WBA OpenRoaming Wireless Federation

DRAFT-TOMAS-OPENROAMING-00
B. TOMAS, B. A. COCKRELL, N. CANPOLAT, M. GRAYSON, S. GUNDAVELLI
MADINAS @ IETF 117
Objectives – Enable ubiquitous Wi-Fi connectivity by private networks using identity provider credentials

OpenRoaming mission statement is to create an open framework for all types of players to develop their Wi-Fi services & business.
A Federation built on IETF Protocols

- 802.1X/EAP based authentication: RFC 3579/RFC 3580
- End user identifier based on chargeable user ID: RFC 4372
- ANP Civic Address (country): RFC 5580
- Dynamic IDP discovery: RFC 7585
- Recommended DNSSec for IDP discovery: RFC 4035
- RadSec secured signaling: RFC 6614/6613
- as well as
  - IEEE 802.11 ANQP
  - WFA Passpoint

WBA & IETF exchange liaison statements on a continuous basis. Helping driving alignment and collaboration; examples are MADINAS, CAPPORT, RADEXT, DISPATCH
Embedded Unique Identifiers

1. “WBAID” for Roaming, Data & Financial Clearing & PKI “UID”

2. Certificate Based Roaming (PKI .cfg “policyIdentifier”)

3. WBA Roaming Consortium Federation (RCOI)

Common identifiers are industry standard, have been registered, and are available to all stakeholders.
CyberSecurity Service

Underpinned by a PKI enabling flexibility for all stakeholders to join the federation

RadSec Technology (IETF RFC 6614) and Certificate Policy governing the ecosystem

All signaling between ANP and IDP as well as federation APIs secured with mutual TLS

Issued an ANP test certificate to IETF-NOC to enable MADINAS experiments
Standard Closed Access Groups: Enable Enhanced Policy Enforcement

* OpenRoaming-Settled: BA-A2-D0-xx-x

* OpenRoaming-Settlement-Free: 5A-03-BA-xx-x
Merging Islands of Connectivity into a Common Federation

Provisioning of individual realms/IDs have been a challenge since 2003 to scale roaming and offload ...

... the introduction of RCOI allows all the defined clusters to coexist to apply policy autonomously.
Replacing “click to accepts Ts and Cs” requires a legal framework.

Access and Identity providers agree terms with brokers – not WBA. **WBA Membership is not required!**

Framework ensures ANP agrees immutable terms related to service availability, quality of experience and handling of personally identifiable information.

IDP agrees to present terms to end-users defining prohibited content.
Status of OpenRoaming

Infrastructure vendor status:
• 6 vendors passed plugfest compliance (June 2023)
• 7 additional vendors implementing and doing customer PoC’s
• 15+ Integrators/hubs deploying OTT solutions

Device vendor status:
• All devices that support Hotspot 2.0 (R1)/ Passpoint are compatible
• Passpoint certification account for 7.000+ devices

Adoption:
• 3 Million hotspots support OpenRoaming globally (enablement vary from couple hours to couple days)
• Growing large scale deployments: Tokyo City, Dublin City, London Stadium, Delhaize Retail, …
Next Steps

- Work with IETF on their results of OpenRoaming experimental system and any consequential I-D improvements
- Update OpenRoaming with MADINAS recommendations, e.g., privacy preservation
- WBA Technical Standards WG is evolving the Federation...
  - Private 5G Cellular (3GPP Release 19 Study Item)
  - Headless IoT Device Onboarding
  Updates and liaison statement will be sent as progress is made with PoCs
Thank you
Bruno Tomas – bruno@wballiance.com
DNS process of resolving OpenRoaming realm authentication

Auth request
user1@openroamingidp.com

First DNS Lookup for NAPTR record "openroamingidp.com"

NAPTR Record(s)

Second DNS lookup for SRV record "_radius tls._tcp.<service-uri>"

SRV Record(s)

Third DNS lookup for A or AAAA record "<radsec-uri>"

A or AAAA Record(s)

Output: Service’s FQDN=
<realm> NAPTR = 50 50 "s" "aaa+auth:radius.tls.tcp" "<service>
RadSec Service, where <service>="_radius tls._tcp.<service-uri>"

Output: Server’s IP Address
<fqdn> A = <ipv4-address>
<fqdn> AAAA = <ipv6-address>