The user then selects a subscription type, and perhaps enters credit card numbers, and that information is sent securely back to the OSU server, which then issues and returns credentials in the form of an X.509 certificate or username-password. The final act is to automatically install these credentials on the mobile device as a secure authentication profile special to that service provider and including key Passpoint identifiers such as the service provider NAI realm.

Now the device will return to the Passpoint SSID with good credentials and in the future will automatically connect to any access point advertising Passpoint reachability to that service provider, as if the credentials had been entered manually, but without the same degree of user intervention.

Since many subscriptions added by OSU will be limited-time, and for other eventualities, there must be a complementary service that deals with mobile devices connecting to a network with credentials that were once valid but have now expired. The service provider handles this by rejecting the authentication attempt and redirecting the device (via a URL) to the Remediation Server (usually co-located with the OSU server). The Remediation Server uses a secure protocol to inform the user that the subscription or credentials are no longer active, and usually prompts for, and performs, a subscription renewal or pushes new credentials.

The final function in Passpoint v2 is a Policy Server. This is usually a function of the OSU server and can be used during online sign-up to push policy profiles to the mobile device. Most available policy preferences deal with network selection. For instance, when a device can see many available hotspots, policies help it establish priority for connection, based on home-or-visited service provider, current load, backhaul bandwidth (advertised over ANQP) and other parameters. Many service providers have preferred roaming partners which can vary by geography so policies can become quite complex.

Authentication to remote service providers

Despite its focus on authentication and authenticator choices and capabilities, Passpoint makes no changes to authentication protocols. The new information in the beacon and ANQP allows the mobile device to determine if a particular hotspot has connections to a service provider can authenticate it, given its choice of credentials, and to choose between hotspots if more than one match exists. But at the end of the hotspot discovery and selection phase, the Passpoint involvement is over, and the mobile device initiates a 'normal' authentication in the same way as it does today.

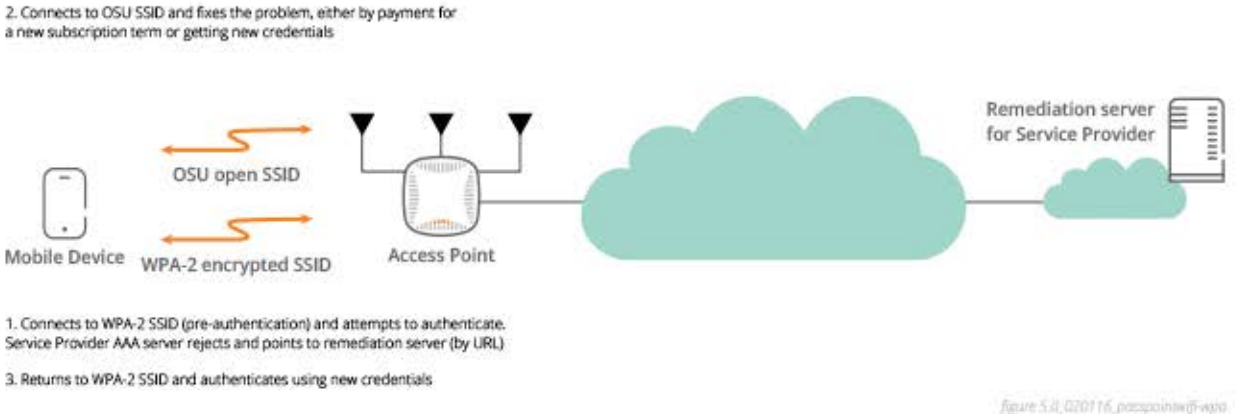

Figure 5. Remediation server associated with a Passpoint WLAN (simplified for clarity)

Passpoint mandates WPA2-enterprise, specifying four EAP types within WPA2-enterprise that are already exercised as part of Wi-Fi Alliance testing: 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. We will continue here with the authentication phase because it's an integral part of the hotspot experience.

When ANQP returns a list of reachable service providers ready to authenticate clients, it optionally attaches an authentication protocol to each. The EAP types mandated in Passpoint:

- EAP-SIM and EAP-AKA are such close cousins they are identical from our Wi-Fi viewpoint. They take credentials stored in the SIM (or USIM) card on a cellular device, and use them to authenticate with the AAA server in the cellular network which issued the SIM. In essence it's the same as authenticating a cellphone on a cellular network, but the information is carried by the 802.1X protocol in WPA2-enterprise.
- EAP-TLS is an existing EAP type that relies on X.509 certificates to authenticate the network to the client and vice versa. No extra userid or password is required.
- EAP-TTLS uses an X.509 certificate on the server, but the client authenticates using a userid/password combination.

Generally we expect cellular operators to use EAP-SIM and EAP-AKA, as they already issue SIM cards and have the matching authentication infrastructure. Common authentication also allows operators to keep track of users and devices as they move between the cellular network and Wi-Fi. Organizations that don't issue SIM cards will use one of the other methods. EAP-TLS is attractive because it uniquely identifies the device using a certificate, and doesn't require any user configuration (setting the userid/password) but generating large numbers of certificates and installing them on devices (and eventually revoking them) can be cumbersome. EAP-TTLS is the default password-based authentication.

When the Passpoint hotspot reports reachable service providers, the field showing available EAP types is optional. Indeed, it should not normally be required, as the mobile device should be pre-provisioned with a list of service providers, their names or realms, and the respective EAP-type and credentials. Thus the EAP-type information should be redundant, as the device already associates authentication type and service provider address.

END-TO-END ARCHITECTURE WITH PASSPOINT

Passpoint enables easy access to public networks by providing information and protocols to assist in discovering and selecting a service provider. After hotspot network selection, the mobile device authenticates, and it is then connected to the Internet or other networks. In this section we discuss the networks that support the authentication and network connection phases. Both of these are outside the Passpoint specifications, but they must be considered by hotspot operators and service providers.

Authentication networks are likely to be quite complex – we show a representative diagram below. All authentication traffic from a Passpoint hotspot using WPA2-enterprise is carried over 802.1X, with RADIUS connections.

As we follow the flow of authentication traffic, it is likely that it will first be routed to a local RADIUS server owned by the hotspot operator. This will allow authentication of the operator's own subscribers, but for roaming users it will act as a proxy and a monitor point for billing and accounting data – if the hotspot operator is authenticating subscribers for other service providers, it will want its own record of this data.

The local proxy RADIUS server will terminate a number of IPSec tunnels, via which authentication traffic will be directed to roaming partners. In some cases this roaming may be a peer-to-peer relationship, as shown in the diagram, with the RADIUS traffic going directly to a partner where it will may be terminated, or converted to DIAMETER to connect to large core networks. Incidentally, this proxy server will also be required to examine mobile device authentication requests and route them to the correct roaming partner, a function that may become complex as the number of roaming partners increases.

However, we believe that Passpoint will broaden the role of existing roaming hub or roaming exchange bureaux. These organizations provide a service where a hotspot operator can reach a large number of roaming partners via a single connection. They can direct the authentication stream to the appropriate service provider, and can also take care of billing and accounting for settlement. As the number of service providers and hotspot operators increases, the number of possible roaming relationships will increase exponentially and the functions provided by roaming hubs will become indispensable.

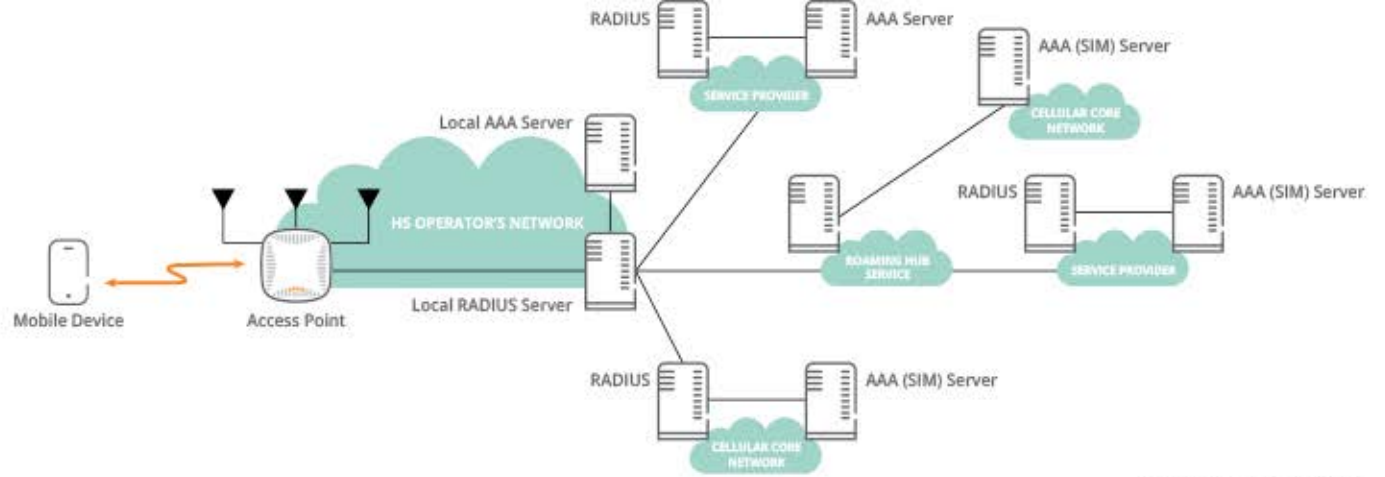

Figure 6. Authentication paths with Passpoint

It is clear that although the authentication, billing and accounting architecture and RADIUS attributes are out of scope of the Passpoint certification, they are essential for a smoothly-functioning hotspot roaming relationship. The Wireless Broadband Alliance and other organizations are working to provide guidelines in this area, as there is currently no universal agreement on required RADIUS attributes for hotspot roaming.

While authentication networks may be extensive and complex, the path followed by data-plane traffic is likely to be much simpler. In most cases, the mobile device will be connected directly to the Internet, probably right at the hotspot's backhaul connection. This is the way most service providers and most subscribers like to work today. However, there will always be circumstances where alternate arrangements are required. Some service providers want subscribers to be connected back to their own network, either because they need to deliver 'walled-garden' services, or to maintain seamless handovers between cellular and Wi-Fi connections, or to monitor users' traffic for other reasons. It is possible to achieve this, as we show in the diagram below. The selection of appropriate network routing can be driven by RADIUS responses from the authenticating service provider.

Corporate networks also need special treatment, but are unlikely to get special routing assistance from hotspot operators and service providers.

HOTSPOT SECURITY WITH PASSPOINT

Current hotspots incorporate relatively weak security so Passpoint improves matters in several areas – mostly using existing Wi-Fi techniques.

The most significant improvement is to mandate WPA2-enterprise for Passpoint hotspots. This implies mutual authentication and strong over-the-air encryption. Whichever EAP-method is used, the access point (or service provider) must identify itself to the mobile device and vice versa. When authentication is complete, unique keys are

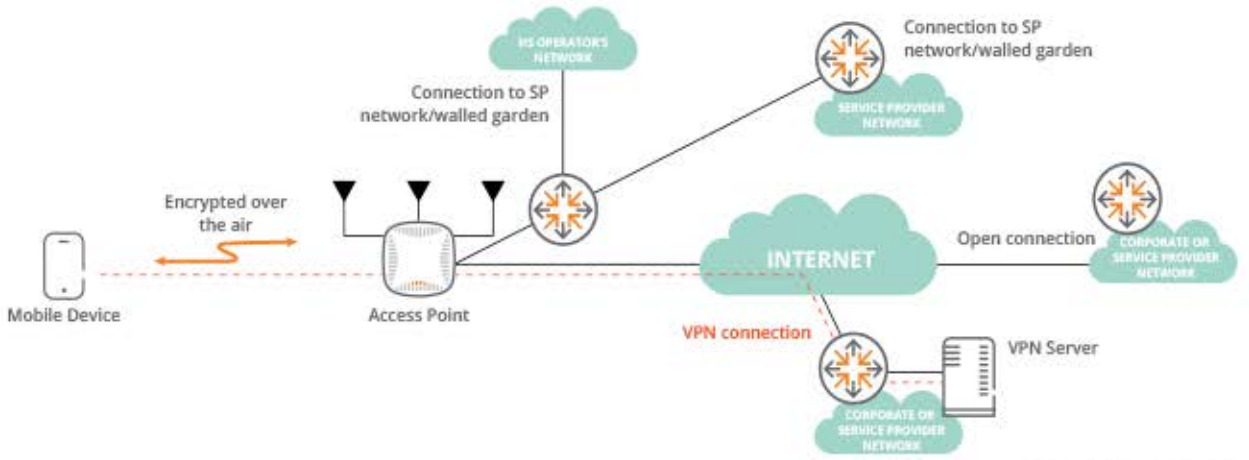

Figure 7. Data paths with Passpoint