WIRELESS WORLD
RESEARCH FORUM®

Network based Aggregation Server for Federated WiFi Access

Yogendra Shah, Yousif Targali
InterDigital Communications, Inc.

Andreas U. Schmidt,
Lakshmi Subramanian, Aamer Chaudry
Novalyst IT AG

Modern WiFi Hotspot Networks‘ Requirements

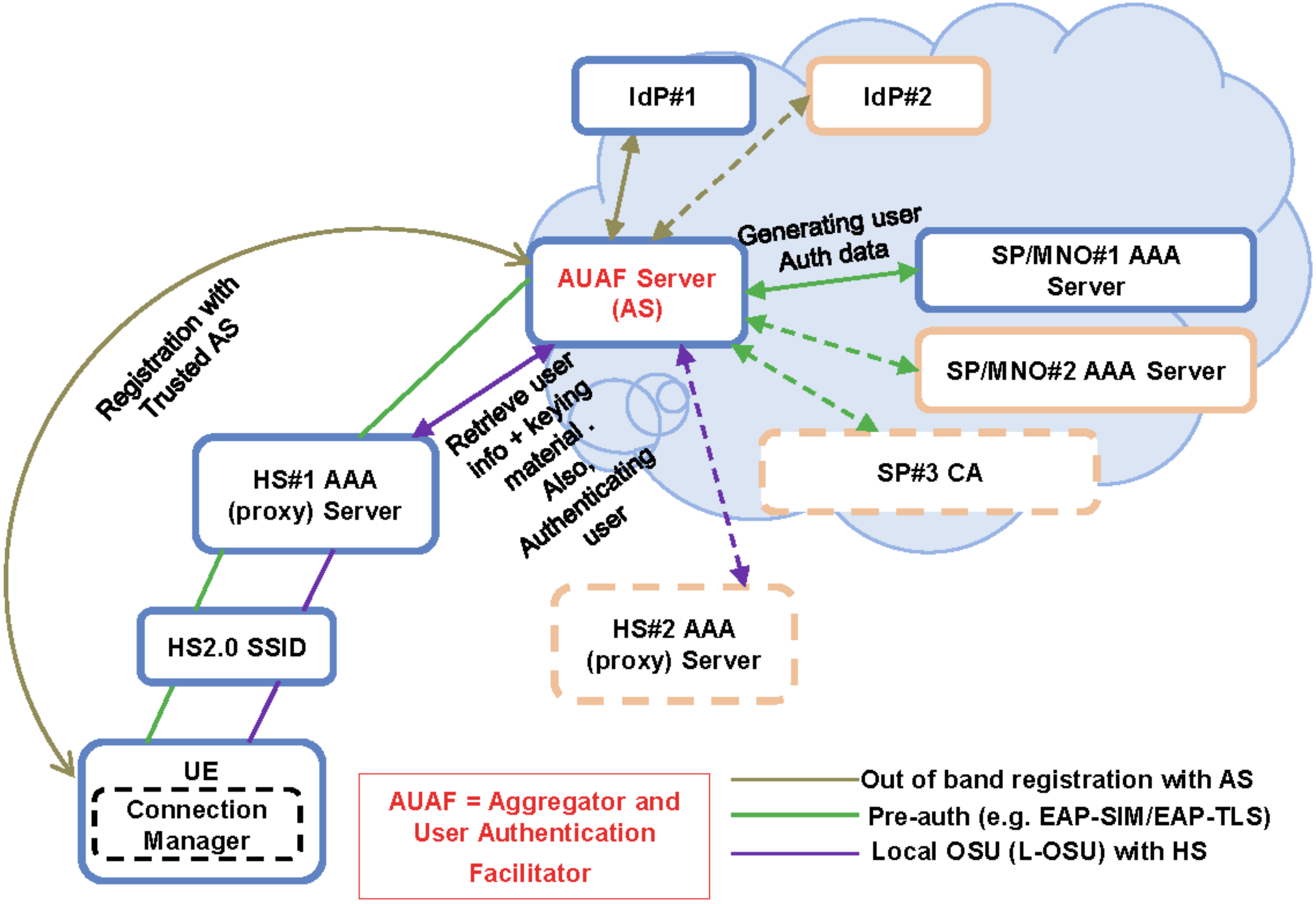
- Attract Users by simplified access
- Simplify and accelerate transition between access networks
- Robust Security – device independent and scalable
- Connect to Over-The-Top (OTT) IdPs

- Technology Framework:
  - WiFi Alliance (WFA) Hotspot 2.0 Requirements
  - WFA On-Line Sign-Up (OSU), dynamic credential provisioning
  - 802.11ai Fast Initial Link setup (FILS)
  - Dynamically support required authentication methods EAP-SIM, -AKA, -TLS, -TTLS

Proposed Aggregator Entity Framework

- Introduce Aggregator and User Authentication Facilitator (AUAF)
- Connects and aggregates across
  - Hotspot Networks
  - Authenticators, e.g., MNOs
  - OTTs
  - User Devices

- Goals:
  - Enable hotspot providers to extend user base without incurring high costs in terms of equipment (e.g. legacy equipment) and establishing multiple service level agreements (SLA) with operators.
  - Providing users without a relationship to an operator to access hotspots sthrough a simplified and transparent OSU authorization and agreement to terms and conditions.

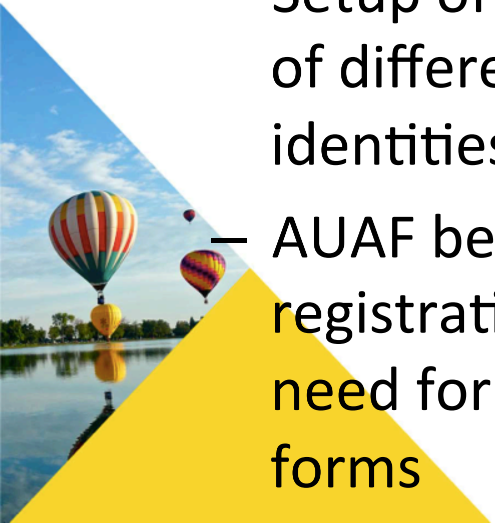

IdP#1
IdP#2
AUAF Server (AS)
Generating user Auth data
SP/MNO#1 AAA Server
SP/MNO#2 AAA Server
SP#3 CA
Registration with Trusted AS
Retrieve user info + keying material . Also, Authenticating user
HS#1 AAA (proxy) Server
HS2.0 SSID
HS#2 AAA (proxy) Server
UE
Connection Manager
AUAF = Aggregator and User Authentication Facilitator
Out of band registration with AS
Pre-auth (e.g. EAP-SIM/EAP-TLS)
Local OSU (L-OSU) with HS

Network Architecture using an AUAF Server.

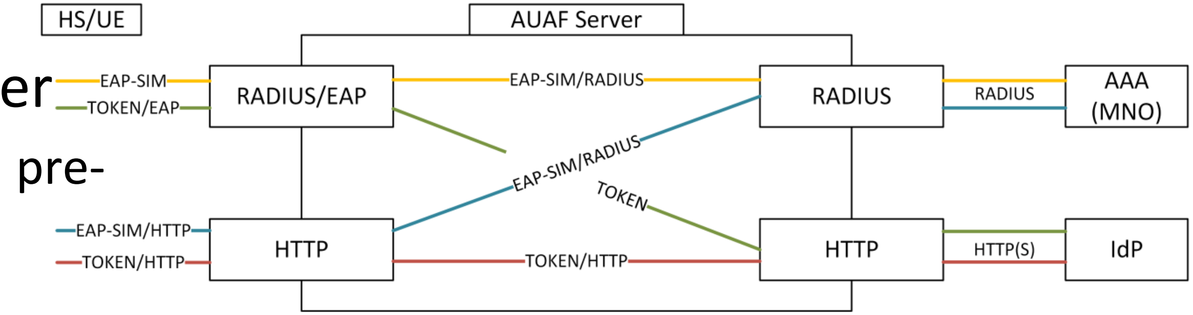
Aggregator and User Authentication Facilitator (AUAF) connects Identity Providers, Hotspot Networks and Authentication Providers such as MNOs.

AUAF-Based Three-Phase Network Attachment

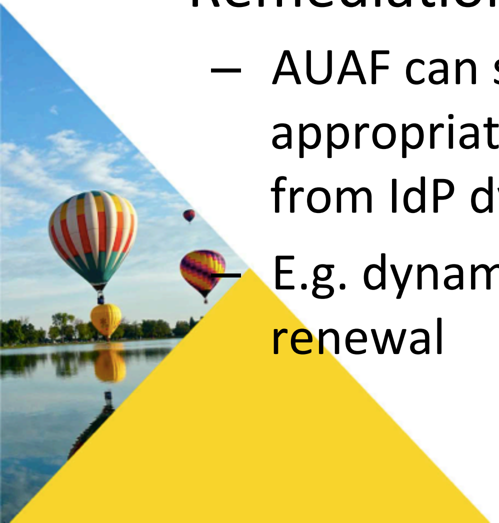
- 1: User Registration
  - User profile and subscription info stored at AUAF
  - Provided by OTT and/or MNO
  - Setup of logical binding of different provider identities
  - AUAF becomes registration cache (no need for registration forms
- 2: Pre-Authentication
  - Authenticate UE once
  - Derive Access credentials for selected hotspot network by AUAF and selected IdP (OTT and/or MNO)
- 3: Setup secure link
  - Using previously derived credentials, pushed down by AUAF



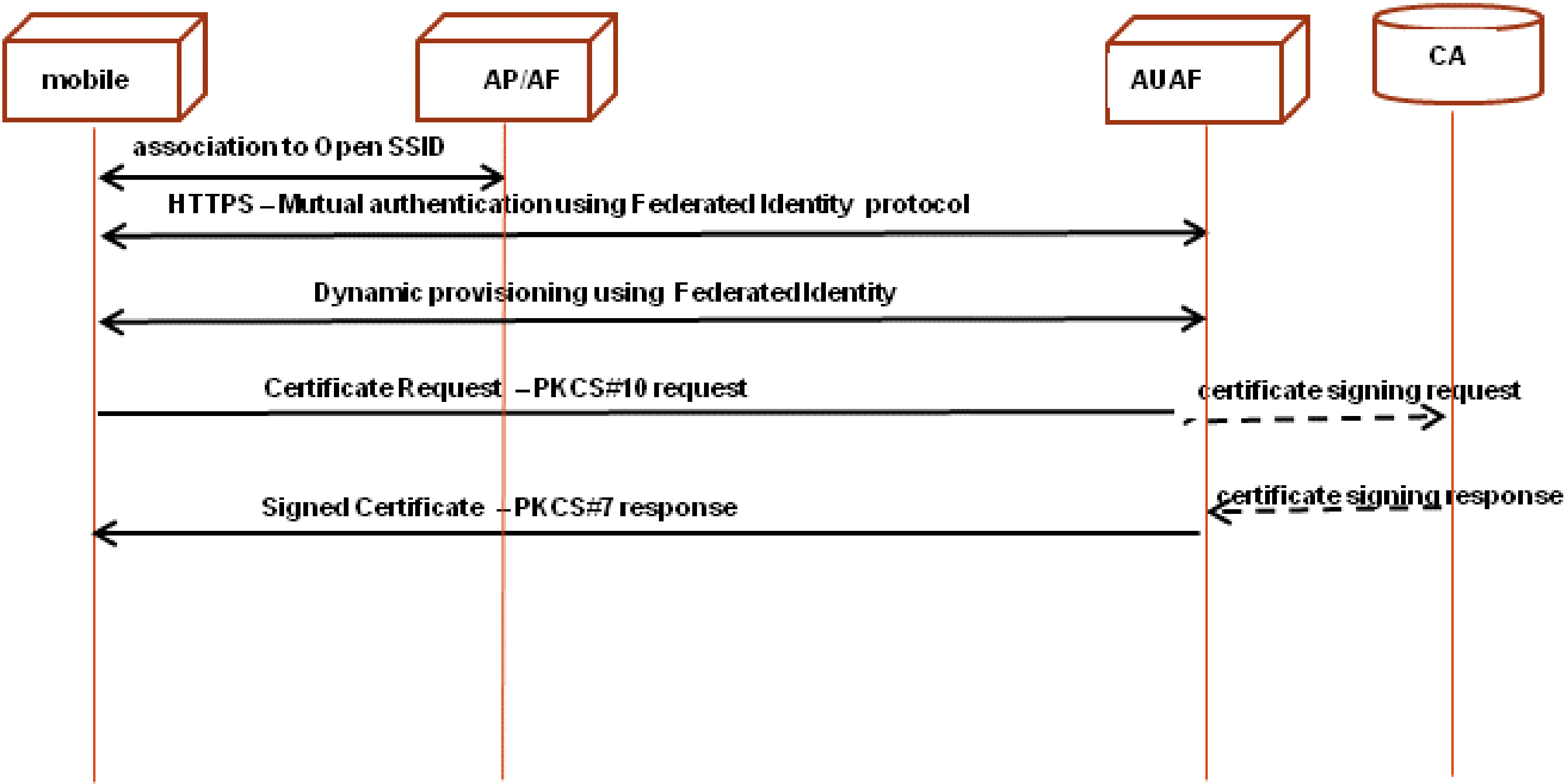
AUAF Core Functionality



- Proxy OSU/AAA Server
  - User registration and pre-authentication
  - Federate across authentication provider
  - Provides proxy AAA for HS network in phase 2
- Remediation Server
  - AUAF can select appropriate credential from IdP dynamically
  - E.g. dynamic credential renewal

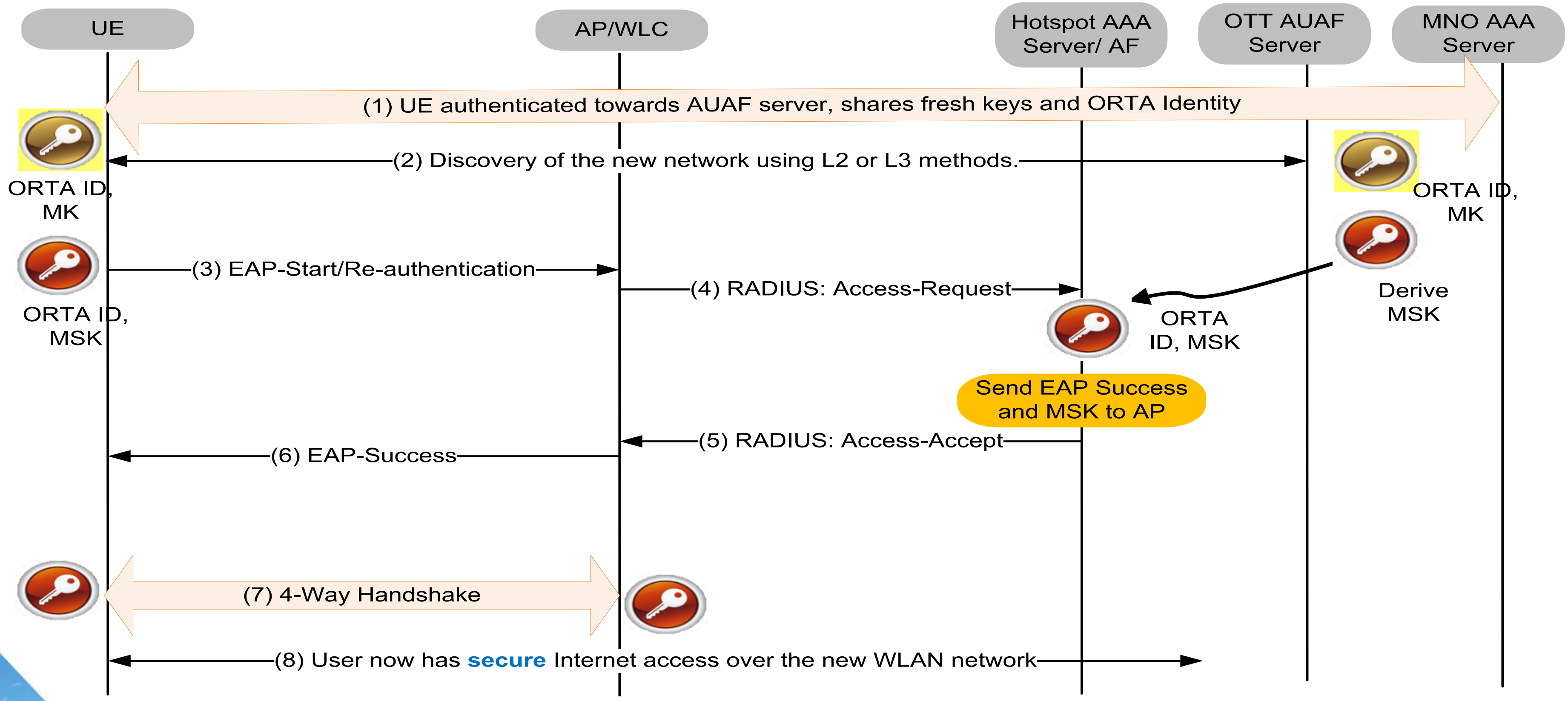


- Network Hiding Gateway
  - MNO AAA is not exposed to HS network
- Protocol Multiplexing (above)
  - Mediates between application-layer authentication protocols (e.g. HTTP carrying Oauth token), and access layer authentication front (e.g. EAP-SIM -and backend, e.g. RADIUS)


mobile
AP/AF
AUAF
CA
association to Open SSID
HTTPS – Mutual authentication using Federated Identity protocol
Dynamic provisioning using Federated Identity
Certificate Request – PKCS#10 request
certificate signing request
Signed Certificate – PKCS#7 response
certificate signing response

Use Case Dynamic Certificate Provisioning

This example illustrates how an AUAF can dynamically provision certificates to a mobile device to enable secure access to a WLAN hotspot using EAP-TLS, in accordance with Hotspot 2.0 On-Line Sign-Up



UE

AP/WLC

Hotspot AAA Server/ AF

OTT AUAF Server

MNO AAA Server

(1) UE authenticated towards AUAF server, shares fresh keys and ORTA Identity

ORTA ID, MK

(2) Discovery of the new network using L2 or L3 methods.

ORTA ID, MK

(3) EAP-Start/Re-authentication

ORTA ID, MSK

(4) RADIUS: Access-Request

Derive MSK

ORTA ID, MSK

Send EAP Success and MSK to AP

(5) RADIUS: Access-Accept

(6) EAP-Success

(7) 4-Way Handshake

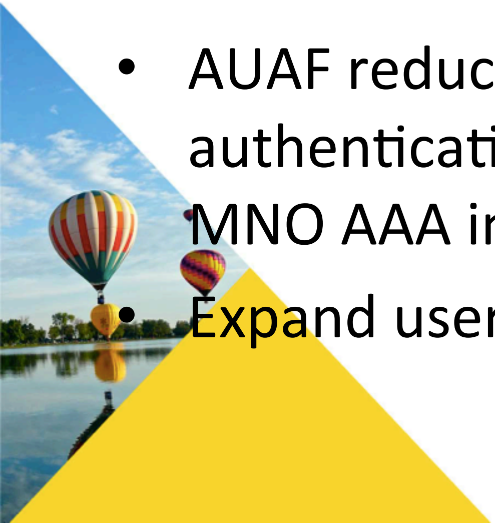
(8) User now has **secure** Internet access over the new WLAN network

Call Flow for Seamless Authentication and Mobility using AUAF

Using a Federated Identity system facilitates optimized authentication and secure access in a new network with minimum added latency

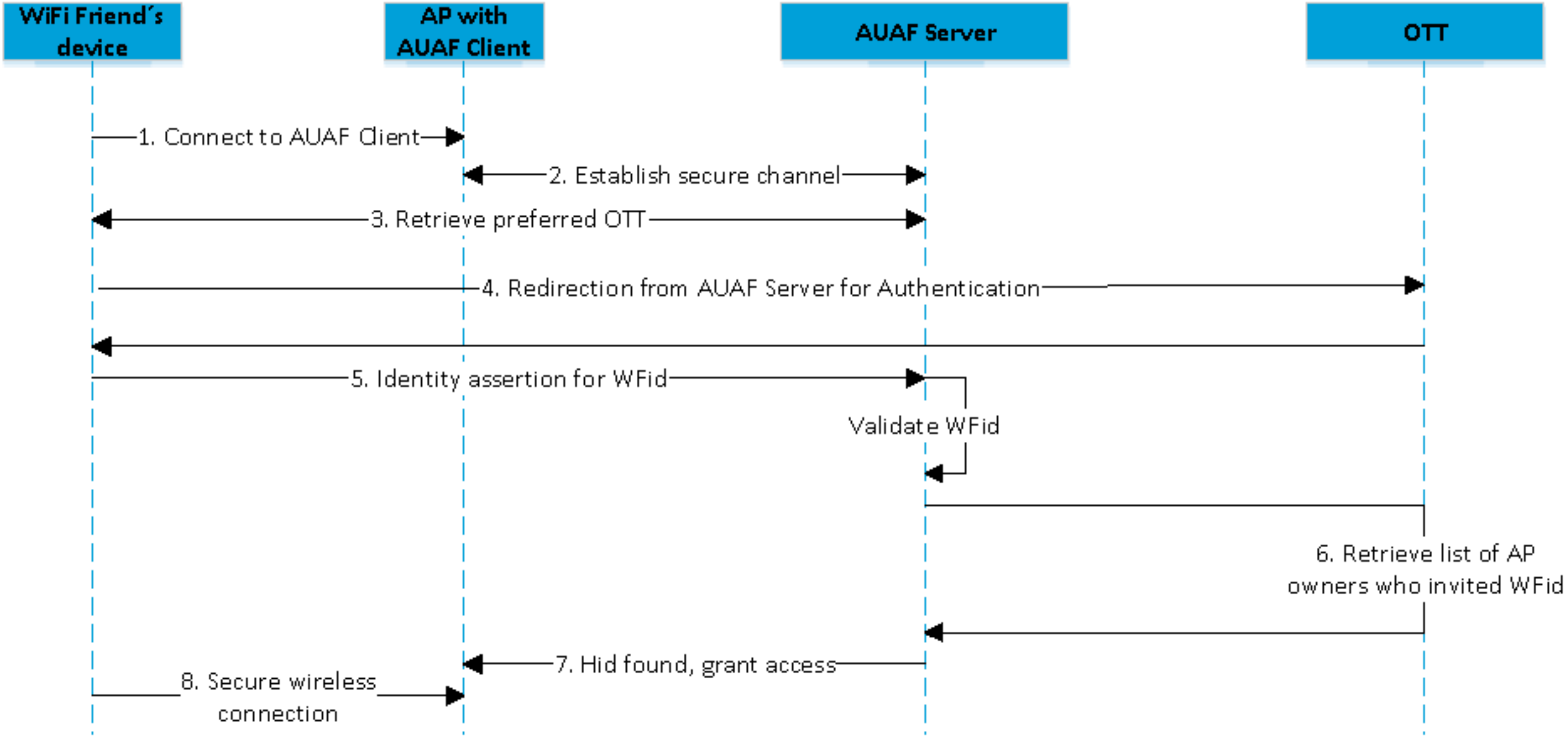
Use Case: Data Offloading

- Public Hotspot access as part of MNOs' 3GPP services offering, as means to offload data
- WFA HS 2.0 is one solution, but challenging for both operators and HS networks
- AUAF may serve as HTTP-based proxy to legacy HS networks (captive portals), auto-filling user info
- More seamless process with less user involvement
- AUAF reduces load on MNO by caching authentication in pre-authentication and providing credentials in phase 3 without MNO AAA involvement – provides for scalability
- Expand user base for data offloading by involving OTT



Use Case Secure Access to home WiFi Networks

- WFA grade security to ‚invite my buddy to my WiFi access point‘ scenario
- Significant legal risks and liabilities in many jurisdictions – need to be reduced by robust security, in particular authentication
- Idea:
  - Exploit OTT user connections for authorization (like FB WiFi)
  - Use AUAF-enabled APs to provide for seamless procedure
  - Follow AUAF three-phase procedure, enhanced by access authorization decision at AUAF server

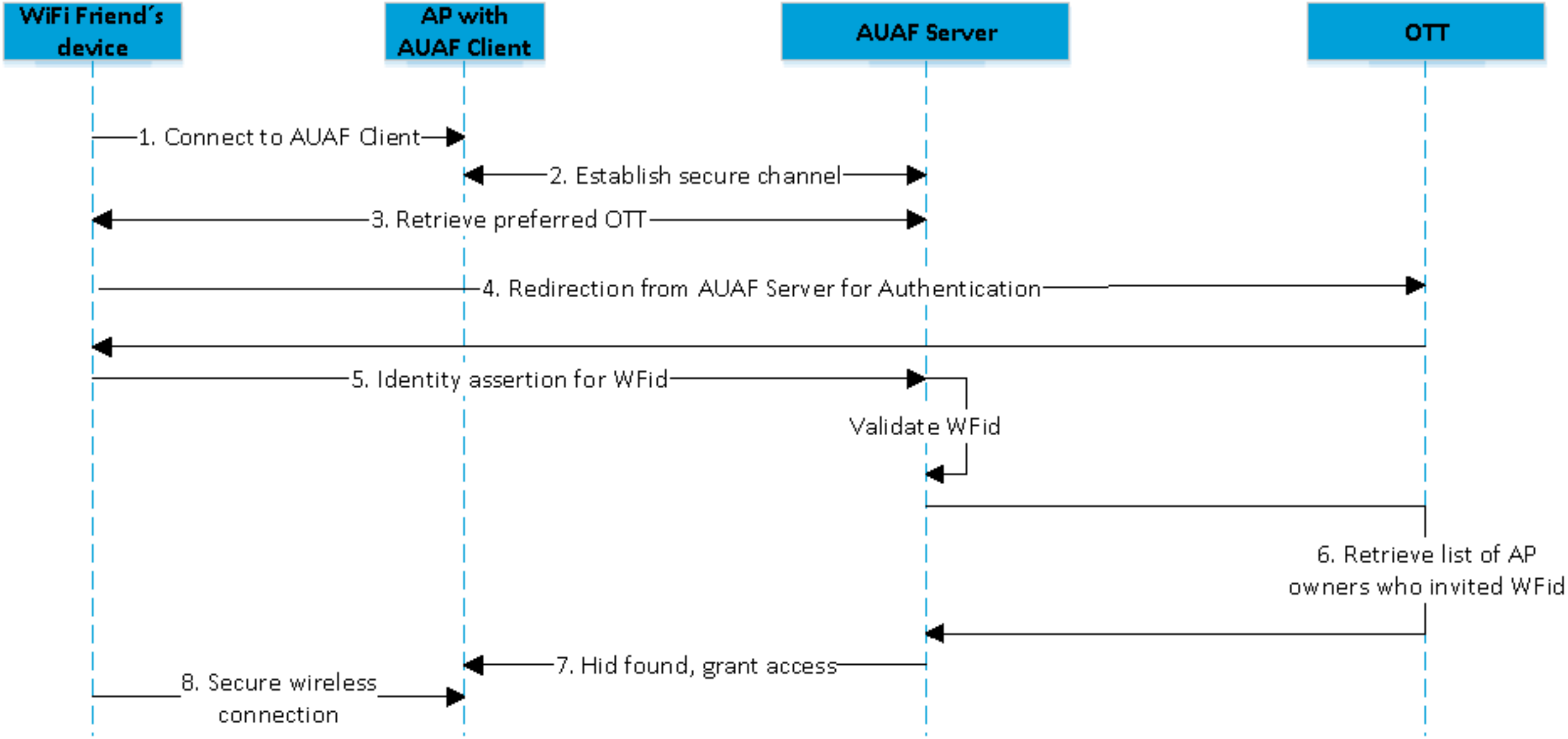

WiFi Friend's device
AP with AUAF Client
AUAF Server
OTT
1. Connect to AUAF Client
2. Establish secure channel
3. Retrieve preferred OTT
4. Redirection from AUAF Server for Authentication
5. Identity assertion for WFid
Validate WFid
6. Retrieve list of AP owners who invited WFid
7. Hid found, grant access
8. Secure wireless connection

Phase 1: Home AP Registration

AUAF server and Home AP (with AUAF client) and AP Owner establish a security association (SA), which is bound to the identity (WFId) of the home owner at a selected OTT provider

Phase 2: Invite WiFi Friends

- Home AP Owner defines ‚WiFi Friends‘ selected from his contacts list at OTT
- OTT propagates the property ‚being a WiFi Friend of Home AP Owner XYZ‘ to profile of respective WiFi Friend
- There it can be accessed when a user wants to connect to a private AP


WiFi Friend's device
AP with AUAF Client
AUAF Server
OTT
1. Connect to AUAF Client
2. Establish secure channel
3. Retrieve preferred OTT
4. Redirection from AUAF Server for Authentication
5. Identity assertion for WFid
Validate WFid
6. Retrieve list of AP owners who invited WFid
7. Hid found, grant access
8. Secure wireless connection

WiFi Friend Access Authorization to Home Owner's WiFi AP

WiFi friend gains access by authorization through the OTT IdP, and secure link setup facilitated by AUAF and AP.

Conclusions

- AUAF architecture enables WiFi access by the Cloud
- Satisfies/enables satisfying HS 2.0 OSU and 802.11ai requirements
- Scalable, centralises only essential aggregation functions, without overhead
- Enhanced user base for HS providers
- Traffic offload for mobile operators
- Business opportunity for OTT provider
- Last not least: convenience and added value for users without compromising security and privacy