January 2020

# OPTIMIZED SIMULTANEOUS AUTHENTICATION OF EQUALS (SAE) IDENTITY PRE-SHARED KEY (IPSK)

Abhishek Dhammawat

Shreshta Besagarahalli Manu

Namsoo Kim

Mansi Jain



# OPTIMIZED SIMULTANEOUS AUTHENTICATION OF EQUALS (SAE) IDENTITY PRE-SHARED KEY (IPSK)

AUTHORS:

Abhishek Dhammawat
Shreshta Besagarahalli Manu
Namsoo Kim
Mansi Jain

## ABSTRACT

Presented here are techniques for the residential deployment of common Wi-Fi® services with an optimized Simultaneous Authentication of Equals (SAE) Identity Pre-Shared Key (iPSK) flow. The techniques presented herein avoid the use of an Authentication, Authorization, and Accounting (AAA) server for clients whose entries are absent through the upfront use of bloom filter information provided by an AAA server. The techniques presented herein can also be used for Wi-Fi Protected Access II (WPA2) iPSK optimization or SAE (Wi-Fi® Protected Access 3 (WPA3) personal), which has more latency sensitive call flow due to SAE auth commit timeouts consideration.

## DETAILED DESCRIPTION

Today, personal Wireless Local Area Networks (WLANs), such as WPA2 Pre-Shared Key (PSK) and WPA3 SAE, are widely used by customers in places such as residential apartments, motels, restaurants, etc. There is a concern regarding the network security when using such WLANs. For example, in a multi-tenant apartment building, managed Wi-Fi is a service that may be provided by a landlord or association. Each apartment tenant will connect to the same single Service Set Identifier (SSID) and a common password may be provided to each tenant. The use of a common password creates a significant security issue (e.g., when a tenant leaves the apartment, as well as with the password being common is available to move-out tenants). As such, the there is a need to provide individual passwords that are unique to each tenant.

As illustrated by the above example, it is common place that all users of a WLAN use a common/shared password to connect to the WLAN. Such setup is typically a WPA2-Personal network deployment where all tenants share same SSID but have their unique password for using common Wi-Fi connectivity. WPA3-Personal aka Simultaneous Authentication Of Equals (SAE) is robust to offline, dictionary, and brute force attacks. However, even SAE is vulnerable (e.g., in above multi-tenant apartment building deployment) to attacks using a single one time password guess to implement an active attack.

One solution to this issue is to provide private password to each user who is going to connect to a WLAN, such as Identity PSK (iPSK) based on Media Access Control (MAC) addresses. For iPSK, the password for each client MAC address is typically configured in the AAA server. Every time a client wants to associate to a WLAN that has MAC filtering configured, the AAA server has to be queried to obtain the password configured for the client and use it for association. The password is required during association for WPA2 PSK and for WPA3 SAE authentication.

There are use-cases where some users/guests are given a common WLAN password and the entries for such client's MAC address are not configured in the AAA server, but the user can still connect to the WLAN with a pre-configured WLAN password. This causes latency (especially in clustered Wireless LAN Controller (WLC) cloud deployment) during the association process, even though the client is using the default WLAN password. This latency is because the Access Point (AP)/WLC still has to wait for the AAA server to process whether the client was configured with a password.

FIG. 1, below, illustrates a standard/conventional SAE iPSK call flow.

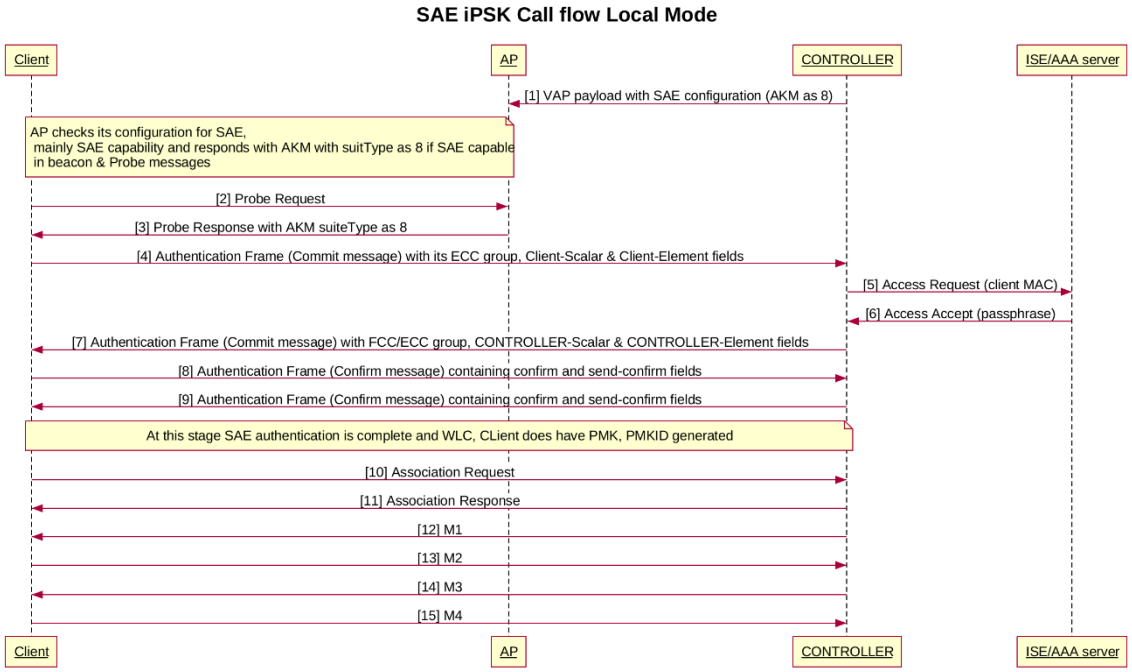


**FIG. 1**

There are a number of improvements required with the standard SAE iPSK shown in FIG. 1. For example, in the above standard call flow of FIG. 1, the clients can timeout or attempt to roam to another AP if there is significant latency between messages 4 and 7. This will be dependent on the ISE message exchange and, typically, a client's SAE auth commit timeout is in milliseconds, thus it can be a deployment impact issue specifically in cloud multi-cluster WLC deployments. As such, it would be possible to reduce AAA/ISE load by avoiding contacting the AAA server for clients for which it is known that the AAA server does not have the password and policy details. In addition, for clients who are guests and don't have an entry in the AAA server, there is no need to contact the AAA server to obtain the password and policy information. When the password and policy information is absent for those clients, the WLC/AP could fallback to use the WLAN password. However, the above access request and response with the AAA server leads to latency in client association and, in particular, in cloud deployments. In addition, in SAE iPSK, as a client is waiting for auth commit, timeout can occur if there is more latency. Overall, it may be possible to reduce network load and messages for ISE communication.

FIG. 2, below, illustrates a call flow in accordance with the techniques presented herein.

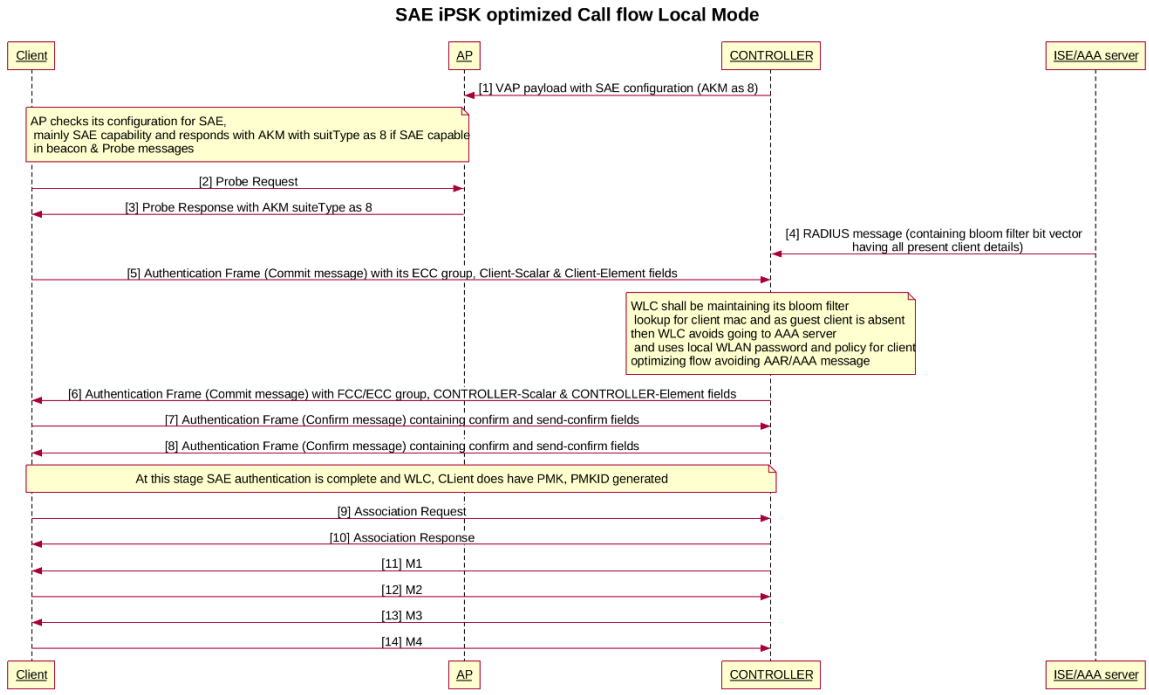


**FIG. 2**

In FIG. 2, flow message 4 is not per client, but instead an out of band periodic RADIUS message containing consolidated bit vector bloom filter details for all clients present in the AAA server. The AAA server and WLC shall have similar hash functions/logic to utilize the shared bloom filter details during lookup at the WLC. For guest clients sure to be absent in the bloom filter, the WLC shall avoid messages AAR/AAA (5,6 in above standard flow), thus reducing latency for client association and load on the AAA server as well.

In accordance with the techniques presented herein, the client (apartment tenant) join/association flow shall be as below:

1. Client provisioning in the AAA server or ISE shall be done as it's done today with ISE having entries for the client MAC PSK/SAE password and other policies.

2. The AAA server or ISE shall maintain a bloom filter for all the client MACs having common bit vector and send the same to WLC.
3. The AAA server periodically sends this bloom filter bit vector details to the WLC containing the client entries bit vector details for which it has entries.
4. When a client tries to associate to the WLC/AP, the WLC/AP it will check whether that client is absent "definitely not present" using the bit vector provided by the AAA and with input as client MAC. If client is present which will be in this case then WLC shall be knowing that client entry is present in AAA server so shall be going to AAA server using Access request/accept as done today.

In accordance with the techniques presented herein, the client (guest) join/association flow shall be as below:

1. The AAA server periodically sends this bloom filter bit vector details to the WLC containing the client entries bit vector details for which it has entries as mentioned above.
2. When a guest client tries to associate to the WLC/AP, the WLC/AP then it will check that the client is absent "definitely not present" using the bit vector provided by the AAA and with input as client MAC.
3. In this case, the client MAC shall be absent in bloom filter then it will indicate that the client MAC is absent at the AAA server. The WLC shall utilize the locally configured WLAN password and local policy, thereby avoiding contacting the AAA server and saving the flow for the WLC to the AAA server of Access request/accept.

In accordance with the techniques presented herein, the client removal from the AAA server (tenant moving out but visited as guest) flow shall be as follows:

1. The AAA server shall be updated with removal of client MAC entry.

2. The AAA server shall provision the updated bloom filter (periodically for optimized performance) to the WLC.
3. When a client joins and an entry is not found in the bloom filter, then the client association flow shall use local WLAN password and policy avoiding going to the ISE.

Another case when, during the periodic refresh, the client is removed from the AAA server, but the bloom filter is not updated at the WLC (transient), then the flow shall be as follows:

1. The WLC finds the client entry in the bloom filter and attempts to send the AAR to the AAA server.
2. The AAA server notifies the WLC that the client is absent and there is a fallback to the WLAN password or configuration

FIG. 3, below, illustrates aspects of the techniques presented herein. In FIG. 3, the client 1) is not configured, which maps to the guest case described above. The client 2) is configured, which maps to tenants using common WIFI service. Client 3) is also not configured, which is the refresh window case when client is removed from the AAA server, but periodic bloom filter update is not received at the WLC and, for those few clients, the WLC still contacts the AAA server and there is fallback to the WLAN password.

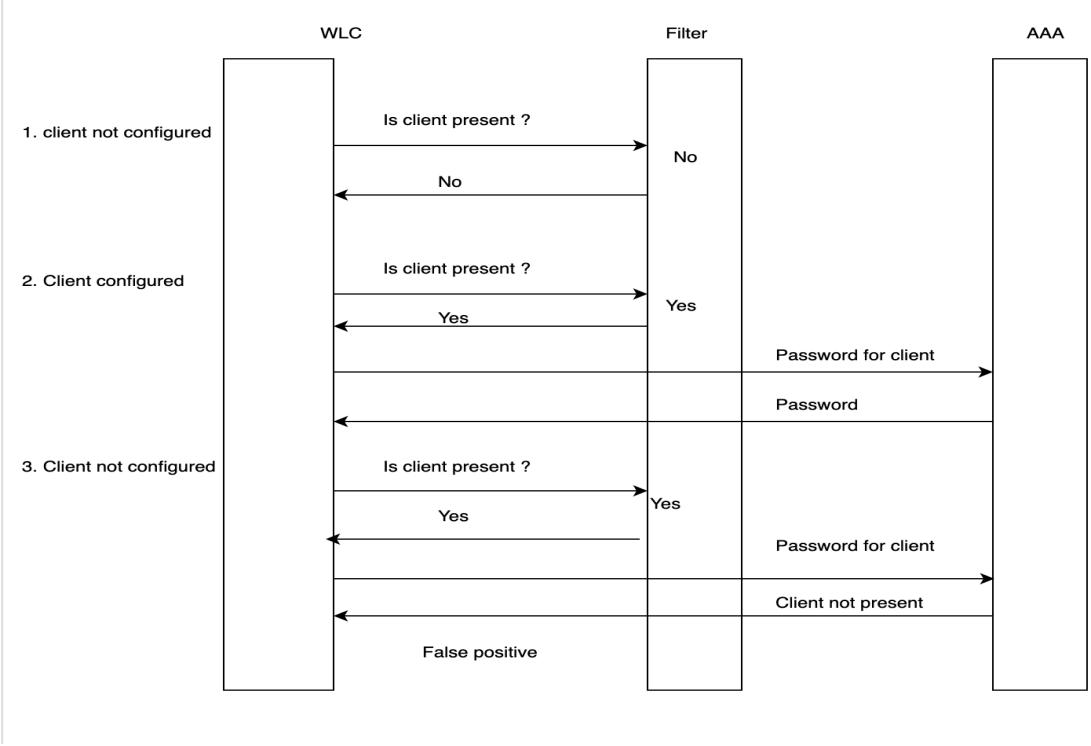


**FIG. 3**

Accordingly, even during this refresh window where the client bloom filter if not updated, the operation is acceptable. In particular, those clients removed from AAA server during this refresh windows shall result in a query and a fallback to the WLAN password.

In another embodiment the bloom filters can be configured per client MAC and per WLAN.

A still other solution approach is:

- Out of band AAA server provides (using RADIUS COA) the WLC with client MAC detail/presence.
- The WLC just maintains the client presence in local bloom filter.

- On client association, the WLC uses the local maintained bloom filter for the identification of whether to use locally configured password and policy for client association or contact the AAA server.
- This method is different from previously mentioned approaches in the sense only the client MAC is shared with the WLC by the AAA server. This is also an efficient embodiment/variation as the WLC need not maintain client DB for clients, which can be huge in number as it is not possible to know when and who will be joining and just maintains bit vector for bloom filter for lookup.