Service Provider Wi-Fi Networks: Scaling Signaling Transactions

Summary

Wi-Fi adoption is in the midst of a transition, from being viewed purely as an extension of the fixed broadband business toward becoming a core capability that is being integrated into end-to-end service provider networks, delivering data connectivity that can complement conventional cellular data access. The recently introduced Wi-Fi Alliance (WFA) Wi-Fi CERTIFIED Passpoint certification program (hereafter referred to as Passpoint) enables smartphone devices to make use of smart card credentials to authenticate themselves to service provider Wi-Fi networks, addressing one of the key barriers to adoption of Wi-Fi by service providers - ease of use. The use of Extensible Authentication Protocol for GSM Subscriber Identity Module (EAP-SIM) and EAP for UMTS Authentication and Key Agreement (EAP-AKA) is seen as an important step in improving the experience of smartphone users on Wi-Fi networks, bringing them on a par with cellular networks where network selection and authentication are fully automated and usually hidden from the user, even in roaming scenarios.

However, the wide-scale adoption of Passpoint-certified mobile devices and operation of EAP-SIM and EAP-AKA brings new scalability challenges to service provider Wi-Fi networks and their mobile network operator (MNO) partner networks. As a consequence, the GSM Association (GSMA, the industry body representing the MNOs) and the Wireless Broadband Alliance (WBA, the industry body representing the service provider Wi-Fi operators) have cooperated on an investigation into the potential for scaling issues associated with the adoption of the Wi-Fi Alliance’s Passpoint-certified devices that make use of smart card credentials to authenticate themselves to service provider Wi-Fi networks.

Cisco provides a comprehensive and proven set of techniques for addressing signaling scale within service provider Wi-Fi networks. Driven by a need to enhance the user experience when connecting to Wi-Fi networks, Cisco has already developed and deployed a set of capabilities that will significantly help ease the burden of signaling when using EAP based authentication in Wi-Fi networks. Configuration options defined with Cisco’s authentication, authorization, and accounting (AAA) and EAP server capabilities can be used to address signaling scaling and enable back-end systems to be protected from any signaling storms.

Using the breadth of techniques being defined by the industry and enabled on Cisco Service Provider Wi-Fi infrastructure, operators can be confident that their Passpoint deployments will be able to scale to accommodate the enhanced ease of use that will accompany EAP-SIM/AKA deployments.

Introduction

Many service providers have adopted access strategies that now include the deployment of a large number of Wi-Fi access points, offering service to a sizable population of users equipped with a range of Wi-Fi-enabled devices.

The recently introduced Passpoint certification program enables smartphone devices to make use of smart card, also known as universal integrated circuit card (UICC), credentials to authenticate themselves to service provider Wi-Fi networks, addressing one of the key barriers to adoption of Wi-Fi by service providers - ease of use. The Passpoint certification program ensures that Wi-Fi devices supporting the Hotspot 2.0 specifications can successfully interoperate.

The use of EAP-SIM and EAP-AKA in Hotspot 2.0 is seen as an important step in improving the experience of smartphone users on Wi-Fi networks, bringing them on a par with cellular networks where network selection and authentication are fully automated and usually hidden from the user, even in roaming scenarios.

However, the wide-scale introduction of Passpoint-certified mobile devices and operation of EAP-SIM and EAP-AKA brings new scalability challenges to service provider Wi-Fi networks and their MNO partner networks. As a consequence, the GSMA and the WBA have cooperated on an investigation into the potential for scaling issues associated with the adoption of WFA's Passpoint-certified devices that make use of smart card credentials to authenticate themselves to service provider Wi-Fi networks.

This white paper builds on material published by GSMA/WBA[1] and describes a comprehensive and proven set of tools that enable service providers to address the scalability challenges of their carrier Wi-Fi deployments.

Adoption of Passpoint

Legacy service provider Wi-Fi systems have conventionally made extensive use of web-based authentication. These systems require scaling to address the requirement to allocate an IP address to every Wi-Fi device that associates with the network. This requirement enables the service provider to redirect users' HTTP browser sessions to a "captive" portal, where they are provided with a web page advertising the Wi-Fi service and are subsequently able to enter their username and password credentials. An improved user experience may be supported on particular devices that transparently make an HTTP request in order to determine whether the Wi-Fi network offers direct connectivity to the Internet or whether user credentials are required to be entered into a captive portal.

Compared with such legacy systems that stress the IP address management (IPAM) functionality of the service provider Wi-Fi network, users of Passpoint devices will instead trigger an EAP dialogue after associating with the Wi-Fi network and before requesting an IP address. This EAP dialogue will typically be transported over RADIUS signaling between the IEEE 802.1X port-based authenticator and the EAP server. Furthermore, when supporting EAP-SIM and/or EAP-AKA methods, as defined in the Hotspot 2.0 Release 1.0 and 2.0 specifications, the EAP server will interface to the home location register (HLR) for EAP-SIM or the home subscriber server (HSS) for EAP-AKA enabling the recovery of subscriber smart card credentials.

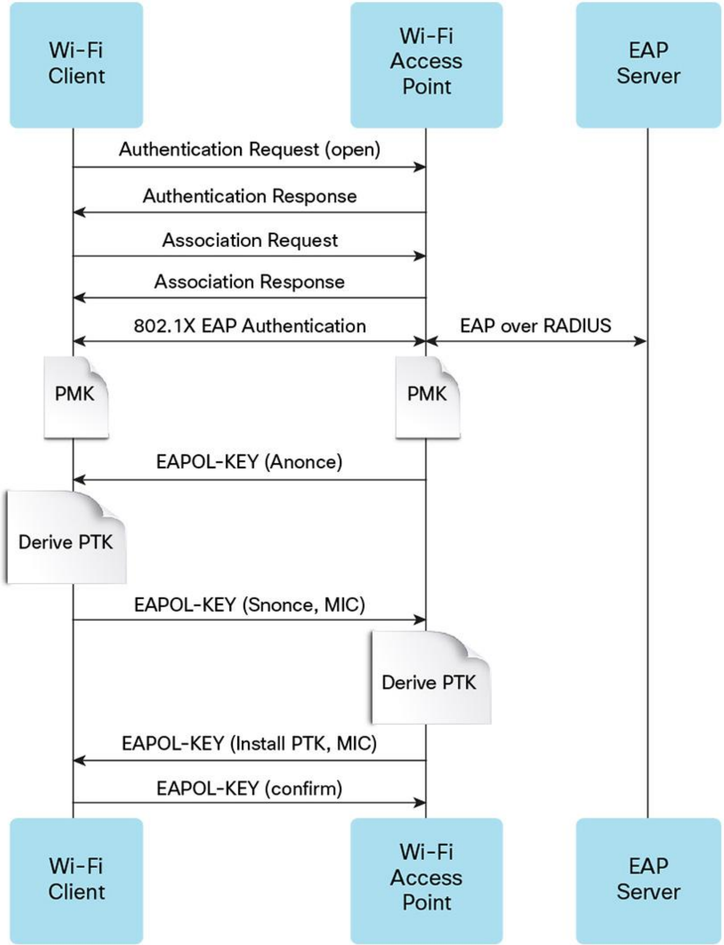
Hence, compared with legacy service provider Wi-Fi architectures that required scalable IPAM infrastructure, mobile operators wanting to accelerate the adoption of Wi-Fi through the use of Passpoint-certified devices need to pay careful attention to the scalability of the end-to-end systems for supporting the EAP dialogue.

Overview of IEEE 802.1X-Based Authentication

It is instructive to review the authentication process when IEEE 802.1X is used as required by the Passpoint architecture. Figure 1 illustrates that the Wi-Fi client initiates the authentication process by sending an authentication request followed by an association request. Subsequent to the association request/response exchange, the access point initiates the EAP sequence. On successful authentication, the AAA server sends a pairwise master key (PMK) to the access point. The client is able to derive the same PMK independently. The PMK is then used to derive another set of keys, termed pairwise transient keys (PTKs). The PTKs are used to secure the traffic between the client and the AP over the encrypted Wi-Fi link. The PTKs are derived and installed based on a four-way handshake using EAP over LAN (EAPOL) key frames. The four-way handshake is required to provide protection from replay attacks as well as man-in-the-middle attacks.

[1] http://www.wballiance.com/tag/authentication-signaling-optimization/

Figure 1. IEEE 802.1X EAP Authentication



Passpoint and EAP-SIM Dialogue

As with all EAP-methods, EAP-SIM and EAP-AKA support end-to-end signaling between an IEEE 802.1X supplicant on the Wi-Fi device and an EAP server. Furthermore, to support smart card-based authentication, EAP-SIM and EAP-AKA require the EAP server to interface to the HLR/HSS. This means that the end-to-end signaling flow includes not only Wi-Fi and AAA equipment, but also HLR/HSS and SS7 networking, as illustrated in Figure 2.

Figure 2. Entities Involved in EAP-SIM/EAP-AKA Authentication

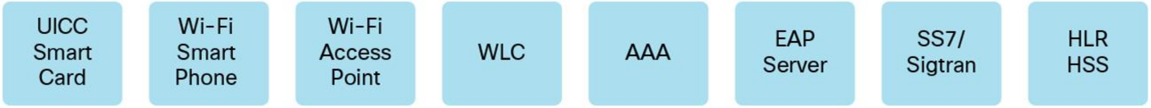


Figure 3 illustrates the end-to-end operation of the EAP-SIM dialogue. The exchange represents a “full” EAP-SIM authentication and shows the number of exchanges as summarized in Table 1.

Figure 3. EAP-SIM Dialogue

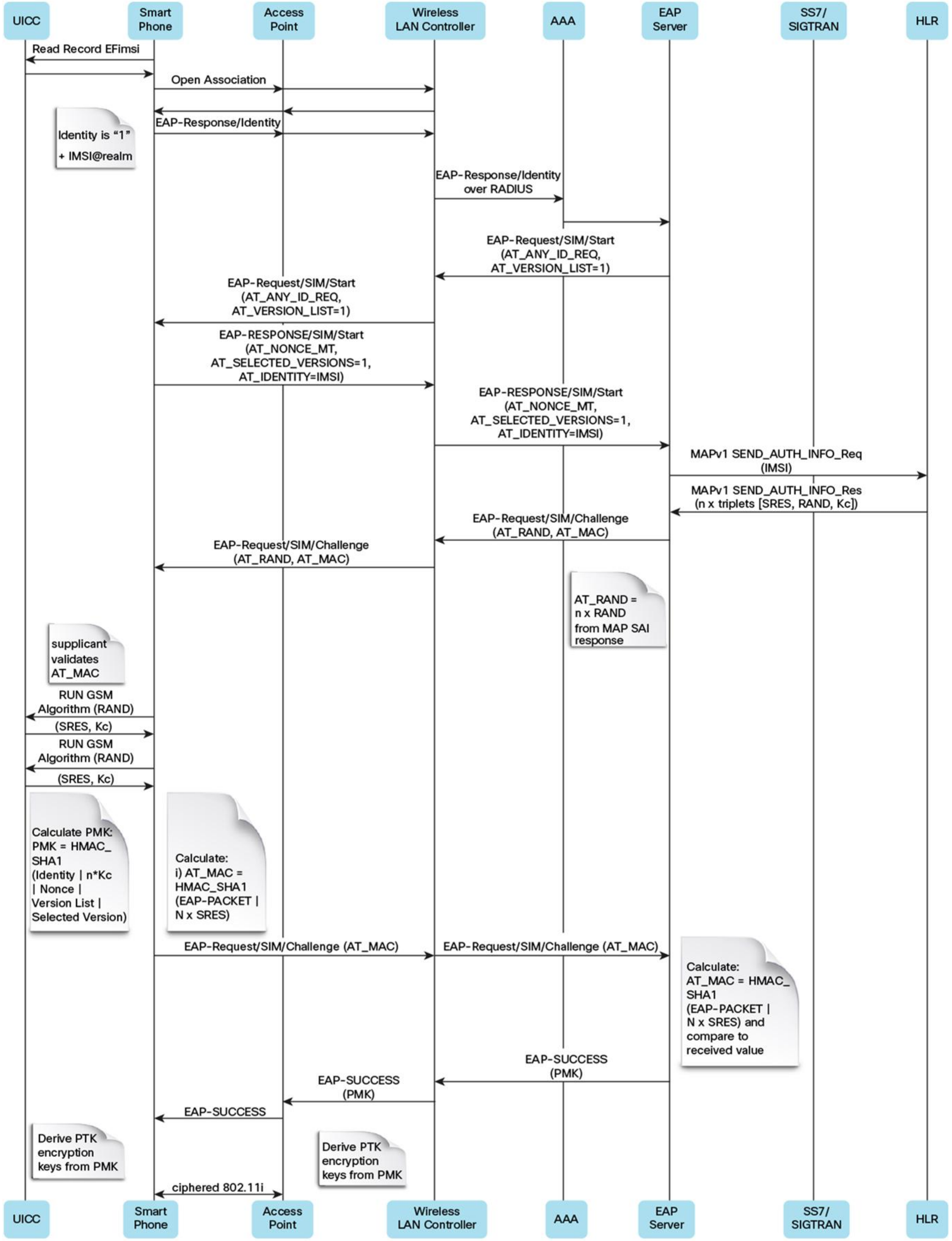

UICC
Smart Phone
Access Point
Wireless LAN Controller
AAA
EAP Server
SS7/ SIGTRAN
HLR
Read Record EFimsi
Open Association
EAP-Response/Identity
Identity is "1" + IMSI@realm
EAP-Response/Identity over RADIUS
EAP-Request/SIM/Start (AT_ANY_ID_REQ, AT_VERSION_LIST=1)
EAP-Request/SIM/Start (AT_ANY_ID_REQ, AT_VERSION_LIST=1)
EAP-RESPONSE/SIM/Start (AT_NONCE_MT, AT_SELECTED_VERSIONS=1, AT_IDENTITY=IMSI)
EAP-RESPONSE/SIM/Start (AT_NONCE_MT, AT_SELECTED_VERSIONS=1, AT_IDENTITY=IMSI)
MAPv1 SEND_AUTH_INFO_Req (IMSI)
MAPv1 SEND_AUTH_INFO_Res (n x triplets [SRES, RAND, Kc])
EAP-Request/SIM/Challenge (AT_RAND, AT_MAC)
EAP-Request/SIM/Challenge (AT_RAND, AT_MAC)
AT_RAND = n x RAND from MAP SAI response
supplicant validates AT_MAC
RUN GSM Algorithm (RAND)
(SRES, Kc)
RUN GSM Algorithm (RAND)
(SRES, Kc)
Calculate PMK: PMK = HMAC_ SHA1 (Identity | n*Kc | Nonce | Version List | Selected Version)
Calculate: i) AT_MAC = HMAC_SHA1 (EAP-PACKET | N x SRES)
EAP-Request/SIM/Challenge (AT_MAC)
EAP-Request/SIM/Challenge (AT_MAC)
Calculate: AT_MAC = HMAC_ SHA1 (EAP-PACKET | N x SRES) and compare to received value
EAP-SUCCESS (PMK)
EAP-SUCCESS (PMK)
EAP-SUCCESS
Derive PTK encryption keys from PMK
Derive PTK encryption keys from PMK
ciphered 802.11i
UICC
Smart Phone
Access Point
Wireless LAN Controller
AAA
EAP Server
SS7/ SIGTRAN
HLR

Table 1. Full EAP-SIM Signaling Scaling

Full EAP-SIM Authentication	
2 or 3	SIM card exchanges
3	AAA exchanges between WLC and EAP server and intermediate proxies
3	EAP-SIM exchanges between smartphone and EAP server
4	Additional request/response exchanges (authentication, association, EAPOL...)
1	HLR query

Note that a single HLR/HSS query can be used to recover up to five triplet/quintuplet sets from the HLR/HSS, whereas Figure 3 illustrates two sets of triplets being used to support a single EAP-SIM full authentication exchange.

Scaling for Mobility Events

Importantly, the signaling exchanges detailed in the previous section highlight how these are necessary to generate keying material to protect the IEEE 802.11 radio interface. Hence, if the service provider Wi-Fi network is poorly designed, it could have the potential to generate the exchanges on every access point transition.

An appreciation of the number of access point changes will provide an upper bound on the signaling events that must be supported. The GSMA has introduced three use cases that are thought to be particularly challenging from an EAP signaling scaling standpoint:

- Community Wi-Fi
- Public transport hub: Rail station
- Stadium

In parallel, the Small Cell Forum (SCF) has examined the issue of mobility event dimensioning (from a small cell licensed radio perspective) and agreed on the following baseline dimensioning:[2]

Static:	0.1 access point changes/user/minute
Steady flow:	1.0 access point changes/user/minute
Tidal flow:	4.8 access point changes/user/minute

Note that there is strong correspondence between the GSMA and SCF use cases; for example, SCF's tidal flow example corresponds to the likely characteristics experienced in the GSMA's public transport hub use case.

However, when compared with these extreme use cases, it is likely that a typical service provider Wi-Fi network will deliver service over a heterogeneous mix of environments. For example, a network that supports a mix of deployment scenarios, such as 40 percent static, 30 percent steady flow, and 30 percent tidal flow type deployments, may experience a weighted mobility rate of (0.4 x 0.1 + 0.3 x 1.0 + 0.3 x 4.8) or 1.78 access point transitions per minute per Wi-Fi device.

[2] http://www.scf.io/en/documents/065_-_Enterprise_reference_scenarios.php

The remainder of this paper will look at techniques available to the operator of the service provider Wi-Fi network to minimize the signaling scaling challenges when deploying Passpoint-enabled service provider Wi-Fi networks. In particular, the scaling challenge with service provider Passpoint deployments involves handling a large number of transactions at the AAA server and HLR/HSS (in the case where EAP-SIM/AKA is the specific EAP method). This paper addresses such issues by describing:

- Techniques to reduce AAA interactions (especially during client mobility events)
- Techniques to reduce the impact to HSS/HLR during authentication

Finally, mechanisms available at the AAA server to handle signaling overload situation in a graceful manner are described.

IEEE 802.11-Based Approaches to Reduce AAA Exchanges

Given that the scaling challenges associated with service provider Wi-Fi networks are predominantly associated with AAA exchanges, it is instructive to understand the range of techniques available within the Wi-Fi access network for reducing the requirement for repeated AAA exchanges associated with full EAP/802.1X authentication.

Sticky Caching

Sticky key caching (SKC) is a form of key caching in which the client keeps track of a list of PMK information used from previously associated access points for a given service provider Wi-Fi network. If a client revisits an access point, the client can attempt to reassociate using the PMK derived from an earlier successful association, as illustrated in Figure 4. If the target access point has the PMK cached, the AAA server exchange is eliminated and the target access point can use the cached PMK to establish a new PTK. Table 2 summarizes the benefit of using SKC on the signaling exchanges.

Note that the IEEE 802.11i standard does not define a maximum number of cached PMKs a Wi-Fi access point needs to support or the lifetime of those cache entries. The WFA test plan only validates that at least one cached PMK is supported.

While SKC has not been widely deployed, it was added to iOS 5.1 as a feature called “pairwise master key identifier caching” (PMKID caching).[3] Client limitations with SKC exist; for example, the client will typically cache information only from the last visited access point(s) with which it has associated.

The Cisco® Wireless LAN Controller (WLC) supports configuration of SKC, storing the keying material for up to the last eight access points that a particular client has associated with. SKC can be enabled on the WLC by entering the following command:

```
config wlan security wpa wpa2 cache sticky enable wlan_id
```

[3] http://support.apple.com/kb/HT5535

Figure 4. Sticky Key Caching Operation

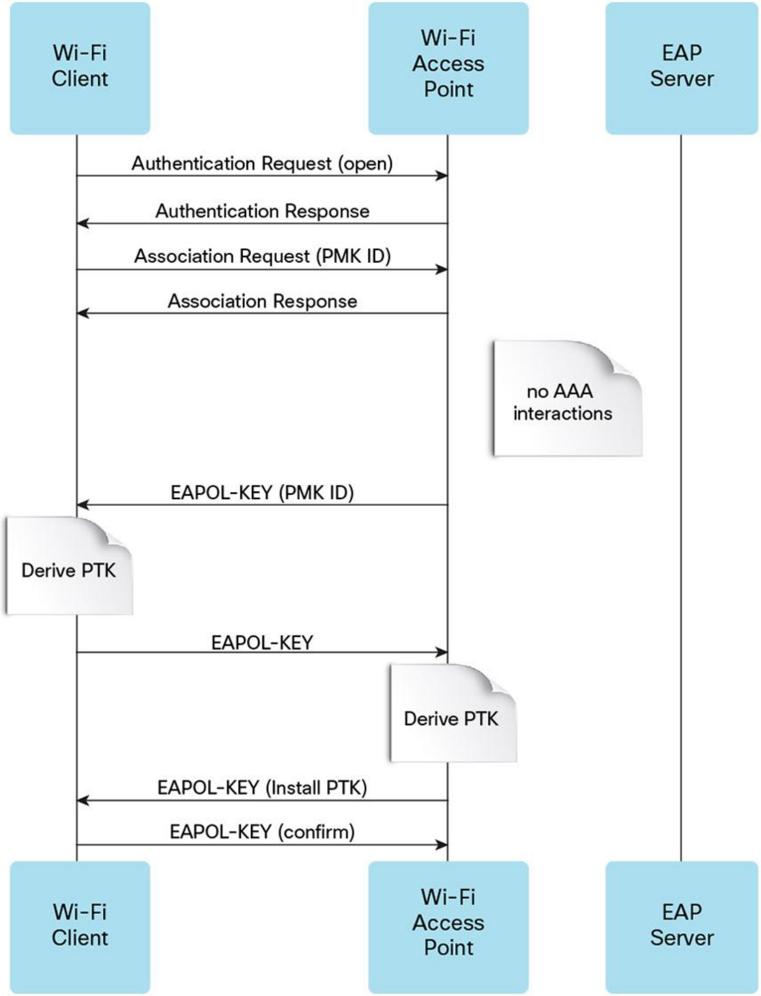


Table 2. Sticky Key Caching Signaling Scaling

Sticky Key Cache Signaling Scaling	
0	SIM card exchanges
0	AAA exchanges between WLC and EAP server and intermediate proxies
0	EAP-SIM exchanges between smartphone and EAP server
4	Additional request/response exchanges (authentication, association, EAPOL, ...)
0	HLR queries

Opportunistic Key Caching

As described in the previous section, SKC requires that the client perform a full authentication to a new access point and use cached keying material only when revisiting the same access point. Opportunistic key caching (OKC) is an alternative key caching functionality that enables cached keying material to be reused across different access points in the same service provider Wi-Fi network.

The client first establishes a PMK based on its initial association with an access point as it enters the service provider Wi-Fi network. When the client subsequently connects to a new access point in the same WLAN (the target access point), it can provide a PMKID (derived from the earlier association with the current access point) in the reassociation request, as illustrated in Figure 5. If the target access point has the PMK associated with the PMKID, the EAP exchange with the AAA server is eliminated. Instead, the target access point uses the cached PMK to establish a new PTK.

In the WLC-based systems typically deployed in service provider environments, the authentication is done by the WLC, and the PMK/PMKID is stored at the WLC. Consequently, when a client roams between two access points connected to the same WLC, the PMKID and PMK are automatically available when accessing the network via the target access point. Furthermore, multiple WLCs may be configured in a mobility group, enabling the PMK/PMKID information to be shared between different WLCs. In such configurations, even when the client roams to a target access point that is associated with a different WLC, the target access point can still have access to the PMKID/PMK and OKC can operate successfully. As a result, the client performs EAP authentication only once when entering with service provider Wi-Fi network, and all subsequently reassociations do not involve AAA servers, thus reducing the consequential signaling exchanges, as indicated in Table 3.

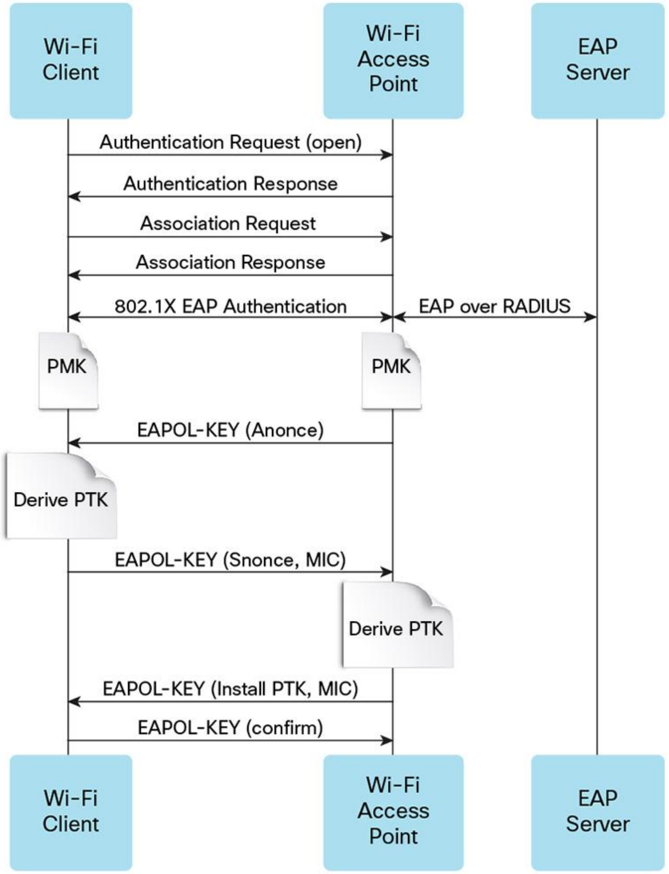
The Cisco WLC has OKC enabled by default. The lifetime of the cached PMKID is based on the timeout value received from the AAA server or the WLAN session timeout setting. On expiration, an EAP reauthentication is triggered.

While supported by the Cisco Wi-Fi infrastructure, the OKC technique has not been widely adopted or deployed. OKC is not suggested or described in the IEEE 802.11 standard and is consequently still not supported by many Wi-Fi Protected Access 2 (WPA2) devices.

Table 3. Opportunistic Key Cache Signaling Scaling

Opportunistic Key Cache Signaling Scaling	
0	SIM card exchanges
0	AAA exchanges between WLC and EAP server and intermediate proxies
0	EAP-SIM exchanges between smartphone and EAP server
4	Additional request/response exchanges (authentication, association, EAPOL, ...)
0	HLR queries

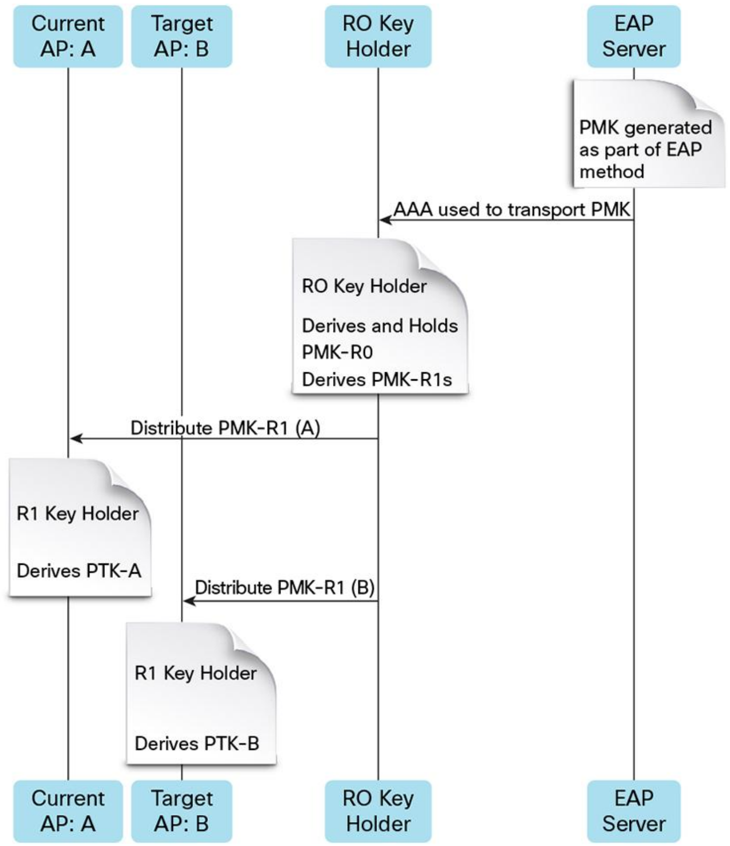
Figure 5. Opportunistic Key Caching



Fast Wi-Fi Mobility

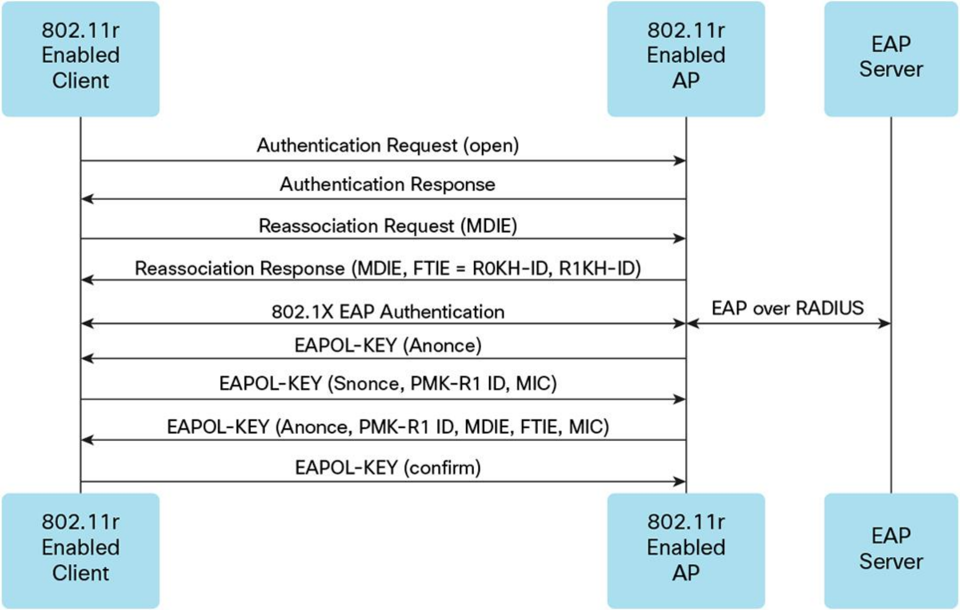
As highlighted in the previous section, one of the key challenges to address in scaling service provider Wi-Fi signaling is accommodating the mobility use cases whereby a Wi-Fi device roams from one access point to another. Compared with the OKC technique that relies on functionality that has not been defined in the IEEE 802.11 standard, IEEE 802.11r (Fast BSS Transition) introduces standardized roaming functionality, ensuring that mobility techniques are compatible between multiple vendor implementations. Fast transition (FT) capability uses a new keying hierarchy, as illustrated in Figure 6, together with an enhanced signaling procedure that enables an initial handshake with a new access point to be performed even before the client roams to the target access point. The initial handshake allows the client and access points to do the PTK calculation in advance. These PTK keys are applied by the client and access point after the client does the reassociation request or response exchange with the new target access point. The fast basic service set (BSS) transition introduced in 802.11r is a way to reduce latency during handover by eliminating the need for a complete authentication during handover.

Figure 6. IEEE 802.11r Keying Hierarchy



On initial connection to the service provider Wi-Fi network, the client performs a complete authentication using IEEE 802.1X procedures, as illustrated in Figure 7. However, in this instance, the client signals the mobility domain information element (MDIE) to the access point, indicating that it supports fast transition functionality. The access point responds with the identity of its R0 and R1 keying hierarchies. The client and EAP server complete the unmodified EAP exchange. With fast transition, the access point and client use the PMK to derive a key hierarchy referred to as PMK-RO, PMK-R1(A), and PTK-A. The PTK-A is used to secure traffic between the client and the current AP-A.

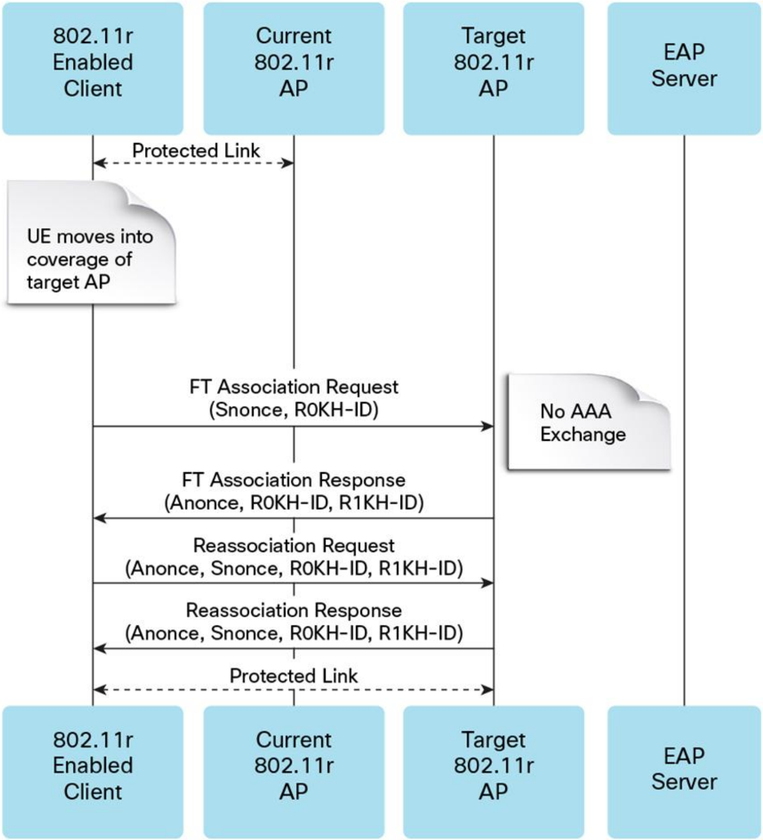
Figure 7. Fast BSS Transition - Initial Authentication


802.11r Enabled Client
802.11r Enabled AP
EAP Server
Authentication Request (open)
Authentication Response
Reassociation Request (MDIE)
Reassociation Response (MDIE, FTIE = R0KH-ID, R1KH-ID)
802.1X EAP Authentication
EAP over RADIUS
EAPOL-KEY (Anonce)
EAPOL-KEY (Snonce, PMK-R1 ID, MIC)
EAPOL-KEY (Anonce, PMK-R1 ID, MDIE, FTIE, MIC)
EAPOL-KEY (confirm)
802.11r Enabled Client
802.11r Enabled AP
EAP Server

Now, when the client transitions to the target AP-B, it provides the PMK-R0 key identifier in the authentication request. The target AP-B will confirm that it can derive a new PMK-R1(B) key based on the provided PMK-R0 identifier. The client and access point proceed to generate a new PTK-B to secure traffic between the client and the target AP-B. Importantly, from a signaling scaling perspective, this is achieved without any interaction with the AAA and/or EAP server, as illustrated in Figure 8.

In the WLC-based systems typically deployed in service provider environments, the authentication is done by the WLC, and the PMK-R0 is stored at the WLC. Consequently, when a client roams between two access points connected to the same WLC, the PMK-R1 is automatically available at the target access point. Furthermore, multiple WLCs may be configured in a mobility group, enabling the PMK-R1 to be shared between different WLCs. In such configurations, even when the client roams to a target access point that is associated with a different WLC, the target access point can still have access to the PMK-R1 and a fast BSS transition can operate successfully.

Figure 8. Fast Transition - Change of Access Point


802.11r Enabled Client
Current 802.11r AP
Target 802.11r AP
EAP Server
Protected Link
UE moves into coverage of target AP
FT Association Request (Snonce, R0KH-ID)
No AAA Exchange
FT Association Response (Anonce, R0KH-ID, R1KH-ID)
Reassociation Request (Anonce, Snonce, R0KH-ID, R1KH-ID)
Reassociation Response (Anonce, Snonce, R0KH-ID, R1KH-ID)
Protected Link
802.11r Enabled Client
Current 802.11r AP
Target 802.11r AP
EAP Server

Note that, as with OKC, the client performs EAP authentication only once when initially attaching to the service provider Wi-Fi network, and all subsequent reassociations do not involve AAA servers. Support for IEEE 802.11r has been added to iOS 6.0, and the WFA's Wi-Fi CERTIFIED Voice Enterprise certification program has been developed to ensure that interoperable, standards-based fast BSS transition implementations are available. In addition, from a protocol perspective, FT eliminates the four-way EAPOL key handshake messages, as highlighted in Table 4, leading to further reduction in handover latency. Hence, the key distinctions between fast BSS transition and OKC are the standardization and multivendor support, together with lower latency authentication.

Table 4. Fast Transition Signaling Scaling

Fast Transition Signaling Scaling	
0	SIM card exchanges
0	AAA exchanges between WLC and EAP server and intermediate proxies
0	EAP-SIM exchanges between smartphone and EAP server
2	Additional request/response exchanges (authentication, association, EAPOL...)
0	HLR queries

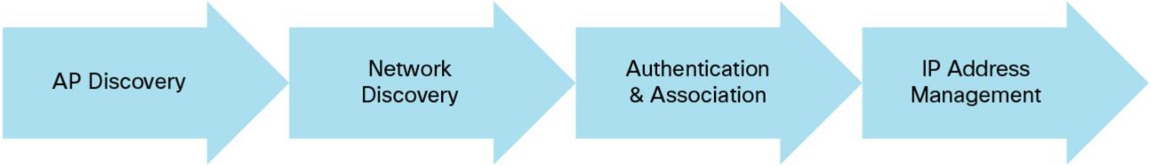
Legacy Wi-Fi clients cannot associate with a service provider Wi-Fi network that has IEEE 802.11r enabled if the driver of the supplicant has not been updated with the TGr Authentication and Key Management suites. In order to assist in the migration toward IEEE 802.11r FT, 802.11r allows two SSIDs with the same name but different security settings (FT and non-FT) to be configured on the service provider Wi-Fi infrastructure.

Fast Initial Link Setup

IEEE 802.11ai[4] is a proposed enhancement to the IEEE 802.11 standard to enable fast initial setup (FILS) for Wi-Fi devices (as of February 2014, IEEE 802.11ai is still an unapproved amendment). The goal of IEEE 802.11ai is for a Wi-Fi device to be able to associate, authenticate, and configure itself so that is able to send and receive packets within 100 ms of entering the coverage area of a Wi-Fi access point. In particular, from a service provider Wi-Fi perspective, reducing the time for link setup will facilitate the scaling of deployments in which a large number of wireless devices simultaneously enter the coverage of a Wi-Fi access point.

The initial link setup can be split into four distinct phases, as shown in Figure 9. Importantly, from an alignment perspective, FILS uses the Generic Advertisement Service (GAS) protocol that is the foundation for delivering Passpoint's Access Network Query Protocol (ANQP) service, enabling the wireless device to recover contextual information from the access point prior to association.

Figure 9. Four Phases of Initial Link Setup



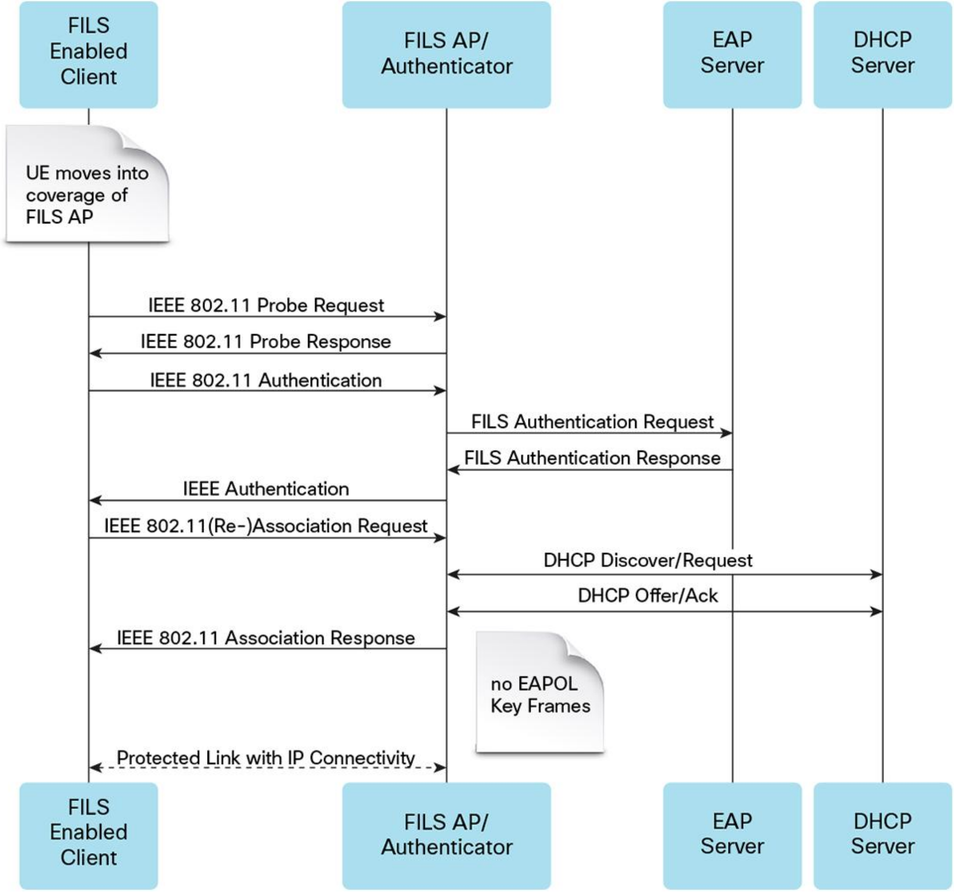
In terms of the access point discovery and network discovery phases, the scanning procedures have been updated with FILS to enable the access point to signal neighbor access point information in beacon, probe response, and fast discovery (FD) frames. The FD frame is a small frame that can be transmitted between beacons to speed up access point and network discovery. This enables the Wi-Fi device to improve its scanning operations, including reducing the chance that it will waste time scanning channels with no access points.

Furthermore, the legacy IEEE 802.11 device may spend several seconds in secure initial link establishment, including the time required to sequentially transmit messages for IP address assignment. FILS addresses this time required for authentication and association by using the EAP-Reauthentication protocol as defined in RFC 6696. On initial connection to the WLAN, the client performs a complete authentication using IEEE 802.1X procedures. In addition to generating the PMK and PTK, the client and AAA server generate another set of keys for FILS operation. The AAA server does not share these keys with the current IEEE 802.1X port-based authenticator (WLC or access point). When the client transitions to a target access point, the client discovers that the target access point supports FILS. In such a case, the client sends an EAP-Initiate element within the authentication request. The EAP element is integrity protected based on FILS keys generated during the initial connection. The AAA server can then validate the client identity and provide the target access point with a PMK used for authenticating the client. Using the PMK, the target generates a new PTK.

[4] IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 7: Fast Initial Link Setup

In addition to decreasing the number of round trips associated with EAP authentication, FILS enables IP address assignment to be piggybacked onto the FILS exchange. This means that authentication, four-way handshake, association, and higher-layer setup, including IP address assignment, are completed in two round-trip signaling messages, as shown in Figure 10.

Figure 10. FILS 4-Way Handshake


FILS Enabled Client
FILS AP/ Authenticator
EAP Server
DHCP Server
UE moves into coverage of FILS AP
IEEE 802.11 Probe Request
IEEE 802.11 Probe Response
IEEE 802.11 Authentication
FILS Authentication Request
FILS Authentication Response
IEEE Authentication
IEEE 802.11(Re-)Association Request
DHCP Discover/Request
DHCP Offer/Ack
IEEE 802.11 Association Response
no EAPOL Key Frames
Protected Link with IP Connectivity
FILS Enabled Client
FILS AP/ Authenticator
EAP Server
DHCP Server

FILS EAP enhancements are primarily applicable where the target access point cannot establish new keys with the Wi-Fi device without completing an EAP exchange. The applicability of such in a service provider Wi-Fi environment may therefore be limited to use cases that look at supporting enhanced mobility between autonomous Wi-Fi access points, for example in a residential environment, or in a multivendor WLC environment where IEEE 802.11r FT may not be supported when roaming between multivendor access points.

Table 5. FILS Signaling Scaling

FILS Signaling Scaling	
0	SIM card exchanges
1	AAA exchanges between WLC and EAP server and intermediate proxies
0	EAP-SIM exchanges between smartphone and EAP server
2	Additional request/response exchanges (authentication, association, EAPOL...)
0	HLR queries

Service Provider Wi-Fi Approaches to Manage Signaling Exchange Scaling

The previous section described the wide variety of techniques that can be used within the Wi-Fi network to reduce the amount of signaling generated as service provider Wi-Fi users attach to the network and/or roam between service provider Wi-Fi access points. This section looks at additional techniques that can be used within the service provider Wi-Fi network to manage the resulting signaling exchange scaling.

WLC Tools for Preventing Signaling Overload

In a controller-based service provider Wi-Fi network, the WLC can provide significant benefits in terms of scaling the signaling system. In particular, the techniques described in the previous section are typically realized by the WLC. For example, the Cisco WLC supports:

- Opportunistic PMKID caching
- Sticky key caching
- Fast BSS transition

In addition to these standardized techniques, the WLC can provide rate limiting functionality, for example, to be able to handle a sudden influx of users. To address such use cases, the WLC can prevent such signaling overload by limiting the association rate for connecting Wi-Fi devices.

> The Cisco WLC supports the ability to control the rate at which clients are able to associate with the service provider Wi-Fi system through the following command:
>
> **config advanced assoc-limit** [number of associations per interval][interval in milliseconds]
>
> When a client tries to associate, it will receive the status code "**Association denied because AP is unable to handle additional associated STAs**" in the association response.

In addition to basic association rate limiting, because Passpoint relies on Generic Advertisement Service (GAS) signaling, a sudden influx of users into the coverage of a Passpoint-enabled access point will trigger a flood of GAS requests. Such an influx can be controlled by rate-limiting the GAS requests by the WLC.

> The Cisco WLC supports the ability to configure the GAS request threshold to limit the number of GAS request action frames that can be sent to the WLC by an access point, using the following command:
>
> **config advanced hotspot gas-limit** [num-of-GAS-required][interval in milliseconds]
>
> When the threshold is passed for an access point, GAS requests are dropped at the access point, thus limiting the ability of affected Wi-Fi devices to fully discover the Wi-Fi network and hence delay association and subsequent EAP signaling.

Finally, scaling the service provider Wi-Fi network will most likely involve deploying multiple WLC instances. To balance the load between individual WLCs and avoid overloading a single element, the Control and Provisioning of Wireless Access Points (CAPWAP) discovery phase enables the access point to discover the WLC type, the total capacity, and the current access point load of the controller, enabling the access point to fall back to a less loaded WLC.

EAP Server Tools for Preventing Signaling Overload

Given the potential impact of Wi-Fi-based EAP-based authentication on HLR and HSS scalability, both the EAP-SIM and EAP-AKA specifications include optional capabilities to support “fast” reauthentication. “Fast” reauthentication has been included in these EAP methods to avoid having to query the HLR/HSS for reauthentication exchanges. The operation of fast reauthentication with EAP-SIM is illustrated in Figure 11. Table 6 shows how the configuration of EAP-SIM fast reauthentication reduces the EAP and AAA exchanges and avoids any SIM card/HLR exchanges.

Figure 11. EAP-SIM Fast Reauthentication

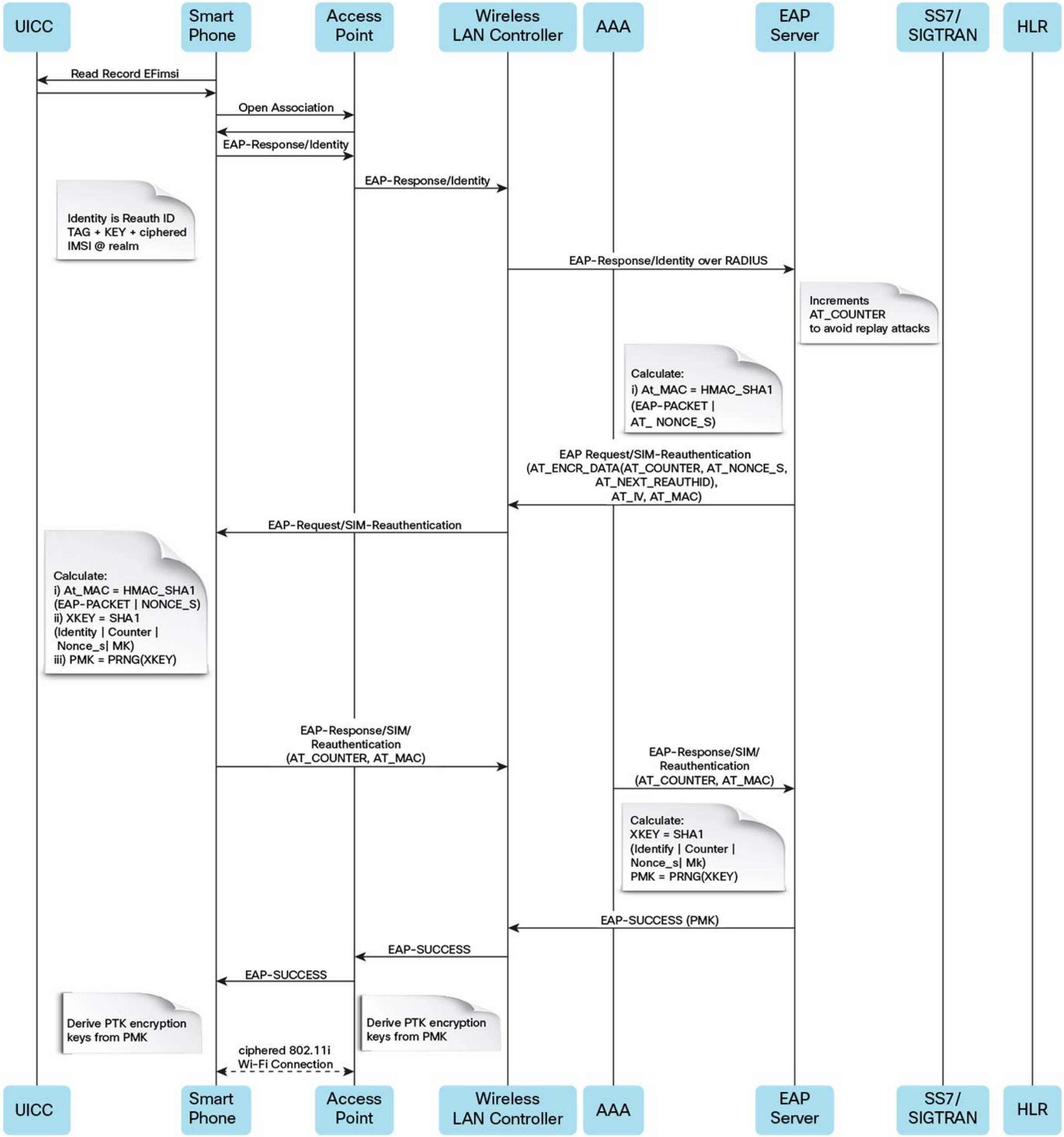

UICC
Smart Phone
Access Point
Wireless LAN Controller
AAA
EAP Server
SS7/ SIGTRAN
HLR
Read Record EFimsi
Open Association
EAP-Response/Identity
EAP-Response/Identity
Identity is Reauth ID TAG + KEY + ciphered IMSI @ realm
EAP-Response/Identity over RADIUS
Increments AT_COUNTER to avoid replay attacks
Calculate: i) At_MAC = HMAC_SHA1 (EAP-PACKET | AT_ NONCE_S)
EAP Request/SIM-Reauthentication (AT_ENCR_DATA(AT_COUNTER, AT_NONCE_S, AT_NEXT_REAUTHID), AT_IV, AT_MAC)
EAP-Request/SIM-Reauthentication
Calculate: i) At_MAC = HMAC_SHA1 (EAP-PACKET | NONCE_S) ii) XKEY = SHA1 (Identity | Counter | Nonce_s| MK) iii) PMK = PRNG(XKEY)
EAP-Response/SIM/ Reauthentication (AT_COUNTER, AT_MAC)
EAP-Response/SIM/ Reauthentication (AT_COUNTER, AT_MAC)
Calculate: XKEY = SHA1 (Identify | Counter | Nonce_s| Mk) PMK = PRNG(XKEY)
EAP-SUCCESS (PMK)
EAP-SUCCESS
EAP-SUCCESS
Derive PTK encryption keys from PMK
Derive PTK encryption keys from PMK
ciphered 802.11i Wi-Fi Connection
UICC
Smart Phone
Access Point
Wireless LAN Controller
AAA
EAP Server
SS7/ SIGTRAN
HLR

Table 6. Fast EAP-SIM Reauthentication Signaling Scaling

Fast EAP-SIM Reauthentication	
0	SIM card exchanges
2	AAA exchanges between WLC and EAP server and intermediate proxies
2	EAP-SIM exchanges between smartphone and EAP server
0	HLR queries

Both EAP-SIM and EAP-AKA include functionality that is able to limit the number of successive fast reauthentications without a full authentication exchange. Both the EAP-SIM/EAP-AKA supplicant and sever should have an upper limit on the number of subsequent fast reauthentications allowed before a full authentication needs to be performed. The counter that controls this operation corresponds to a 16-bit number, and so in theory the protocol allows for over 65,000 fast reauthentications before a full reauthentication is required.

Cisco Prime™ Access Registrar supports EAP-SIM and EAP-AKA authentication methods. Cisco Prime Access Registrar offers the following controls over the operation of fast reauthentication signaling optimization:

EnableReauthentication [True | False]

MaximumReauthentications [Reauth Counter]

ReauthenticationTimeout [Reauthentication timeout]

The default Cisco Prime Access Registrar configuration enables fast reauthentication to be performed 16 times before a subsequent full authentication is required and requires subscribers to perform a full authentication every 3600 seconds.

AAA Tools for Preventing Signaling Overload

Because service provider Wi-Fi systems may be used in roaming scenarios, a home AAA system may be connected to a number of different Wi-Fi access systems. The RADIUS proxy should therefore be configured to be able to continue operation when experiencing sudden increases in RADIUS traffic coming from the different access networks.

Cisco Prime Access Registrar Director provides a set of capabilities built for intelligent RADIUS load balancing and proxying. Cisco Prime Access Registrar Director redirects packets based on its policy engine or customized extension points, providing intelligent load balancing capabilities.

Cisco Prime Access Registrar offers two options to tackle traffic bursts by limiting incoming AAA traffic using the “enforce traffic throttling” property when defining AAA clients.

The number of incoming AAA packets per AAA client can be limited using the following property:

MaximumIncomingRequestRate [allowed requests per second]

Similarly, Cisco Prime Access Registrar can also be configured to limit the number of outstanding requests per AAA client, using the following property:

MaximumOutstandingRequests [requests processed per second]

When a burst of AAA requests are received that exceed the configured thresholds, Cisco Prime Access Registrar will drop those excessive requests.

Tools for Preventing Signaling Overload in SS7 Networks

When Cisco Prime Access Registrar connects to the backend SIGTRAN-M3UA system, it can be configured to limit the number of outstanding requests per remote server (back-end system) based on the MaximumOutstandingRequests property described above. When the number of requests exceeds this number, Cisco Prime Access Registrar queues the remaining requests, sending them as soon as the number of outstanding requests drops below the configured threshold.

Summary of Techniques for Scaling Signaling Transactions in Service Provider Wi-Fi Networks

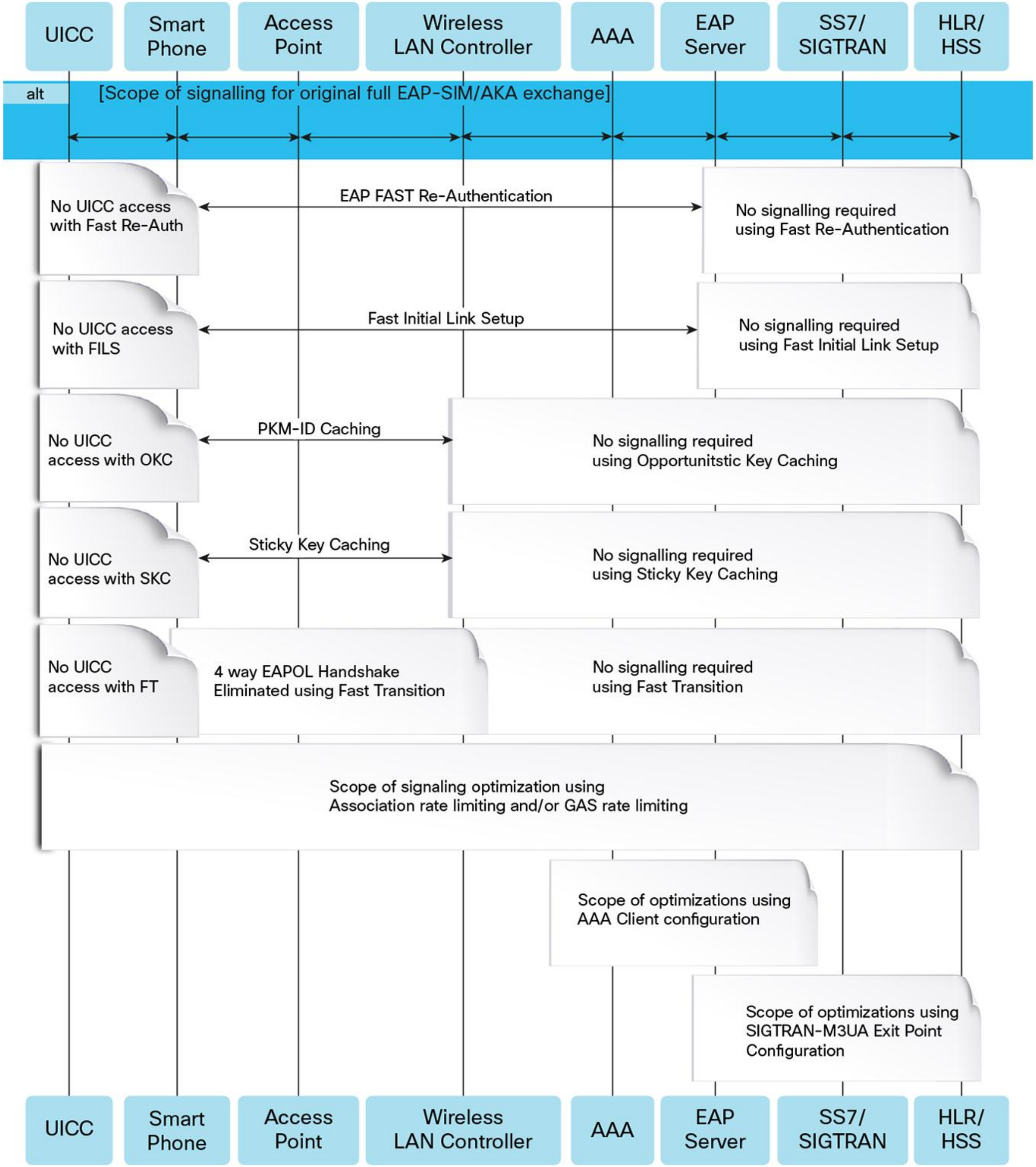
The wide-scale adoption of Passpoint-certified mobile devices and operation of EAP-SIM and EAP-AKA will bring new scalability challenges to service provider Wi-Fi networks and their mobile network operator partner networks.

This white paper has described a range of techniques for addressing signaling scale within service provider Wi-Fi networks. Importantly, driven by a need to enhance the user experience when connecting to Wi-Fi networks, Cisco has developed a proven set of capabilities that can significantly ease the burden of signaling when using EAP based authentication in Wi-Fi networks. Figure 12 provides a summary of the scope of techniques described in this paper.

Further, the white paper has described the configuration options of Cisco’s AAA and EAP server functionalities that can be used to address signaling scaling and enable back-end systems to be protected from any signaling storms. Where appropriate, configuration commands have been highlighted that enable signaling optimization on the Wi-Fi network, AAA infrastructure, and EAP-SIM/AKA servers.

Using the breadth of techniques being defined by the industry and enabled on Cisco Service Provider Wi-Fi infrastructure, operators can be confident that their Passpoint deployments will be able to scale to accommodate the enhanced ease of use that will accompany EAP-SIM/AKA deployments.

Figure 12. Summary of Optimization Techniques and Their Scopes


UICC
Smart Phone
Access Point
Wireless LAN Controller
AAA
EAP Server
SS7/ SIGTRAN
HLR/ HSS
alt
[Scope of signalling for original full EAP-SIM/AKA exchange]
No UICC access with Fast Re-Auth
EAP FAST Re-Authentication
No signalling required using Fast Re-Authentication
No UICC access with FILS
Fast Initial Link Setup
No signalling required using Fast Initial Link Setup
No UICC access with OKC
PKM-ID Caching
No signalling required using Opportunitstic Key Caching
No UICC access with SKC
Sticky Key Caching
No signalling required using Sticky Key Caching
No UICC access with FT
4 way EAPOL Handshake Eliminated using Fast Transition
No signalling required using Fast Transition
Scope of signaling optimization using Association rate limiting and/or GAS rate limiting
Scope of optimizations using AAA Client configuration
Scope of optimizations using SIGTRAN-M3UA Exit Point Configuration
UICC
Smart Phone
Access Point
Wireless LAN Controller
AAA
EAP Server
SS7/ SIGTRAN
HLR/ HSS

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 C11-731038-00 03/14