.0: Status Check

Wi-Fi Operator	Phase 1 (~2014)
• Automatic • Secure	• Internal Users • Contract Customers • Apple Focused (largely)
Release 2	**Release 2 (~2015)**
• Online SignUp • Operator Policy • Device Standards	• Internal and Roaming Users • Contract and PayGo • Apple and Android

The WBA is planning its Next Generation Hotspot (NGH) Phase 3 trials, which will be based on Hotspot 2.0 Release 2. We expect a number of operators to participate in the NGH Phase 3 trials and some to conduct their own private trials. Commercial deployments will follow.

Ruckus®
Simply Better Wireless.

Ruckus Wireless, Inc.
350 West Java Drive
Sunnyvale, CA 94089 USA
(650) 265-4200 Ph \ (408) 738-2065 Fx

www.ruckuswireless.com