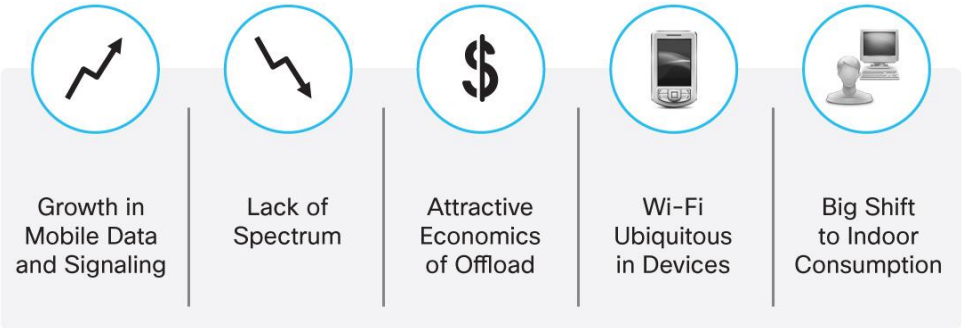
White Paper

Service Provider Wi-Fi: Authorization Options for the Mobile Network Operator

Introduction

Several trends in the market are causing operators to incorporate small cell solutions into their network infrastructure plans. Service Provider Wi-Fi is one approach to meeting such a demand, taking advantage of the near-ubiquitous availability of Wi-Fi in the latest smartphones, the worldwide availability of globally harmonized unlicensed spectrum, and the shift to consuming most mobile data from indoor locations (Figure 1).

Figure 1. Service Provider Wi-Fi Market Trends



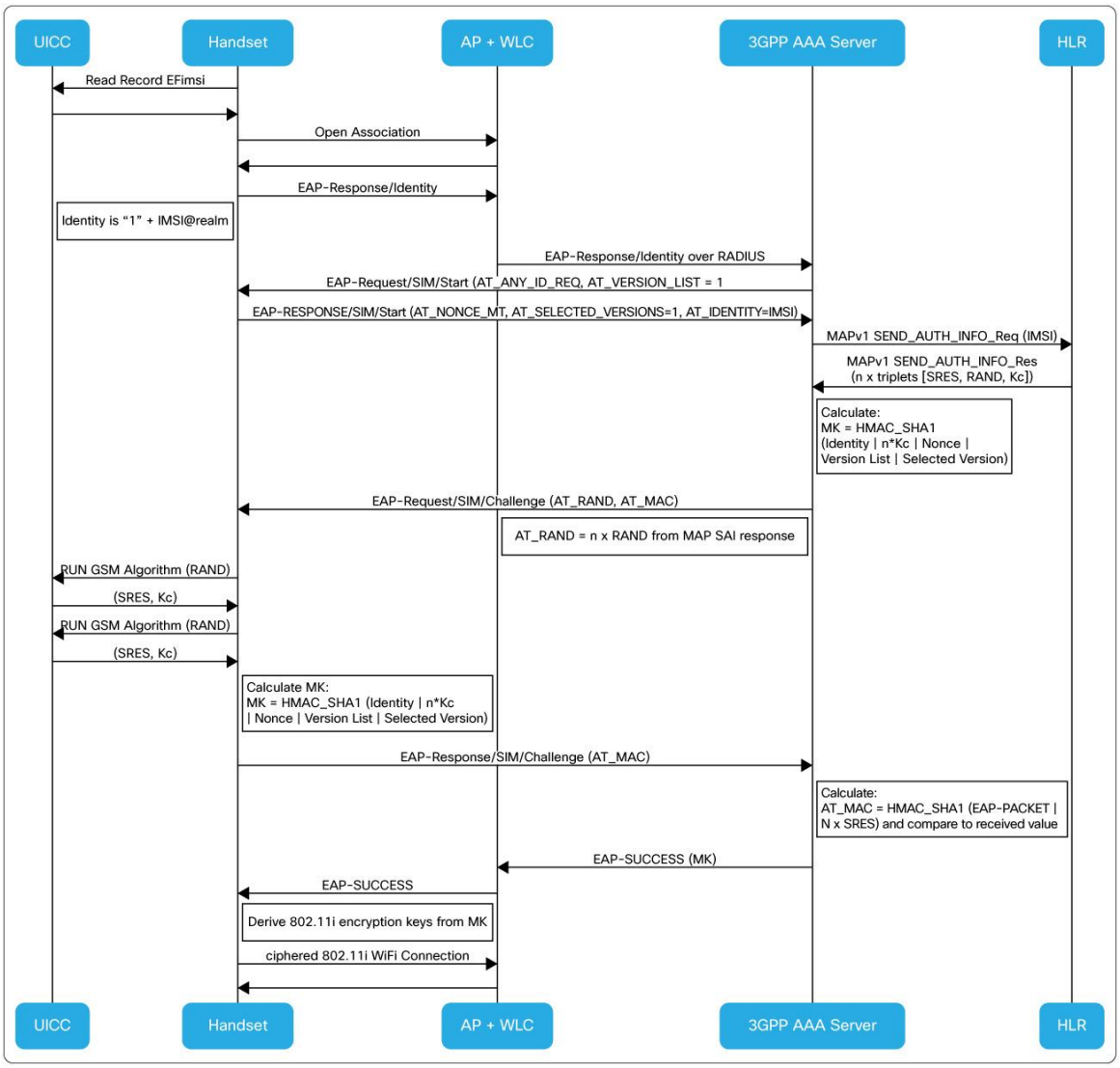
One critical capability lacking in earlier generations of Wi-Fi equipment was the ability to transparently authenticate access to the network and to deliver secure Wi-Fi operation. The foundational Extensible Authentication Protocol Subscriber Identity Module (EAP-SIM) and EAP Authentication and Key Agreement (EAP-AKA) methods, together with IEEE 802.1X and 802.11i standards for authentication and encryption, have been included in 3rd Generation Partnership Project (3GPP) specifications since 2005. However, there has been no agreed certification program supporting the wide range of Wi-Fi-enabled smartphones. This omission has recently been addressed by the Wi-Fi Alliance (WFA) in its Passpoint certification program [1], which requires Passpoint-certified products to support the latest EAP-SIM and EAP-AKA smartcard-based authentication techniques. This allows the same smartcard-based security credentials used to authenticate a device onto the cellular network to be reused for authenticating the device onto the Wi-Fi network.

The availability of WFA-certified Passpoint devices will remove the historical friction users have faced in getting their Wi-Fi devices to access the network. Although this is of critical importance, the next issue to address, now that we have a standard technique for authenticating the user within a Wi-Fi environment, is how should we authorize a particular user for access to the Wi-Fi network?

Passpoint Authentication

WFA's Passpoint enables legacy cellular authentication credentials to be reused for authenticating Wi-Fi devices onto the IEEE 802.11 network. An example of the EAP-SIM dialogue is illustrated in Figure 2, highlighting how the existing Home Location register (HLR) is signalled to recover standardized SIM-based challenge and response credentials for the Wi-Fi device.

Figure 2. EAP-SIM-Based Wi-Fi Authentication



The MAP SEND AUTH INFO messages are a standardized message exchange supported by all HLRs to enable cellular devices to be authenticated by a visited GSM core network.

Cellular Authorization Procedures

The Passpoint specification reuses cellular authentication signalling for authenticating the device onto a Wi-Fi network. Can a similar approach be reused for recovering Wi-Fi authorization information from the HLR? This section will analyze the possible reuse of per-subscriber cellular authorization information for authorizing service provider Wi-Fi services.

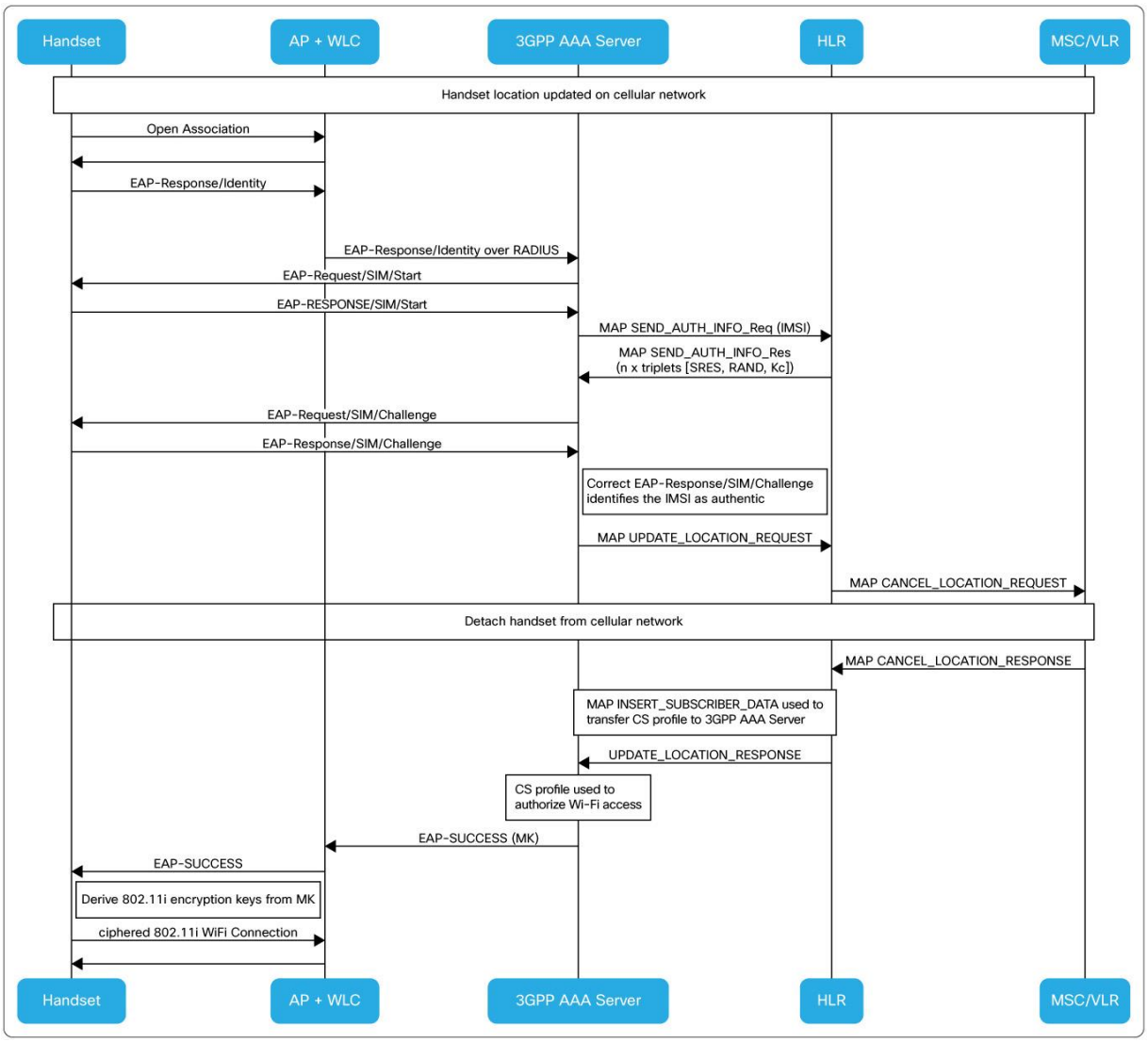
When subscription data is stored in the HLR, it is separated into information pertinent to two distinct domains, corresponding to circuit-switched (CS) and packet-switched (PS) services. From the HLR's perspective, when the 3GPP authentication, authorizing, and accounting (AAA) server recovers authentication credentials, it is acting as either a mobile switching center/visitor location register (MSC/VLR) in the circuit-switched domain or as a Serving

GPRS Support Node (SGSN) in the packet-switched domain. This can in theory trigger a structured Location Update procedure to recover the circuit-switched or packet-switched portion of the subscription profile.

The issue with using conventional authorization based on MSC/VLR or SGSN is that the reception of the Location Update Request message from the 3GPP AAA server will include an International Mobile Subscriber Identity (IMSI) that may already be associated with an attached device on the cellular network. For recovering the circuit-switched portion of the subscription profile, the 3GPP AAA server is effectively masquerading as an MSC/VLR, so the HLR will interpret this as a normal mobility event. 3GPP has specified that in such a situation, the HLR should trigger the cancelling of the registration of the IMSI in the "old" MSC/VLR, as illustrated in Figure 3. The unfortunate consequence is that the smartphone cannot be simultaneously authorized for access to voice services on the cellular network and data services on the Wi-Fi network, a situation that is far from ideal.

Note: An optional HLR feature defined by 3GPP called Super-Charger allows the HLR not to send the cancel location request to the old network element when receiving a new location update request. Such a feature would avoid the inconvenience of automatically deactivating a smartphone's cellular connection when authenticated on a Wi-Fi network. However, as commercial MSC/VLRs increased in scale, the claimed benefits of Super-Charger for decreasing VLR-HLR signalling traffic have diminished.

Figure 3. VLR-Based Wi-Fi Authorization



The procedures described in Figure 3 enhance the 3GPP AAA server to masquerade as an MSC/VLR to recover the subscriber's circuit-switched profile, but a similar approach can be used to recover the packet-switched profile by having the 3GPP AAA server masquerade as an SGSN. Unfortunately, similar limitations apply: authorization of the user onto the Wi-Fi network will trigger a deactivation of any established GPRS connectivity.

Although the Super-Charger functionality is known to have been deployed in some MSC/VLR deployments, its focus was never on scaling the SGSN's packet-switched domain. Thus as soon as the 3GPP AAA server, masquerading as an SGSN, requests authorization information from the HLR, all established cellular data connections will be lost. Such a situation is contrary to the recent recommendations published by the GSM Association (GSMA) regarding support for simultaneous Wi-Fi and cellular connectivity [2].

GSMA PRD TS.22 Wi-Fi Cellular Recommendations

It is important that the mobile network connection must be kept when the Wi-Fi access has been performed for the following reasons:

- For core network capacity (e.g., no new PDP context establishment on 3GPP on every Access Point connection)
- Charging tickets processing load
- Transparent user interface
- Network inactivity timer mechanism keeps working as normal

Because there are problems with using a full circuit-switched location update procedure for authorizing Wi-Fi access, an alternative approach has been proposed to use a VLR error recovery procedure to trigger the transfer of the circuit-switched subscription profile from the HLR to the 3GPP AAA server. 3GPP has defined the MAP-RESTORE-DATA structured procedure to account for VLR failures, and Cisco first supported such capabilities in 2003 [3] for Wi-Fi authorization. Figure 4 shows the operation of such an authorization approach, illustrating how the circuit-switched profile can now be recovered by the 3GPP AAA server without triggering deactivation of the IMSI on the cellular network.

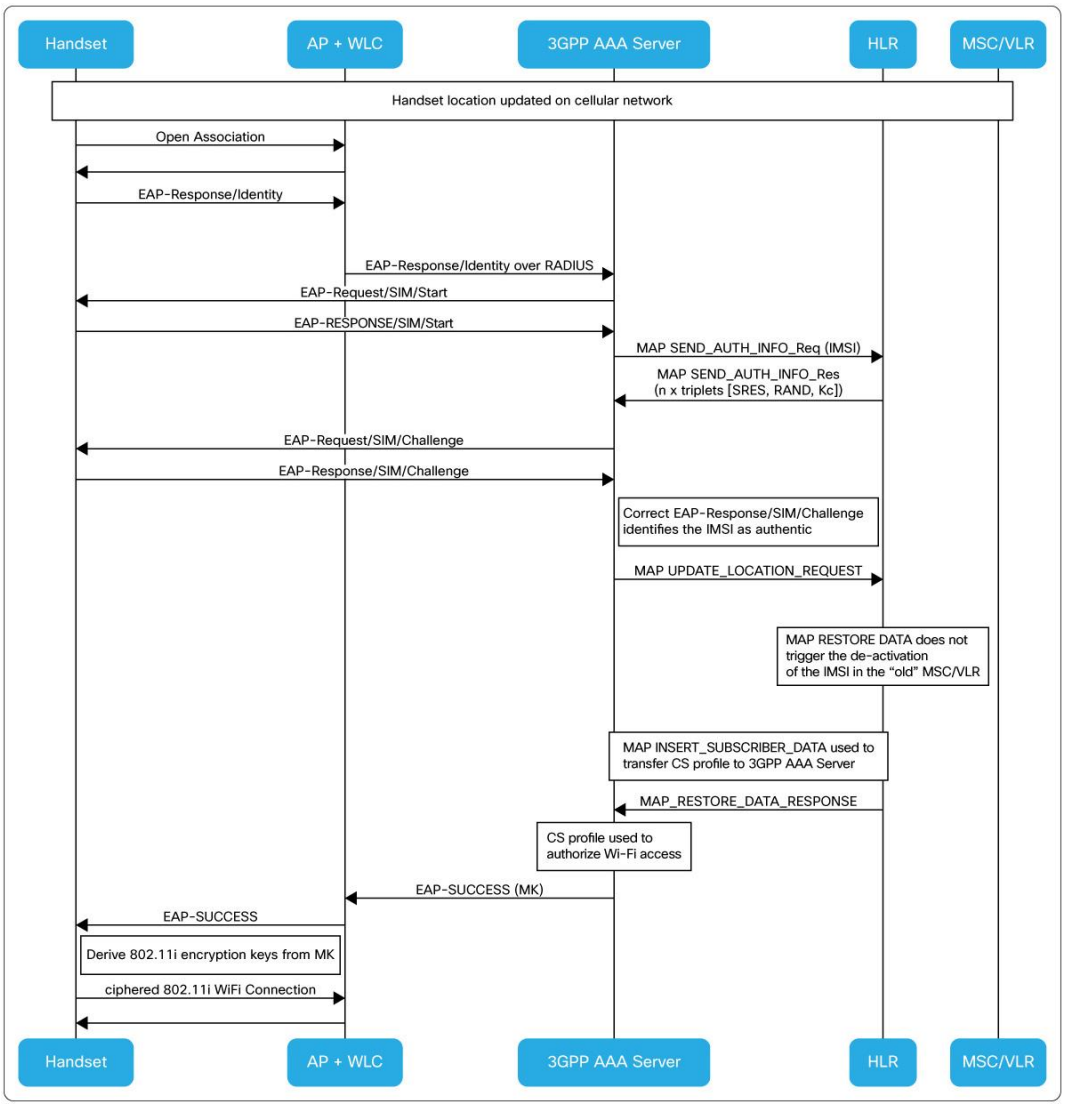
When Cisco first delivered such capability in 2003, it experienced deployment issues due to the unspecified operation of a HLR in these situations:

- Receiving a VLR error recovery message for an IMSI that was not presently location-updated on the network
- Receiving an error recovery message from a VLR that is different from the last known registered VLR

Integration testing with a range of HLRs at that time indicated that Ericsson's HLR in particular did not permit a MAP-RESTORE-DATA-based error recovery procedure for an IMSI that was not already registered in the cellular network.

Note: After the implementation of MAP-RESTORE-DATA for triggering transfer of the circuit-switched profile by Cisco, 3GPP clarified operation of the HLR. It should return an error to the VLR if the subscriber is not registered on that VLR [4].

Figure 4. MAP-RESTORE-DATA Wi-Fi-Authorization

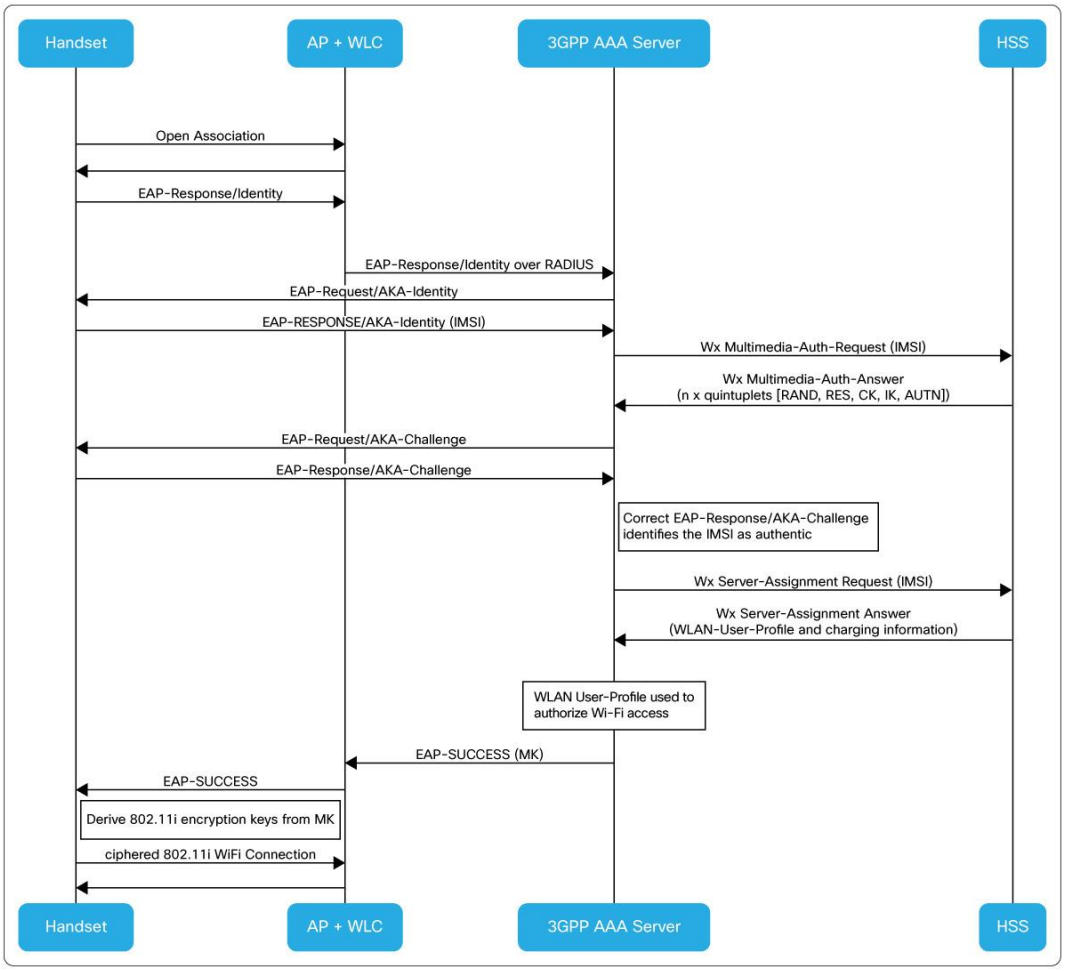


Wi-Fi Authorization Procedures

3GPP has enhanced its architecture to allow integration of Wi-Fi access networks for EAP-SIM and EAP-AKA authentication. These developments have standardized Wi-Fi service authentication and authorization using the Diameter-based Wx interface between the 3GPP AAA server and the Home Subscriber Server (HSS) [5].

The Wx interface is first used with a Multimedia-Auth-Request/Multimedia-Auth-Answer exchange to recover the quintuplets used to authenticate the Wi-Fi device based on EAP-AKA. A second Wx exchange using Server-Assignment-Request/Server-Assignment-Answer is then used to recover authorization data from the HSS (Figure 5).

Figure 5. Wx-Based Wi-Fi-Authorization



3GPP Subscriber Wi-Fi Authorization Profile

Once an IMSI is determined to be authentic, the second Wx exchange is used to recover the WLAN user's profile and charging information. The charging information corresponds to the Charging Characteristics Information Element, an integer value that can be used by network elements to determine how to charge for Wi-Fi access. The WLAN user profile is more insightful, providing the information listed in Tables 1 and 2 to the 3GPP AAA server.

Table 1. Wx-Based Subscriber Wi-Fi Profile

Wi-Fi User Profile	Comments
Subscription-ID	END_USER_E164 Mobile Subscriber Identity Number (MSISDN) or END_USER_IMSI (IMSI)
WLAN-Access	WLAN_SUBSCRIPTION_ALLOWED or WLAN_SUBSCRIPTION_BARRED
WLAN-3GPP-IP-Access	WLAN_APNS_ENABLE or WLAN_APNS_DISABLE
Session-Timeout	Session timeout in seconds prior to re-authentication
APN-Authorized	See Table 2 for more details
Maximum-Number-Access	Maximum concurrent Wi-Fi access

Wi-Fi User Profile	Comments
WLAN-Direct-IP-Access	Whether user is authorized to directly access external IP networks
QoS-Resources	Subscriber's 3GPP WLAN quality of service (QoS) profile

Table 2. Wx-Based Access Point Name (APN) Authorized Information

Wi-Fi User Profile	Comments
3GPP-WLAN-APN-Id	The W-APN that the subscriber is authorized to access
APN-Barring-Type	No barring, Home barring, Visited barring, or Internet access barred
Framed-IP-Address	Optional static IPv4 assignment
Framed-IPv6-Prefix	Optional static IPv6 prefix assignment
Max-Requested-Bandwidth	Maximum allowed bandwidth
QoS-Resources	RFC 5777 defined QoS filter policies

Compared with the well-defined Wx WLAN user profile that enables users to be authorized for particular "APN-type" services with associated QoS and bandwidth restrictions, the MAP-RESTORE-DATA procedure is used to recover the circuit-switched profile of a particular subscriber. Examples of the data transferred using the INSERT-SUBSCRIBER-DATA procedure is shown in Table 3.

Table 3. Example of VLR-Based Subscription Information

VLR User Profile
• IMSI
• MSISDN
• MS Category
• Subscription Restrictions
• Access Restriction Data
• Closed Subscriber Group
• Provision of Bearer Service
• Provision of Teleservice
• Bearer Capability Allocation
• Barring Information
• Supplementary Service Information
• CAMEL Service Information

In particular, a range of bearer services have been defined in GSM, which may not be applicable to the latest 3G deployments [6]. The 3GPP AAA server can benefit by reusing an indication that an IMSI is provisioned with one of these bearer services to indicate that an IMSI is authorized to access the Wi-Fi network. For example, Bearer Service 41 was defined to indicate support for Packet Assembly Disassembly (PAD) access at 300 bps. If this is indicated as being enabled in the circuit-switched subscription profile, the 3GPP AAA server may then infer that the IMSI is authorized for Wi-Fi access.

Note: When the comprehensive Wx based Wi-Fi service authorization is compared with the circuit-switched profile used in the MAP-RESTORE-DATA approach to Wi-Fi authorization, it is evident that the opportunity to define full-featured Wi-Fi authorization services is compromised by the desire to leverage older HLR elements.

Required Wi-Fi Authorization Information

After considering the binary authorization information available using the MAP-RESTORE-DATA approach or the more comprehensive Wi-Fi authorization information available using the Wx-based approach, it is interesting to compare the authorization information used in today's standalone Wi-Fi deployments.

Table 4 provides a list of typical information stored in the subscriber database for a service provider Wi-Fi deployment. The database includes some of the information typically found in billing systems. However, when we look at the credential information we see that when compared to the simple reuse of SIM credentials, the service provider Wi-Fi infrastructure may be simultaneously required to support web authentication use cases, SMS-One Time Password authentication, as well as MAC-based Transparent Auto Logon (MAC-TAL) for a plurality of devices associated with the subscriber (IMSI).

Furthermore, access restrictions, which in 3GPP have been defined on the per-network level (Visited Public Land Mobile Network [VPLMN] and Home Public Land Mobile Network [HPLMN] based), are defined on a more granular basis as a number of "AP-Groups." Users are then selectively authorized to access the network through Wi-Fi access points associated with different AP-Groups.

Table 4. Example of Subscription Information from a Service Provider Wi-Fi Deployment

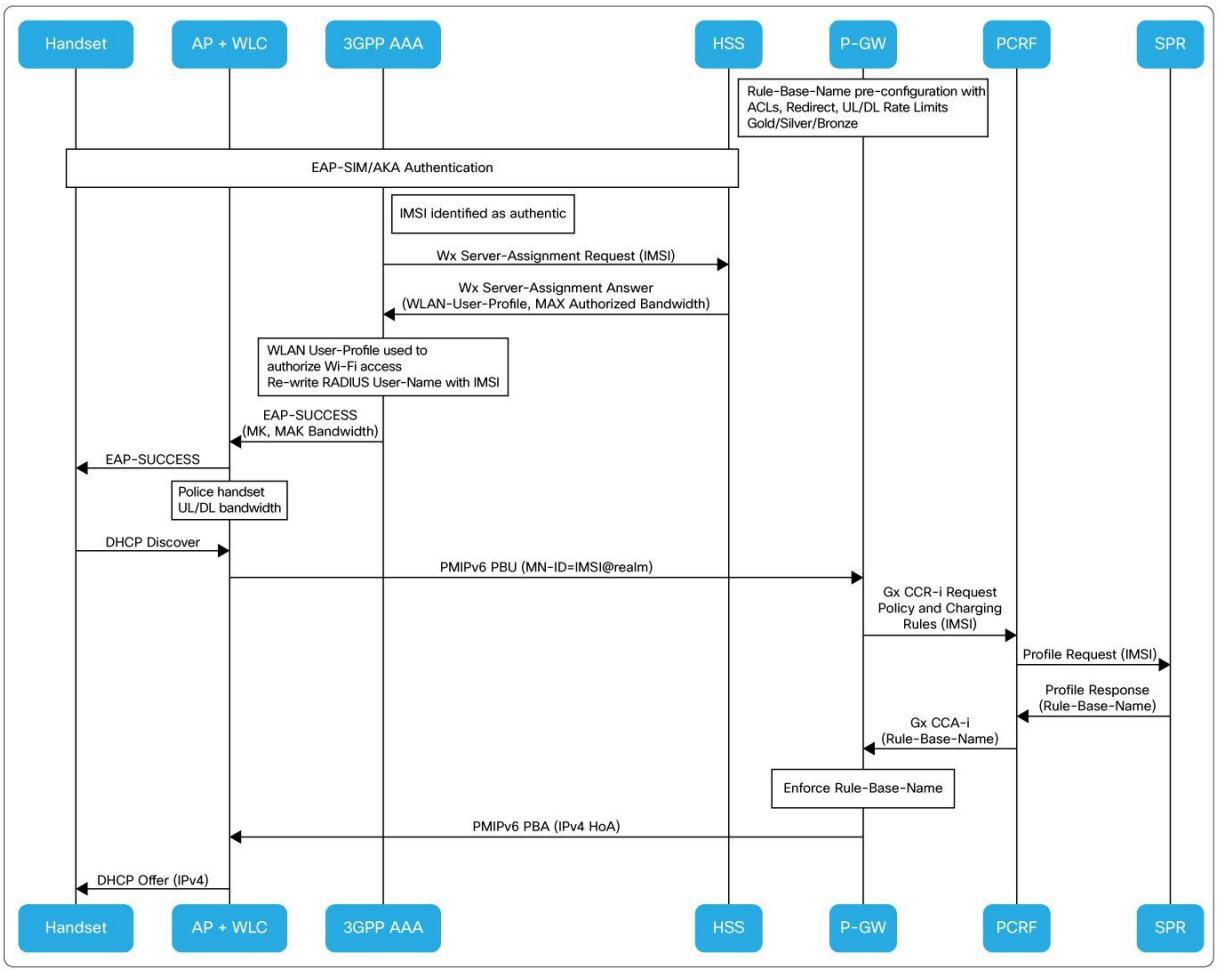
SP Wi-Fi User Profile	Information
Subscriber Information	Firstname, Lastname
	Service Start Date
	Service Stop Date
	Service Status Enabled/Disabled
	External Identity
Billing Information	Charging Identity
	Rate Plane Code
	Monthly Billing Cycle
	Pre-Paid or Post Paid
Notifications	Email Address
	SMS Address
	Notification Preference
	Notifications Enabled/Disabled
Credentials	EAP-SIM/AKA Enabled/Disabled
	Web auth Enabled/Disabled
	User-name & Password
	SMS-OTP Enabled/Disabled
	MAC-TAL Devices 0-3
	Authorized MAC#1 & Expiry date
	Authorized MAC#2 & Expiry date
	Authorized MAC#3 & Expiry date
Location Restrictions	Location Restrictions Enabled/Disabled
	Authorized AP-Group Names

SP Wi-Fi User Profile	Information
Authorized Services	Service Name Charging Enabled/Disabled Service Definition: Open Garden Service Service Definition: UL/DL Rate limits Service Definition: Access Control Lists (ACLs) Service Definition: Gold/Silver/Bronze Service Definition: Session Timeout Service Definition: Idle Timeout Service Definition: L4Redirect Service Definition: Virtual Route Forwarding (VRF) Assignment Access Enabled/Disabled

For service definition, it is evident that the typical Wi-Fi authorization information includes a richer syntax compared to the simple APN (VRF) and bandwidth limits encoded in Wx. In this regard, the Wi-Fi authorization information can be viewed as aligned with Gx-type rule-base information whereby the rule-base name can be used by the policy enforcement function to activate predefined policies regarding ACLs, rate limits, etc.

3GPP has defined a Subscriber Profile Repository (SPR) that can be queried by policy servers to identify those services that a user is authorized to access. Instead of a service name used in the Wi-Fi subscriber information, a rule-base name is used to identify a set of preconfigured services on the gateway that provides per-subscriber services. Figure 6 shows an example of a flow where a public data network (PDN) Gateway (P-GW) is used to provide services for service provider Wi-Fi subscribers and an SPR is queried to recover the authorized rule-base names for a particular subscriber.

Figure 6. Gx-Based SPR Wi-Fi Authorization



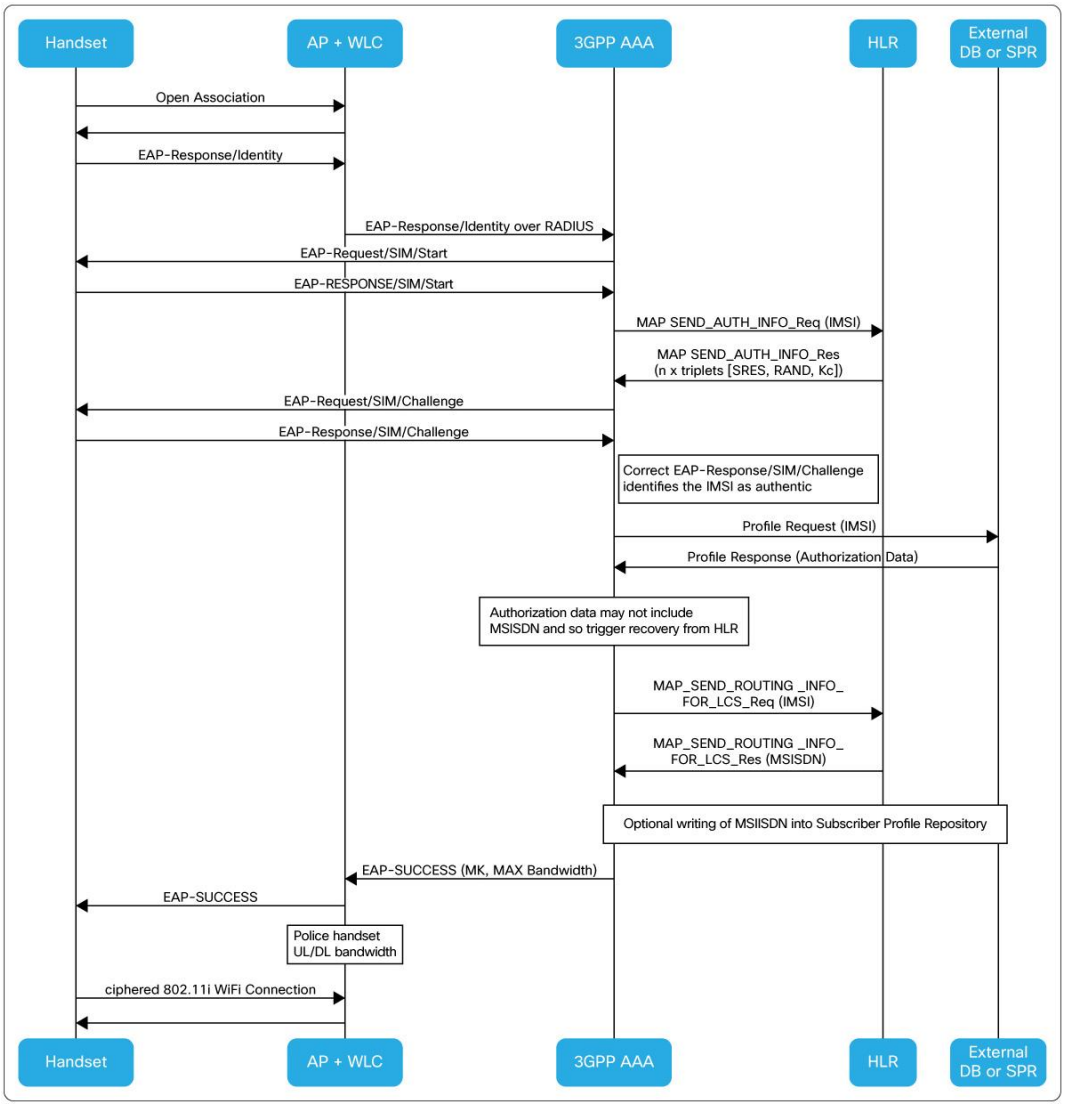
Note: The SP reference point between the PCRF and SPR has not been standardized by 3GPP, and therefore the SPR is viewed as a proprietary implementation.

SPR-Based Wi-Fi Authorization

Rather than leverage standard Wx-based Wi-Fi authorization techniques, the definition of SPR has highlighted how nonstandardized policy repositories can be integrated into 3GPP architectures (Figure 7). Using an evolution of such approaches, some mobile network operators are motivated to build a separate standalone system for Wi-Fi authorization outside of the conventional subscriber profile stored in the HLR/HSS, with functionality similar to SPR.

However, although the data listed in Tables 1, 2 and 4 can be defined in an external database, an important capability of the Wx interface is to enable the 3GPP AAA server to be signalled the MSISDN of the user. The MSISDN is particularly important because, as a general rule, charging functionality within mobile operators' networks is largely based on MSISDN, rather than IMSI.

Figure 7. SPR-Based Wi-Fi-Authorization

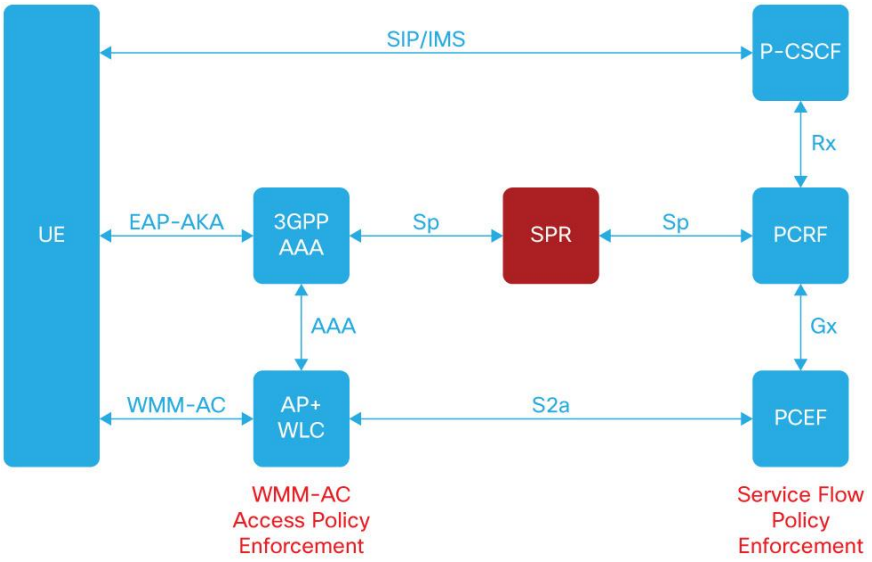


This poses a restriction on any standalone Wi-Fi authorization database, because its provisioning has to be closely coupled to the operational systems that enable mapping between IMSI and MSISDN. Because these back-end systems are rarely fully specified, Cisco has enhanced the 3GPP AAA server to enable reuse of an older HLR for providing the mapping between IMSI and MSISDN. This capability uses a standardized MAP exchange whereby the HLR can be queried with the IMSI derived as part of the EAP-SIM or EAP-AKA exchange and have the HLR return the MSISDN associated with the IMSI [7].

Figure 7 shows the operation of such an approach. The 3GPP AAA server is augmented with MAP_SEND_ROUTING_INFO_FOR_LCS signalling capability, which then can automate the mapping between IMSI and MSISDN. The authorization information recovered from the SPR is delivered to the Wi-Fi access network, in this case to allow per-user uplink rate limiting to be performed by the Wi-Fi access point.

Moving forward, this approach can be used to support a richer access network policy. For example, the Wi-Fi Alliance now has a certification program for Wi-Fi Multimedia Admission Control (WMM-AC), whereby the access network can be configured to mandate applying admission control procedures prior to allocating voice and/or video air interface resources to particular device. Figure 8 illustrates how the authorization information stored in the SPR can then be augmented with information defining whether a particular user has access to voice and/or video services in the access network or whether only best-effort Wi-Fi service is available.

Figure 8. SPR-based Wi-Fi Access and Service Authorization



Summary

Cisco has been offering Wi-Fi authentication and authorization capability for mobile network operators for nearly a decade, allowing older HLRs as well as the latest HSS equipment to support Wi-Fi integration into mobile networks. The adoption of WFA's Passpoint certification program is likely to dramatically increase the interest in Wi-Fi integration options, including foundational authentication and authorization functionality.

As the feature richness of the Wi-Fi access network is enhanced, service provider Wi-Fi operators will increasingly need to address the definition of Wi-Fi authorization information. Although Wx-based definitions are significant improvements over the binary information available using MAP-RESTORE-DATA approaches, the adoption of real-time media services over the Wi-Fi access network will promote the definition of new capabilities that will require corresponding definition of authorization information.

References

[1] http://www.wi-fi.org/knowledge-center/white-papers/wi-fi-certified-passpoint%E2%84%A2-new-program-wi-fi-alliance%C2%AE-enable-seamless.

[2] http://www.gsma.com/newsroom/wp-content/uploads/2012/06/TSG_PRD_TS.22_v1.0_Recommendations_for_Minimal_Wi-Fi_Capabilities_of_Terminals.pdf.

[3] http://www.cisco.com/warp/public/cc/pd/witc/itp/prodlit/mapga_wp.pdf.

[4] http://www.3gpp.org/ftp/Specs/html-info/29002.htm.

[5] http://www.3gpp.org/ftp/Specs/html-info/29234.htm.

[6] http://www.3gpp.org/ftp/Specs/html-info/0202.htm.

[7] http://www.cisco.com/en/US/docs/net_mgmt/prime/access_registrar/6.0/release/notes/60relnot.htm.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-728077-00 05/13