# Network based Aggregation Server for Federated WiFi Access

Yogendra Shah, Yousif Targali
InterDigital Communications, Inc.
781 Third Ave, King of Prussia, PA 19406, USA
{Yogendra.Shah,Yousif.Targali}@InterDigital.com

Andreas U. Schmidt,
Lakshmi Subramanian, Aamer Chaudry
Novalyst IT AG
Robert-Bosch-Strasse 38, 61184 Karben, Germany
Andreas.Schmidt@Novalyst.de

***Abstract* — With the move towards mobility and the use of smartphones for connected services, there is an increasing need to provide users with seamless and automated authentication to securely access heterogeneously connected networks. We provide an overview of how Federated Identity systems may be utilized to provide seamless and secure access to WiFi networks. This can facilitate the offload of mobile data traffic to WiFi hotspots in locations such as at cafes, airports, malls, and hotels and also cater to scenarios such as online sign-up for WiFi hotspot access and secure access to home WiFi APs.**

***Keywords — federated identity, seamless handoff, authentication, automated WiFi access.***

## I. INTRODUCTION

With the increasing use of smartphones and the need to offload mobile data traffic to WiFi hotspots, in locations such as cafes, airports, malls, hotels, etc., comes a need to provide robust security yet, at the same time, simplify and accelerate the transition and switch from one network to another. This includes scenarios where users arrive at a hotspot, move from one hotspot to another, as well as when they move from a mobile network to a hotspot.

One key component to enable this is a smooth connection to the hotspot network with no or minimal user intervention. Various solutions exist and are being developed to facilitate this handoff functionality at a protocol level, especially those being specified by the WiFi Alliance (WFA) [1, see 2 for an overview] in specifying automated transition and strong security for hotspot networks. The WFA has specified several requirements to facilitate secure and automated connectivity to WiFi networks using various EAP methods [3] which automate the process and provide seamless network access to users. The WFA is also currently developing solutions for Online Sign-Up (OSU) for those users who wish to gain access to a hotspot network but are unknown to the hotspot network and do not have an affiliation with an operator.

We show how federated identity systems may be used to create a persistent security association at the application layer and which may then be subsequently used to drive the security protocols at the access layer. The goal of our work is to demonstrate the viability and benefits of a unified and integrated architecture, in which operators, WiFi hotspot network service providers as well as identity providers (IdPs) with large user bases such as Google, Facebook, Yahoo, and hotspot aggregators etc. (generically called Over-The-Top or OTT service providers) can connect in a federated fashion to secure, automate and simplify usage of hotspot networks by users. i.e. making it a three way federation. We also wish to fulfill the intent of the WFA HotSpot 2.0 requirements by providing a high grade of security to the broadest reach of hotspot service providers from legacy hotspots to new hotspots and even home APs with a low install and operational cost.

Additionally, our approach can enable not only data offloading to WiFi hotspots but also facilitate session continuity through being compatible with the mechanisms currently being proposed in the IEEE 802.11ai Fast initial Link Setup (FILS) work group activity [4].

## II. OVERVIEW OF FEDERATED WIFI ACCESS SYSTEM

There are many challenges to providing users with seamless and secure access to WiFi hotspots such as:

- Enabling hotspot service providers to provide hotspot service to their users without incurring high costs in terms of equipment (e.g. replacing existing equipment with WFA HS2.0 compliant equipment) and establishing multiple service level agreements (SLA) with operators.
- Providing users who do not have a relationship with an operator to access hotspot services through a simplified and preferably transparent OSU authorization and agreement to terms and conditions.

We propose the introduction of an Aggregator and User Authentication Facilitator (AUAF), an entity which can facilitate authentication of users to a hotspot network and at the same time act as an aggregator entity. On the one hand providing hotspot service providers simplified access to a trustworthy entity in the cloud for automated authentication and seamless access to hotspot services and on the other hand acting as an aggregator entity, which can establish service level agreements with multiple operators to facilitate access to operator controlled credentials for authentication by multiple hotspot service providers. The AUAF acts as an online service

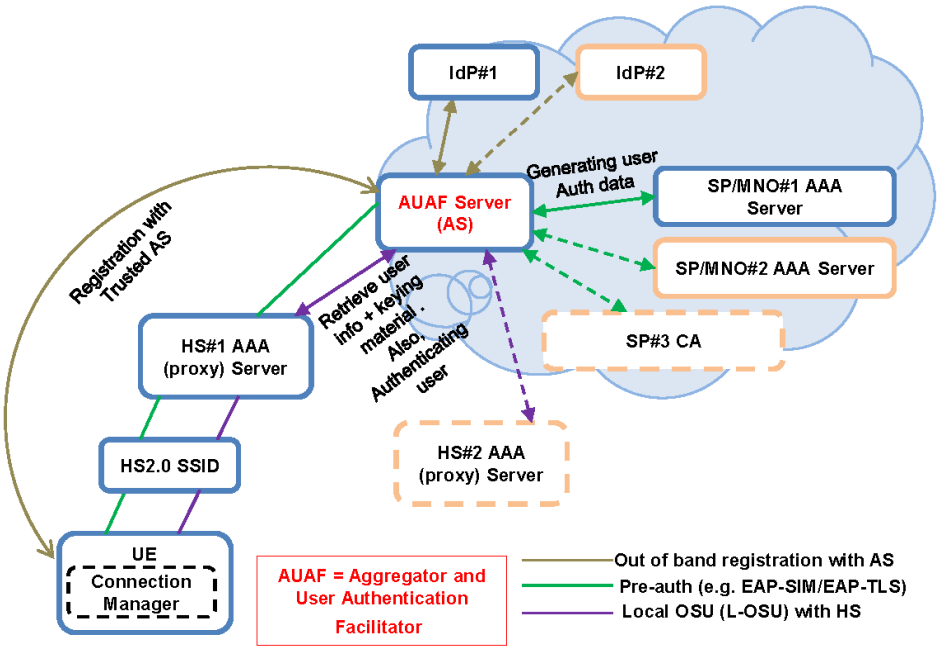


Fig. 1. Network Architecture using an AUAF Server.

for federation of user identities for the specific purpose of provisioning hotspot service access.

The authenticator function of the AUAF uses a simplified application layer protocol, which helps hotspot service providers by eliminating the need to install infrastructure elements, interfacing to multiple operator authentication servers, and at the same time removing the need to establish a SLA for each operator whose customers they wish to service. The authenticator function provide a means to support a variety of authentication protocols including EAP-SIM, EAP-AKA, EAP-TLS and EAP-TTLS as specified by WFA HS2.0 [1], through a federated delegation protocol. The AUAF also assists operators, especially mobile network operators, by reducing the number of SLAs they need to establish with hotspot service providers and at the same time, reducing the security risk involved in broadening the scale of 3rd party entities interfacing to their authentication infrastructure.

The aggregator function aids the OSU process for hotspot service providers by making it more attractive to users of hotspots by serving as a trustworthy intermediary, known to users due to an application layer affiliation such as a social networking (OTT) or other service function. Once registered with the AUAF server, users may connect to all hotspots that are integrated to work with the AUAF server using a simple process, thereby eliminating the privacy concerns and often frustrating process of user registration, especially when the user tries to connect using a mobile device. The AUAF maintains user subscriptions to hotspot services, and all necessary user profile information for the use of hotspot networks is also available including pre-accepted terms and conditions information for the hotspots. Finally, the AUAF server facilitates seamless mobility between cellular and WiFi networks by enabling the dynamic provisioning of credentials, which may be used at a hotspot network when a user roams to a new network.

In our proposed architecture, the network attachment process is broken down into multiple phases as follows:

- Phase 1 performs the registration process for the user, as a result of which the user profile and subscription information becomes available at the AUAF server for further use in subsequent phases when the user wishes to connect to a hotspot network having no relationship with his/her home operator. The user may already be registered with some commonly used identity providers such as Google, Facebook or some other OTT service provider. The OTT may then provide a registration process to gather basic user information such as user identity (e.g., email address), personal info (e.g., personal address, credit card details etc.) together with the authentication credentials of their Station/UE. In this approach, at the end of the OSU registration process, the AUAF relieves the user from the cumbersome process of registration when approaching a hotspot where he otherwise would have had to perform a registration to gain access to its services. Only minimal user intervention is required and most of the provisioning and billing functionality is handled by the different network entities themselves.
- Phase 2 referred to as Pre-Authentication performs an authentication procedure between the Station/UE and the Operator (e.g., a Mobile Network Operator (MNO), or cable operator) wherein the AUAF acts as an intermediary to dynamically derive access credentials to enable connectivity to the hotspot.
- Phase 3 allows the user to securely connect to the hotspot network using the dynamically generated and provisioned credentials from the previous phase.

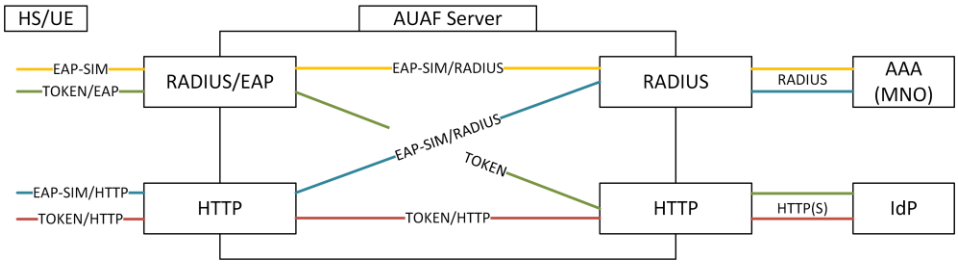


Fig. 2. AUAF Server Multiplexing between Different Application-layer Protocols.

## III. System Operation Using the AUAF

The functions of the AUAF server in the network along with the other entities required in the process of OSU and user authentication, its different roles in the different connectivity phases are briefly described in this section.

### A. Network Architecture with AUAF

A high level network architecture diagram of the AUAF server with its different phases is shown in Figure 1. UE represents user equipment which contains the WiFi connection manager. HS2.0 SSID corresponds to the WiFi hotspot SSID to which the UE wishes to connect. The AUAF server acts as an entity which interacts with and provides information to the hotspot networks, and aggregates information from the identity providers and the SP (Service Provider)/MNO AAA servers. Optionally, there could also be an AAA server at every hotspot which acts as a relay server forwarding the authentication and other requests towards the AUAF.

### B. Functions of the AUAF

From the AUAF network architecture, different functions are performed in each of the network attachment phases described previously. The main functional blocks are described below.

*1) Proxy OSU Server:*

In the first phase, registration, the AUAF server federates and aggregates information across existing IdPs bearing user information and allows users to provide additional information such as subscription preferences, payment information and also to pre-accept terms and conditions for the different hotspot networks. This function is usually carried out by the OSU server which builds the user subscription profile.

In the second phase, pre-authentication, the AUAF server may interact with several SPs/MNOs AAA Servers that might be needed for initial user authentication. The AUAF server, being a trusted intermediary, can provide user profile information that it gathered during phase one to the SP/MNO AAAs as needed in the OSU process. In this way, the AUAF server exhibits close similarity to the functions of a typical OSU server and hence can be referred as the “Proxy OSU Server".

*2) Proxy AAA Server:*

In the third phase, secure access, the AUAF server behaves like a Proxy AAA server as it authenticates the user on behalf of the SP/MNO´s AAA server. This is possible because during phase two, the pre-authentication, the AUAF server is provisioned with the authentication credentials that are required for successive authentications of the user/UE. Thus the user/UE, who is trying to gain secure access to the HS network, can be authenticated by the AUAF server without interaction with the SP/MNO core AAA servers.

*3) Remediation Server:*

The AUAF server has all the user profile and subscription related information and also the authentication credentials, therefore any account or credential related remediation could also be initiated and processed by the AUAF server. For example, when the user authentication credentials have expired, they must be renewed. This is because after the expiry of those credentials, the AUAF Sever can no longer authenticate the user on behalf of the SP/MNO AAA. When the AUAF server encounters expired authentication credentials for user profiles, it can act as the Remediation Server and run phase two (pre-authentication) again between the user/UE and the respective SP/MNO AAA.

*4) Network Hiding Gateway:*

Since the AUAF server is the entity which mainly interacts with the hotspot networks on behalf of the SP/MNO AAA Servers, the SP and in particular the SP/MNO AAA servers and other important entities are not exposed directly to third parties such as the hotspot operators. Thus, the AUAF acts as a network hiding gateway for the SP/MNO’s core network, providing protection of the SP/MNO’s core network against the outside world.

*5) Identity Provider (OTT):*

The main function of the AUAF architecture is to interconnect identity providers of various kinds with wireless access networks and network providers. The OTT IdPs bear user information and identities and handle them at the application layer, and also facilitate user authentication. In a collapsed deployment, the AUAF function may be absorbed into the OTT creating new business opportunities for the OTT to provide network connectivity services to their users.

### C. System Operation

*1) Protocol Multiplexing Functionality of AUAF*

In the different phases discussed above to obtain connectivity, the AUAF server acts as a central entity that is coordinating with the different hotspot networks, identity providers and the MNO AAAs. To provide the interoperability between different entities, the AUAF server has to support multiple protocols with which these entities may communicate. To enable this trust and communication relationship between these entities, it becomes important for

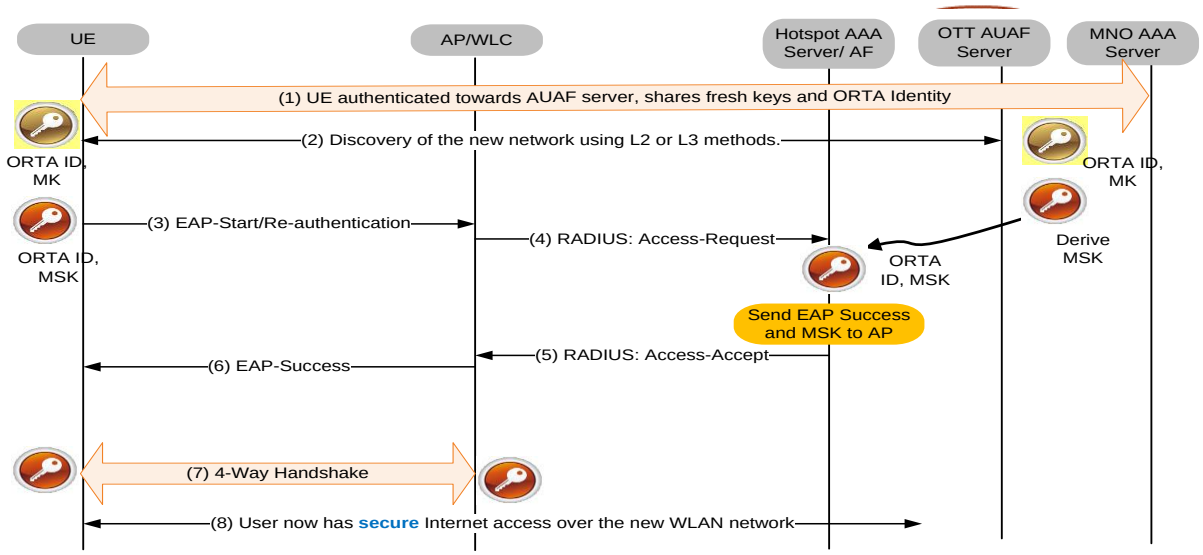


Fig. 3. Call Flow for Seamless Authentication and Mobility using AUAF

the AUAF server to also behave like a protocol multiplexer, thereby enabling it to interpret the messages sent to it using different protocols and also to relay messages between these entities in the protocol they understand. Figure 2 above explains the concept of protocol multiplexing at the AUAF server. The AAA servers work mostly with the Radius protocol, Identity providers usually work with HTTP and hotspot networks might use both depending on the needs. Thus, the AUAF server, being an intermediate protocol multiplexer makes this work easier by translating between the different protocols.

Specific examples of messages which can be multiplexed by the AUAF are application layer messages between UE and IdPs, used to obtain user identities and authentication tokens in the pre-authentication phase. One way to enable such messaging when a user does not yet have a secured connection to a hotspot is to tunnel HTTP inside EAP. This is not an uncommon practice, cf. [5].

*2) Dynamic Credential Provisioning using AUAF*

Figure 3 shows an example illustrating how an AUAF can dynamically provision certificates to a mobile device to enable secure access to a WLAN hotspot using EAP-TLS.

*3) WiFi Access using Federated Identity Protocol*

The AUAF approach addresses the problems of data offloading and mobility across heterogeneous networks, without compromising security and through minimal impact to existing deployments. This is done through a combination of a federated identity system and an efficient mobility management protocol such as Mobile IP.

Using a Federated Identity system facilitates optimized authentication and secure access in a new network with minimum added latency as illustrated in Figure 4. In this scenario, the AUAF function is absorbed by an OTT, which we refer to as OTT AUAF. The OTT AUAF behaves like a Proxy AAA Server, authenticating the UE/user at the application layer by interfacing with the MNO´s AAA Server, and is provisioned with the authentication credentials that are required for successive authentications of the user. The user gains secure access to the hotspot network by authenticating to the OTT AUAF server without interaction with the MNO AAA Server. The proposed approach assumes a federated identity protocol such as OpenID is used between the UE and the OTT AUAF server to establish a persistent security association. The UE and the OTT AUAF perform a full authentication run to dynamically generate session keys on both the UE and the OTT AUAF. Additionally, a temporary identity in the form a Network Access Identifier (NAI) is generated on both the UE and the OTT AUAF. These credentials are then used to facilitate an optimized EAP, which we refer to as EAP-ORTA (EAP-One Round Trip Authentication), to attach to the new network.

1. It is assumed in this step that the UE and OTT AUAF server have an already established security association and generated fresh master keys, MK (e.g. using EAP-AKA). In addition an ORTA identity is created on both the UE and the OTT AUAF server or it may be sent securely from the OTT AUAF server to the UE. The ORTA identity is generally a temporary identity that is used to trigger the EAP-ORTA authentication procedure.

2. Network discovery information may be obtained by the UE from the beacon information of a newly discovered network. Alternatively, in an L3 network discovery example, the UE may request WLAN network info from the Access Network Discovery and Selection Function ANDSF [6] (pull case) and/or the ANDSF may push WLAN network information to the UE over a secure 3GPP connection. The network information may include available APs, SSIDs, authentication methods supported (e.g. EAP-AKA, EAP-ORTA), and other access network parameters. As another variant, network discovery information may be obtained using 802.11u (e.g. using Generic Advertisement Service (GAS) and ANQP [6]).

3. The UE, having discovered that an AP of interest supports EAP-ORTA, sends an EAP-Start/Re-authenticate message {SEQ, ORTA ID-NAI, [IP-CFG-REQ], crypto suite, Auth-tag[1]} to that. The EAP-ORTA message includes the ORTA identity, SEQ for replay protection, and crypto suite used. To achieve further EAP optimization through concurrency, the UE may request IP address configuration by including an optional (IP_CFG_REQ) in the same EAP message. The EAP message is protected using an integrity key. As an alternative, the UE may request IP address configurations using a DHCP message carried in the same EAP message.
4. The AP forwards the EAP message {SEQ, ORTA ID-NAI, [IP-CFG-REQ], crypto suite, Auth-tag} using an Access Request to the WLAN AAA server.
5. The AF module on the WLAN AAA server uses the ORTA identity to discover and obtain the session key from the AUAF server. The WLAN AAA server generates and sends the session key (MSK) to the AP along with EAP-Success message {MSK, EAP-Success, Auth-tag}. If the UE sent [IP_CFG_REQ] in the EAP-Response message, the AAA server sends the required IP configurations to the UE in [IP_CFG_Reply] field of the EAP-Success message. If the UE sent DHCP message instead, the AAA server acts as DHCP relay and obtains the required IP configurations from a DHCP server. In addition, the AAA server may send channel binding information [CB-Info] in the EAP-Success message so that the UE can verify that the EAP message was received via the right AP and not a compromised one.
6. The AP forwards an EAP-Success message to the UE {SEQ, ORTA ID-NAI, [IP-CFG-Reply], crypto suite, [CB-Info], Auth-tag}.
7. A 4-Way Handshake, as per the 802.11i protocol, is performed, to finish the authentication of the UE by the AP and establish encryption keys on both ends.
8. The UE has secure Internet access over the new WLAN network and ongoing sessions from the previous network are switched over to the WLAN network without interruption.

## IV. EXAMPLE USE CASES

The suggested approach in this paper is aligned with standards-based activities that are addressing problems of offloading and mobility across heterogeneous networks, without compromising security and through minimal impact to existing deployments. The standards activities include the WFA HS2.0 Passpoint program [1] and IEEE 802.11ai [4].

### *A. Hotspot 2.0 Seamless Data Offloading*

Wireless network operators seek an interworking solution that allows Public Hotspot access as part of their 3GPP services offering, with minimum impact on their existing infrastructure and operations. There are two main types of Public Hotspots, depending on the access methods used, namely: Browser based and 802.1x/EAP Hotspots.

The Wi-Fi Alliance Hotspot 2.0 program [1] tries to remove problems associated with 802.1x/EAP based access by defining a more mature network access capability for WiFi, creating a good user experience and supporting operator goals of leveraging WiFi technology to securely offload data from their cellular networks. The main Hotspot 2.0 requirements are support for:

- WPA2 (EAP-SIM, EAP-AKA, EAP-TLS, EAP-TTLS)
- 802.11u/v

However, there are still some challenges with the WFA HS2.0 access procedures including:

- Legacy hotspot APs are not supported and have to be replaced with HS2.0 compliant APs
- The hotspot AAA server is required to support EAP-SIM/AKA. This requires an IP based AAA server to support and implement a complex SS7/Diameter interface towards the MNO's HLR/HSS. Typical hotspot AAA servers do not support such a complex interface.
- Additional network elements are required such as HS2.0 compliant Online Signup and Registration servers.
- The hotspot operator is required to establish, possibly multiple, SLAs with MNOs to enable use of MNO credentials for authentication etc.
- Performance issues are anticipated as a result of HS2.0 procedures for network discovery, registration, association, and authentication.
- In addition, mobility between WiFi and 3GPP might break and become non-seamless to the end user.

Therefore, hotspot operators are likely to incur high deployment and operational expenses and user experience is likely to be poor, especially for real time applications (such as VoIP). By introducing a federated identity protocol using the AUAF server in the network, a number of benefits can be achieved in seamless offloading scenarios, both from the user's and the network operator's perspectives.

#### *1) Simplified User Experience*

[1] Note that the computation of Auth-tag is performed over the entire EAP message.

In an online sign up process to a hotspot, the user is required to register and provide details of login when he needs to establish a connection with that hotspot. This process becomes tedious when the user has to perform these tasks on the mobile phone's browser, significantly impeding usage of hotspot networks. The AUAF server as proposed in this document (in Phase 1 and 2) can play a beneficial role in improving user experience, by securely storing the information that the hotspot may need when the user wants to be connected to the hotspot and provide the information directly without user involvement. Providing a solution to this problem using this approach can result in higher usage and thus higher revenue for the hotspot operator.

*2) Reduction of MNO AAA Network Traffic*

For the user to gain secure and automated access to hotspot networks, authentication by the MNOs AAA Server is required. The user is then provisioned with the credentials for secure access to the hotspot network. This is not scalable because for every user, the MNO AAA Server has to perform first user authentication and then provisioning of the secure access credentials. If the number of users becomes high and the scale of hotspots grows, then there will be a significant increase in the authentication traffic to the MNO's core network and AAA server.

As proposed for phase 3, the AUAF securely stores the user authentication related credentials (generated during the Pre-authentication phase between the User and the MNO AAA Server) locally and then can authenticate the user on behalf of the MNOs AAA Server. The credentials may be refreshed based on operator policies thus significantly reducing traffic to the MNO network.

*3) Business Opportunity for OTT IdP*

Through the methods described here, OTT IdPs may be enabled to provide secure access to hotspot networks for their subscribers and at the same time also offer their user base to hotspot network service providers as an asset. The construction maintains an appropriate level of security as per the requirements of the hotspot network, since it allows for integration of strong, e.g., MNO-based authentication.

*4) Easier Adoption for Hotspot Operators*

Since the federated approach can be facilitated through a software upgrade of existing hotspot networks or though installation of a low cost consumer grade WiFi AP, there is a reduced cost of installation. Authentication of WiFi users is facilitated through a lightweight protocol between the AP and AUAF server. Additionally, the burden of establishing SLAs with Operators and the infra-structure required to interface to the Operator network's AAA servers is delegated to the AUAF, resulting in a reduced cost of operation for hotspot operators.

## *B. Fast Initial Link Setup*

This use case extends the data offloading work to support mobility. A secure link setup process of no more than 100ms is specified by the work currently being carried out by IEEE 802.11ai. In order to support such a stringent requirement and provide session continuity, a combination of a federated identity management system as has been described here combined with an efficient mobility management protocol such Mobile IP is required. The work presented in [2,7] describes how the advantage of obtaining dynamic session keys through federated identity systems along with an efficient authentication protocol and concurrent authentication of UE and IP address assignment, can be used to address seamless authentication and mobility across heterogeneous networks.

## *C. Secure Access to Home WiFi Networks*

As a final, practical example we propose to use the AUAF architecture to enable secure (WFA grade) WiFi access to home APs. In a concrete use case, a Home AP Owner wants to invite some of his friends on a social networking site to use his AP.

The social network service provider may be a typical 'Over-The-Top' (OTT) service and identity provider in our scenario. We use the abbreviation Hid and WFid for the OTT identifier of the Home AP Owner and a friend whom he wants to share his AP with (a 'WiFi Friend'), respectively. Hid and WFid are sometimes used interchangeably with those players. The following call flows illustrate how OpenID 2.0 [8] may be

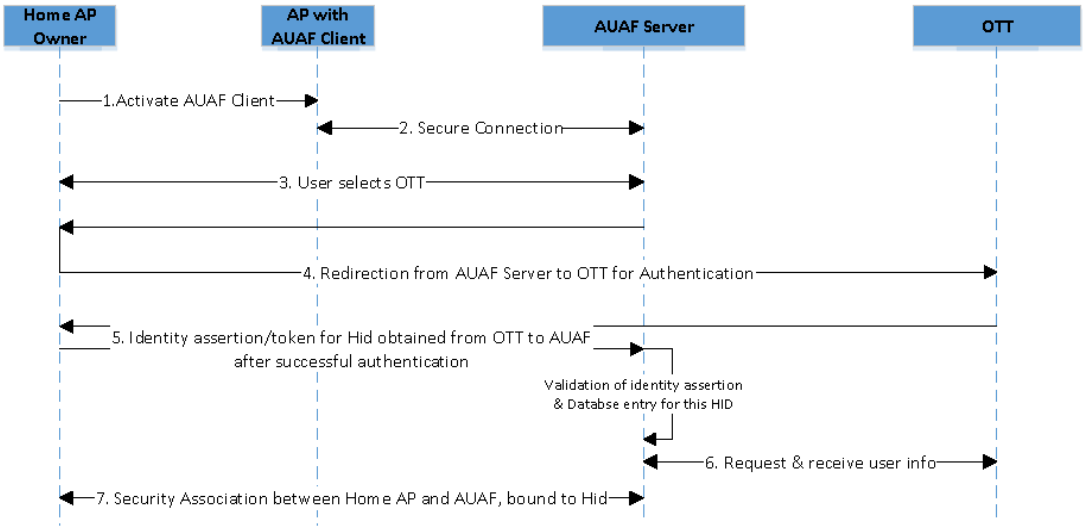


Fig. 5. Home AP Owner Registration of AP with the AUAF system via Social Network Identity Provider, OTT.

used for application layer user authentication and identity management. As an alternative, the call flows could be implemented using OpenID Connect and OAuth tokens as information bearers. The use case scenario proceeds in three phases.

*1) Registration of Home AP by Owner*

As a general precondition it is assumed that the Home AP Owner has installed the AP at his home and Internet access is provided (most commonly, the AP includes a cable modem and router). The home AP contains a piece of firmware, the AUAF client, which facilitates an application layer connection to the AUAF server. The wireless connectivity of the home AP owner to the home AP is initially secured by a basic, i.e., identity-less, method such as WPA-PSK. Alternatively, all messages on the application layer which are prior to a link layer authentication and security context set up, may be established through a HTTPS session between the Home AP Owner and the AUAF server. The goal after completion of phase 1 is that the AUAF server and the Home AP Owner establish a security association (SA), which is bound to the identity of the home owner, Hid with a selected OTT provider.

Referring to Figure 5, at step 1, the home AP owner activates the AUAF client, which for instance may come with a Web interface for that purpose. The AUAF client initiates connection to the AUAF server, selected by the Home Owner.

At step 2, the AUAF client and server establish a secure connection through which all further messages in the registration process are tunneled. This may be carried out using various methods offering different security properties:

- The TLS server certificate of the AUAF server is used to establish a TLS tunnel over which an HTTPS connection runs.
- TLS client and server certificates are used. The AUAF server will need to check the client certificate with some CA, e.g., the home AP vendor.
- TLS-PSK with a group key, valid for all AUAF clients is used to set up a TLS tunnel.
- TLS-PSK with individual keys is used to set up a TLS tunnel. The AUAF server needs to look up the key in a database for this approach, e.g., the home AP vendor.

At step 3, the owner selects from which OTT (from a list of OTT providers with a trust agreement with the AUAF server) he would like to obtain authentication for the registration with the AUAF server. If there is only one OTT then this selection step can be automated. The AUAF server requests authentication with the OTT provider, by an indirect request, usually initiated using an HTTP REDIRECT message.

At step 4, the owner authenticates with the OTT provider, which results in the derivation of session credentials both at the owner UE and at the OTT.

At step 5, the successful result of the authentication is returned, by way of an authentication assertion, or token, to the AUAF server. That is, the assertion goes from the OTT over the Home AP Owner's device and Browser Agent to the AUAF server. The AUAF server validates the authentication assertion and then creates a record in his database in which the home owner OTT identifier, Hid, is associated with unique credentials for the registered AP.

Similarly to the previously described scenario for seamless authentication (cf. Fig. 4) these credentials, e.g., a symmetric key, may be obtained from the OTT, along with other user information, at step 6.

Note that the registration is not complete at this stage, since the home AP owner's identity needs to be bound to the individual AP (in the possession of the home owner) and a persistent SA to that AP needs to be established, i.e., binding credentials need to be created. If such a binding is not achieved early in the AP's lifecycle, the home AP owner incurs a generic risk that someone else may register his AP with the AUAF system and enable network access for an uncontrolled group of potentially malicious users. This risk is mitigated by the following steps.

At step 7, the SA between the AP (which may be maintained in the AP by the AUAF client) and the AUAF server is established. There are many ways to do this, for instance keying material may be extracted from the TLS channel between the AP and AUAF server using methods of

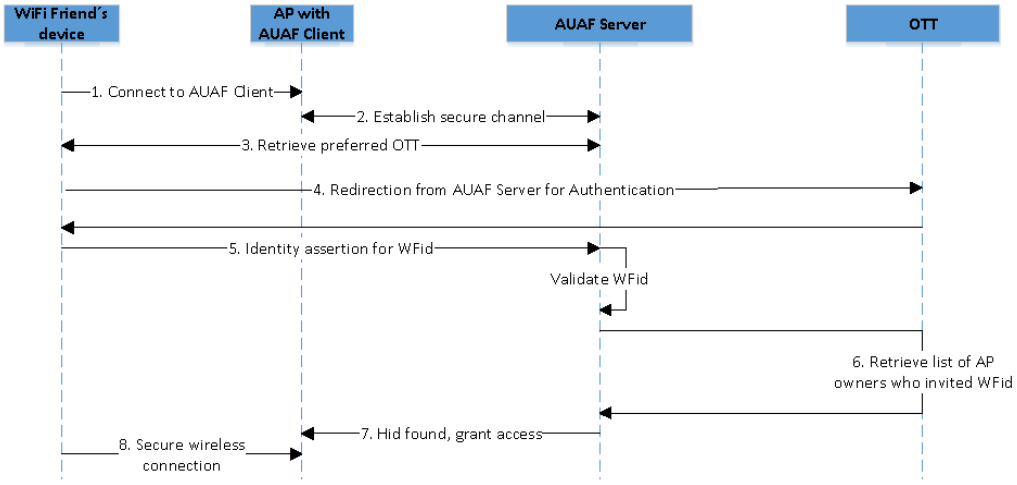


Fig. 6. WiFi Friend Access Authorization to Home Owner's WiFi AP

RFC5246, and combined in a key derivation algorithm with the previously obtained AP credentials, a random number, and Hid, to make it unique to the home owner and AP, and private to the AP and AUAF server. The SA is securely stored in the AUAF server's database record for Hid.

To prevent any other user who may gain access to the AP by accident (e.g., wireless access security is disabled), some proof of possession of the AP may be required to be yielded to the AUAF server. This might have been established already at step 1, if the activation of the AUAF client requires a credential from the user, and the AUAF server is aware of this security property of the client. Another method is to insert a step 7a in which the home AP owner is asked to enter credentials directly at the AUAF server's Web interface. The credentials may be a code printed on the AP casing, or have come with the AP documentation.

*2) Inviting WiFi Friends*

In the second phase, the Home AP Owner invites some of his friends, temporarily or permanently, to join his WiFi Friends group using the web interface provided by the OTT. As a result of the addition of friends to the network, appropriate profile information for each of his friends is added to a list (maintained by the OTT) of allowed users that can connect to his home AP. It is important to note that this property is maintained in the profiles of Hid's WiFi Friends, but controlled via Hid's OTT profile. Differently from normal friend relationships via an OTT, the WiFi Friend relation is unidirectional.

*3) Authenticating a WiFi Friend*

The process of a WiFi Friend authenticating and gaining access to Hid's AP is, at the application layer, rather similar to phase 1, which has the distinct advantage, that many existing server-side components may be re-used.

Referring to Figure 6, at step 1, an initial connection from the WiFi Friend's device (again, the OTT identifier WFid is used as an abbreviation for Hid's WiFi Friend) to the AP and the AUAF client interface to the AUAF server is established. The same security considerations are valid for this initial connection as mentioned in the preconditions of phase 1. At step 2, the AUAF client and server establish a secure connection, using the SA from phase 1, through which all further messages are tunneled.

At step 3, the AUAF server retrieves the WiFi Friend's preferred OTT. The AUAF server requests user authentication with the selected OTT provider, by an indirect request, using an HTTP REDIRECT message. As an alternative approach, when more than one OTT has been provisioned, the WiFi Friend may initiate a "get friend access" through selecting a preferred OTT, from a list of the OTT providers he would like to obtain authentication for access to the friend AP. The OTT list is registered with the AUAF server by Hid and is restricted to the OTTs who have a trust agreement with the AUAF server.

The design of phase 3 so far has the advantage of providing a seamless and automated experience to the WiFi Friend and not requiring any modifications to the WiFi Friend's device. However, it should be noted that the above variant of step 3 requires a minimal user interaction. A practical solution for this would involve an 'AUAF App' on the WiFi Friend's device, which interacts with the AUAF.

At step 4, the WiFi Friend authenticates with the OTT, which then, at step 5, issues an authentication assertion. The AUAF server validates the assertion and then at step 6, makes a request to the OTT to seek if the WiFi Friend may be granted access. The OTT inspects the list of home AP owners associated with the WiFi Friend, WFid and their corresponding authorizations for access to their respective APs, Hids. If the Hid is found in that list, then at step 7, the AUAF server signals back to the AUAF client that access to WFid is granted. If the Hid is not found in the list of authorizations then the home AP owner may be asked for explicit authorization for access by the WiFi Friend, by way of an application layer communication between the OTT and the Owner.

The subsequent setup of a secure wireless link between the WiFi Friend, WFid and the AP, at step 8, may be performed using various methods. The credentials used for securing this link may be valid for a certain period of time, as configured by the AP owner at the OTT, allowing access for a single session which expires when the WiFi Friend detaches, from the home AP of the friend, through to continued access authorization without performing another application layer re-authentication.

## V. CONCLUSION

With the growth in the use of federated identity systems for application layer authentication and access to connected services, the notion of a persistent security association between a User/User Device and OTT players such as Facebook or Google is common. We have shown how such services, using Open Web standards (such as OpenID), may be leveraged to address seamless connectivity to heterogeneously connected networks. In particular we have shown how such an approach may be used to simplify and ease secure User access to WiFi networks regardless of whether the network is a WiFi Hotspot or home AP. We also satisfy all of the WFA HS2.0 and 802.11ai requirements as well as providing WFA grade security for access to home WiFi APs, addressing many of the shortfalls of using WPA-PSK based security in home networks.

## REFERENCES


[1] HS2.0, "Marketing Requirements Document for Hotspot 2.0", Version 1.0 . s.l. : WFA, March, 2011.

[2] Targali Y. M., Choyi V., Shah Y., "Seamless Authentication Across Heterogeneous Networks using Generic Bootstrapping Architecture Systems" published in the International Wireless Communications and Mobile Computing Conference in Cagliari, Italy, July 2013.

[3] Extensible Authentication Protocol (EAP), B. Aboba, L. Blunk, J. Vollbrecht, J. Carson, H. Levkowetz, RFC 3748, June 2004.

[4] 802.11ai, IEEE 802.11-11/0238r18, "Use Case Reference List for TGai," April,2011.

[5] N. Cam-Winget, P. Sangster, PT-EAP: Posture Transport (PT) Protocol For EAP Tunnel Methods". Internet Draft. IETF https://datatracker.ietf.org/doc/draft-ietf-nea-pt-eap/

[6] 3GPP TS 23.402 Architecture enhancements for non-3GPP accesses.

[7] Targali Y. M., Choyi V., Shah Y., "Seamless Authentication and Mobility Across Heterogeneous Networks using Federated Identity Systems," published in the Second IEEE ICC Workshop on Telecommunication Standards: From Research to Standards, June 2013.

[8] OpenID Foundation. http://openid.net