

WBA OpenRoaming Wireless Federation

DRAFT-TOMAS-OPENROAMING-00

B. TOMAS, B. A. COCKRELL, N. CANPOLAT, M. GRAYSON, S. GUNDAVELLI

MADINAS @ IETF 117

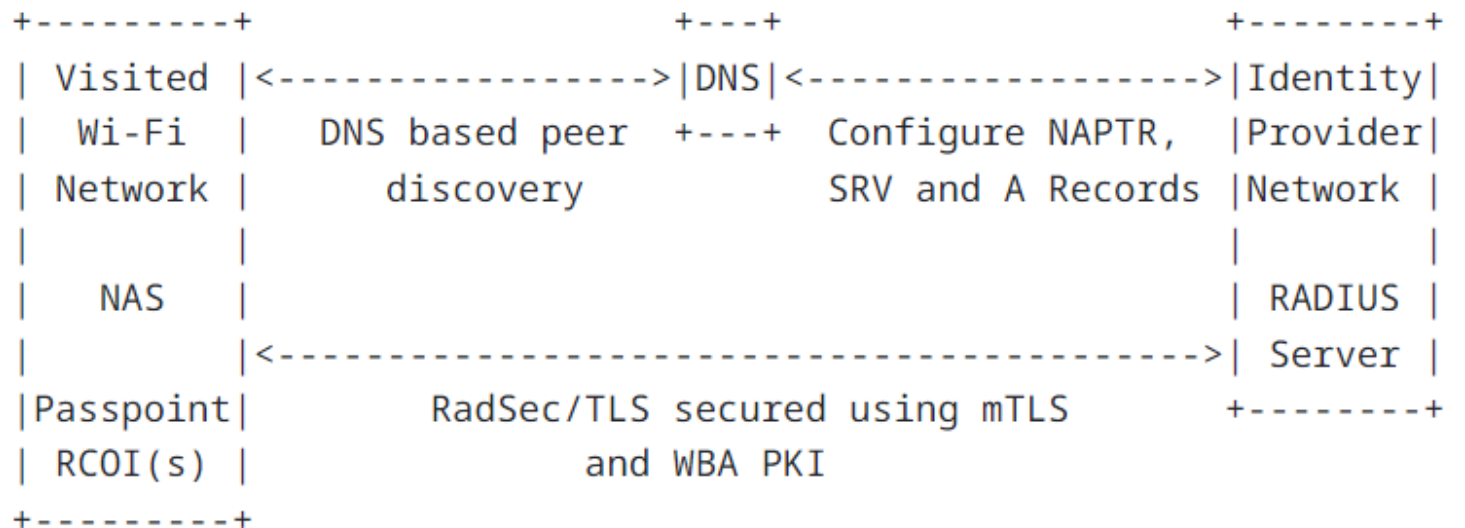
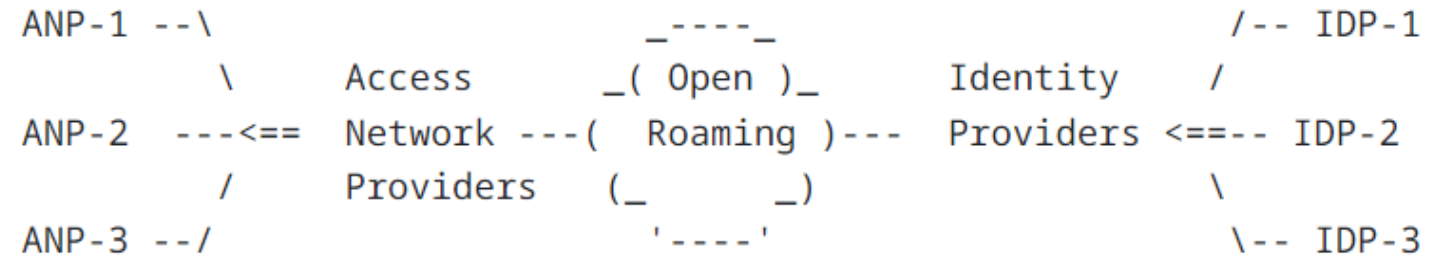
Objectives – Enable ubiquitous Wi-Fi connectivity by private networks using identity provider credentials

OpenRoaming mission statement is to create an open framework for all types of players to develop their Wi-Fi services & business

Cloud Federation

Cybersecurity Service

Network Automation



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, CAPPOT,
RADEXT, DISPATCH

Embedded Unique Identifiers

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



Operator Namespace Identifier for Radius Attribute 126

Identifier	Token	Contact
0x34	WBAID	WBA Director

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



SMI Network Management Private Enterprise Codes:

Prefix: iso.org.dod.internet.private.enterprise (1.3.6.1.4.1)

PEN: 14122

3. WBA Roaming Consortium Federation (RCOI)



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

* OpenRoaming-Settlement-Free: 5A-03-BA-xx-x

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

Level	Description	Comment
Level 1	OpenRoaming Root Certificate Authority	Operation managed by WBA
Level 2	OpenRoaming Policy Intermediate Certificate Authority	Operation managed by WBA. Instantiates WBA policy OID
Level 3	OpenRoaming Issuing Intermediate Certificate Authority	Operated by an OpenRoaming broker
Level 3	OpenRoaming Registration Authority	Optional and when used, operated by an OpenRoaming broker
Level 4	OpenRoaming Entity	A WBA member or non-member. WBA's Certificate Policy requires the Entity's WBAID is included in the Subject UID field in the certificate.

Standard Closed Access Groups: Enable Enhanced Policy Enforcement

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

* OpenRoaming-Settlement-Free: 5A-03-BA-xx-x

OUI-36 Octet 4								OUI-36 Octet 5			
B7	B6	B5	B4	B3	B2	B1	B0	B7	B6	B5	B4
LoA	QoS	PID	ID-Type	Reserved - set to 0							

LoA Field	Description
B7	
0	Baseline Identity Proofing
1	Enhanced Identity Proofing

QoS Field		Description
B6	B5	
0	0	Bronze
0	1	Silver
1	0	Reserved
1	1	Reserved

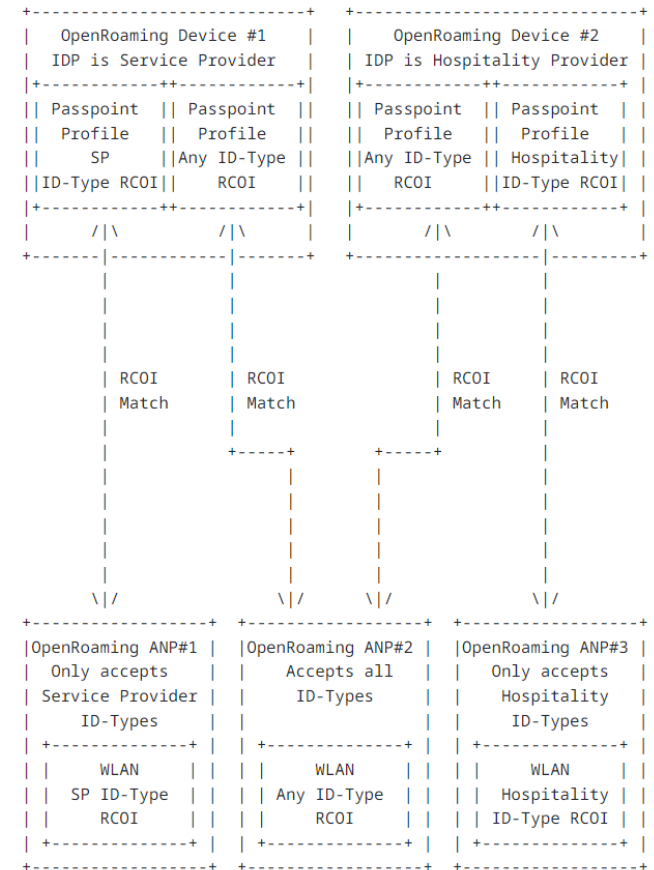
PID Field	Description
B4	
0	Baseline ID Policy applies, i.e., users remain anonymous whilst using the service
1	A Permanent ID will be returned by the IDP

Merging Islands of Connectivity into a Common Federation

ID-Type Field				Description
B3	B2	B1	B0	
0	0	0	0	Any identity type is permitted
0	0	0	1	A service provider identity
0	0	1	0	A cloud provider identity
0	0	1	1	A generic enterprise identity
0	1	0	0	A government identity, e.g., including city
0	1	0	1	An automotive identity
0	1	1	0	A hospitality identity
0	1	1	1	An aviation industry identity
1	0	0	0	An education or research identity
1	0	0	1	A cable industry identity
1	0	1	0	A manufacturer identity
1	0	1	1	A retail identity
other values				Reserved

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



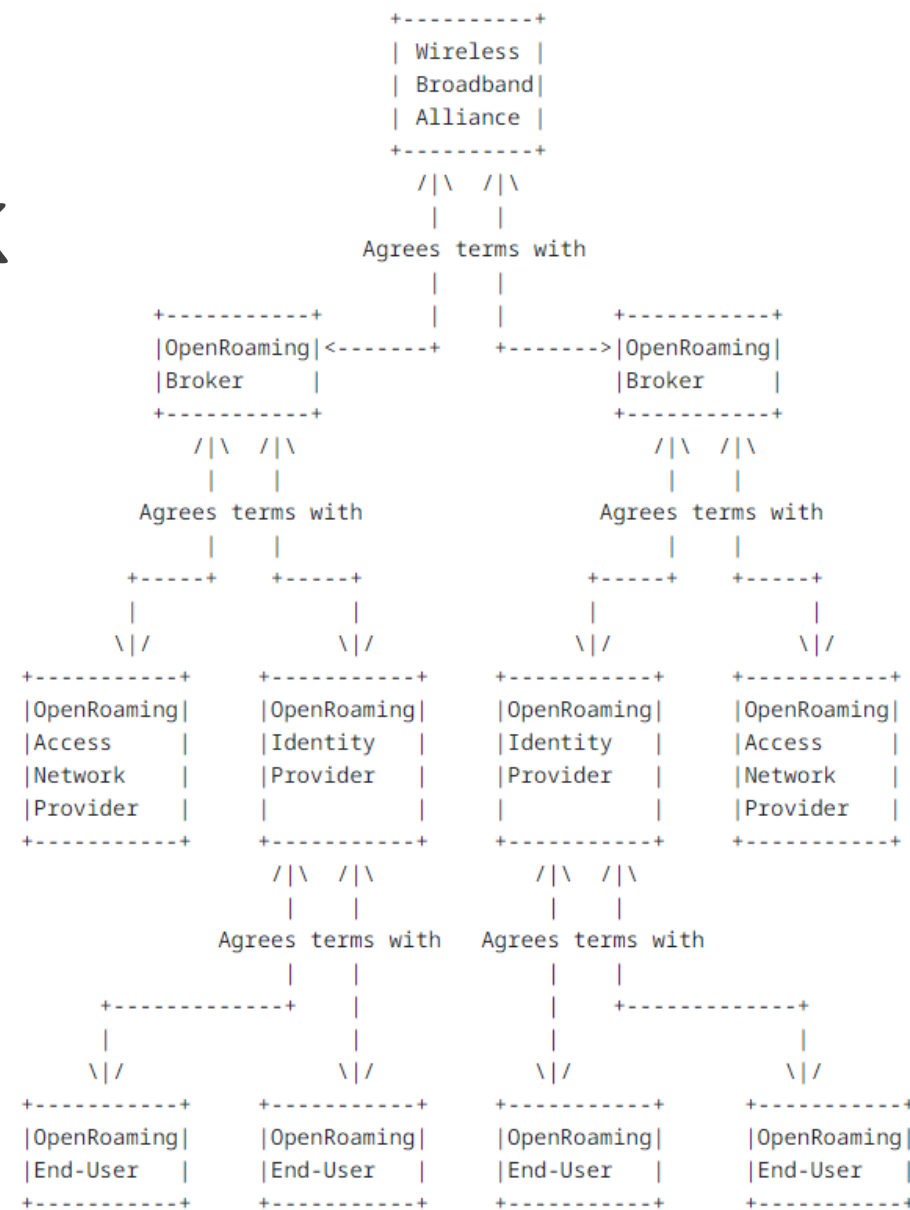
Scalable Legal Framework

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



Q&A

Thank you

Bruno Tomas – bruno@wballiance.com

DNS process of resolving OpenRoaming realm authentication

