Workgroup: Independent Submission
Internet-Draft: draft-tomas-openroaming-00
Published: 13 June 2023
Intended Status: Informational
Expires: 15 December 2023
Authors: B. Tomas
Wireless Broadband Alliance, Inc.
M. Grayson
Cisco Systems
N. Canpolat
Intel Corporation
B. A. Cockrell
SingleDigits
S. Gundavelli
Cisco Systems

WBA OpenRoaming Wireless Federation

Abstract

This document describes the Wireless Broadband Alliance's OpenRoaming system. The OpenRoaming architectures enables a seamless onboarding experience for devices connecting to access networks that are part of the federation of access networks and identity providers. The primary objective of this document is to describe the protocols that form the foundation for this architecture, enabling providers to correctly configure their equipment to support interoperable OpenRoaming signalling exchanges. In addition, the topic of OpenRoaming has been raised in different IETF working groups, and therefore a secondary objective is to assist those discussions by describing the federation organization and framework.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 15 December 2023.

Copyright Notice

(https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Table of Contents

1. Introduction

WBA OpenRoaming is a roaming federation service of Access Network Providers (ANPs) and Identity Providers (IDPs), enabling an automatic and secure Wi-Fi experience globally. WBA OpenRoaming creates the framework to seamlessly connect billions of users and things to millions of Wi-Fi networks.

Figure 1: OpenRoaming Federation

WBA Openroaming was inspired by eduroam [RFC7593], the roaming federation that has become the standard for secure access in research and education and which performs over half a billion roaming authentications per month. WBA OpenRoaming leverages the same capabilities defined to be used across the eduroam community, including the RadSec protocol [RFC6614] which has allowed eduroam to replace static routing of RADIUS signalling [RFC2865] based on realm routing tables with [RFC7585] based DNS based dynamic discovery of RADIUS endpoints and mutual authentication of RADIUS peers using TLS.

WBA OpenRoaming builds on these same foundations and defines a global federation that is targeted at serving all communities, while supporting both settlement-free use cases where "free" Wi-Fi is being offered to end-users in order to support some alternative value proposition, as well as traditional settled "paid" for Wi-Fi offered by some cellular providers.

OpenRoaming is designed to deliver end-to-end security between a Network Access Server deployed by an OpenRoaming Access Network Provider and an EAP Server [RFC3748] deployed by an OpenRoaming

Identity Provider. The security of the solution is based on mTLS using certificates issued under Wireless Broadband Alliance's Public Key Infrastructure [RFC5280].

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Terminology

Access Network Query Protocol (ANQP):

An IEEE 802.11 defined protocol that allows for access network information retrieval in a pre-association state. ANQP has been further extended by the Wi-Fi Alliance (WFA) as part of its Passpoint program [PASSPOINT].

Access Network Provider (ANP):

An entity that has joined the federation and serves OpenRoaming end-users by configuring the OpenRoaming RCOI(s) in its Wi-Fi equipment.

Broker:

An entity that has joined the federation and performs certain specific roles to help scale the operation of the federation. The separate roles of a broker can include:

1. Assigning WBA identities to ANPs and IDPs.

2. Operating an issuing intermediate certificate authority under the WBA's PKI and issuing certificates to ANPs and IDPs.

3. Operating a registration authority to a third party operated issuing intermediate certificate authority under WBA's PKI to enable certificates to be issued to ANPs and IDPs.

Closed Access Group (CAG):

The definition of the 12 most significant bits of an OUI-36 RCOI to indicate OpenRoaming policy controls that can be enforced by ANPs and IDPs.

Identity Provider (IDP):

An entity that has joined the federation and includes the OpenRoaming RCOI(s) in the Passpoint profile of its end-user devices and authenticates end-user devices on OpenRoaming ANP networks.

Level of Assurance (LoA):

An ISO/IEC 29115 term that is used to define equivalent levels for handling of end-user enrollment, credential management and authentication amongst different IDPs.

OpenRoaming-Settled:

The "base RCOI" of BA-A2-D0 that is used to indicate that the ANP expects to receive payment for providing OpenRoaming service to end-users.

OpenRoaming-Settlement-Free:

The "base RCOI" of 5A-03-BA that is used to indicate that the ANP provides the OpenRoaming service to end-users at no cost to the IDP.

Passpoint Profile:

Passpoint is a Wi-Fi Alliance (WFA) certification program that defines the use a Passpoint profile, that includes the user's credentials and the access network identifiers, to enables mobile devices to discover and authenticate to Wi-Fi hotspots that provide Internet access [PASSPOINT].

PLMN Id:

It is a unique identifier for a mobile network operator. The identifier consists of a MCC (Mobile Country Code) and MNC (Mobile Network Code).

Roaming Consortium Identifier (RCOI):

RCOI identifies the groups of identity providers that are supported by the network. It is a 3-octet, or a 5-octet value carried in the 802.11 beacon information element (IE). It is also sent in the ANQP messages. Based on the access technologies, the specific link-layer protocols will be used for carrying the RCOI. RCOI is also part of the Passpoint profile.

Subscriber Identity Module (SIM):

The SIM is traditionally a smart card distributed by a mobile operator.

WBA Identity (WBAID):

A hierarchical namespace that is used to uniquely identify every OpenRoaming entity.

Wireless Roaming Intermediary eXchange:

A framework, aimed at facilitating interconnectivity between operators and the Wi-Fi roaming hub services.

2. Wireless Broadband Alliance

The Wireless Broadband Alliance (WBA) defines the Wireless Roaming Intermediary eXchange (WRIX) framework, aimed at facilitating interconnectivity between Wi-Fi operators and the Wi-Fi roaming hub services, as well as the Carrier Wi-Fi Services program that provides guidelines to improve customer experience on Carrier Wi-Fi networks. Both of these programs leverage the Wi-Fi Alliance specified Passpoint functionality [PASSPOINT] to enable automatic and secure connectivity to Wi-Fi networks, allowing devices to be provisioned with network access credentials with minimal user interaction.

WBA programs have traditionally focussed on "offloading" cell phone data from cellular networks onto Wi-Fi networks. Deployments of such systems have seen uneven adoption across geographies, with cellular operators frequently limiting their engagement to premier locations that have deployed Wi-Fi and experience a significant footfall of operator's customers.

Whereas conventional Carrier Wi-Fi has focused on premier locations, the last decade has seen a continued increase in the requirements of private Wi-Fi networks to be able to serve visitors, contractors and guest users. Moreover, in most of these scenarios, the Wi-Fi network is primarily being used to support some alternative value proposition; an improved retail experience in a shopping mall, a more efficient meeting in a carpeted office, a superior stay in a hospitality venue, or a better fan experience in a sporting arena. Traditionally, this segment has made wide-scale use of captive portals and unencrypted Wi-Fi links to onboard end-users onto their networks [RFC8952]. However, the decreasing costs for cellular data means end-users are less motivated to search out and attach to such "free" Wi-Fi networks, and as a consequence, captive portal conversion rates continue to decrease.

As a consequence, in 2020 WBA launched its OpenRoaming federation, designed to provide a better on-boarding experience to end-users, that is seamless, scalable and secure.

3. OpenRoaming Architecture

Figure 2 contrasts a conventional carrier Wi-Fi roaming system with OpenRoaming. As illustrated, conventional Wi-Fi roaming is typically based on:

1. IPSec [RFC6071] tunnels established between access networks, hub providers and identity providers used to protect exchanged signalling.

2. Static routing of RADIUS signalling [RFC2865] based on realm routing tables populated according to agreements between access networks and hub providers.

3. Passpoint primarily used with SIM based identifiers, where individual PLMN-IDs are configured in the access networks WLAN equipment and cellular providers enable Passpoint based SIM authentication in end-user devices.

4. EAP-AKA [RFC4187] based passpoint authentication exchanged between the Supplicant in the end-user device and the EAP Server in the cellular provider's network.

5. A primary focus on carrier based identities where the end-user has a billing relationship with the carrier.

In contrast, OpenRoaming is based on:

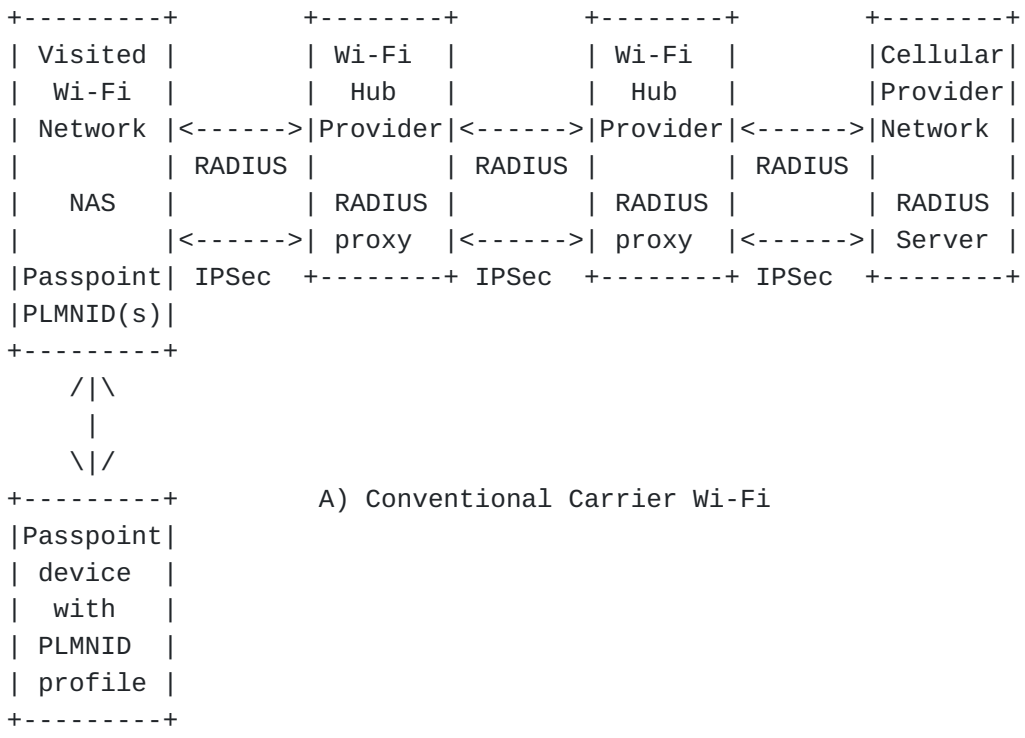
1. RadSec signalling [RFC6614] secured using mTLS with certificates issued under WBA's private certificate authority.

2. Dynamic routing of RADIUS based on DNS-based discovery of signalling peers [RFC7585]

3. Passpoint based network selection based on 36-bit Roaming Consortium Organization Identifiers (RCOIs), where WBA defines the use of 12-bits of the RCOI to embed closed access group policies.

4. Passpoint authentication that can use any of the Passpoint defined EAP methods.

5. Encompassing new identity providers who do not have a billing relationship with their end-users.



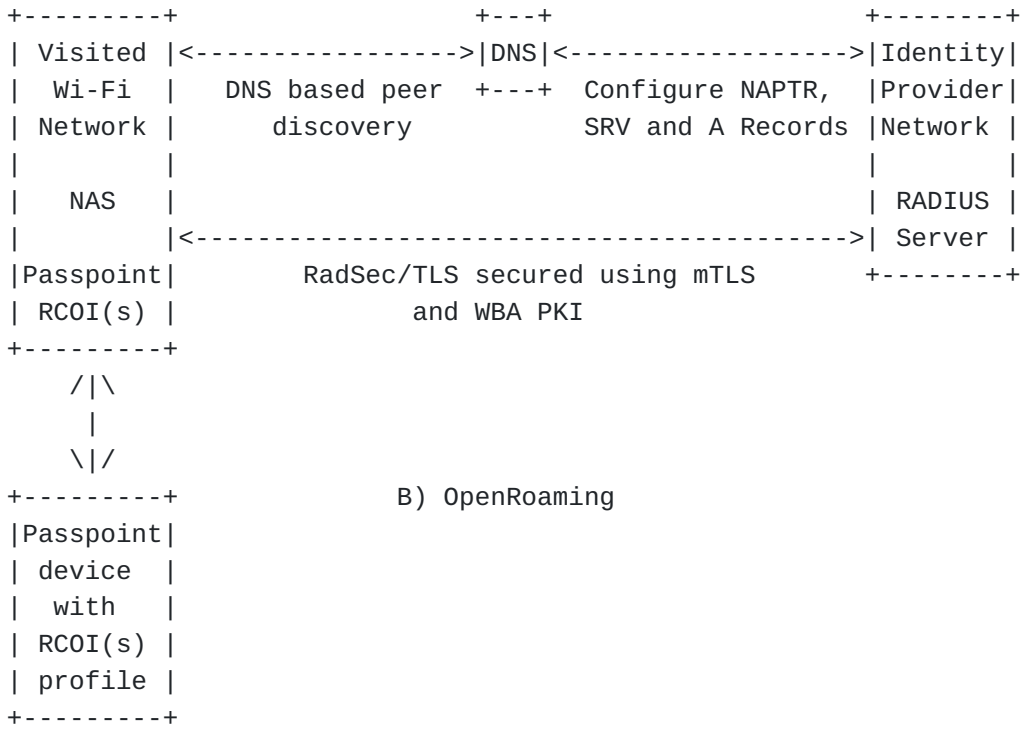


Figure 2: Contrasting Carrier Wi-Fi and OpenRoaming Architectures

4. Identifying OpenRoaming Entities

All OpenRoaming providers and OpenRoaming brokers are allocated a WBA Identity (WBAID). The WBAID is defined to be transported in the RADIUS Operator-Name attribute (#126) [RFC5580]. WBA has been allocated the Operator Namespace identifier 0x34 "4" to identify an Operator-Name attribute carrying a WBAID.

The WBAID is a hierarchical namespace that comprises at its top level the identity allocated by WBA to a WBA Member and is of the form shown in Figure 3 where the optional 2 upper case characters represent an ISO-3166 Alpha-2 country code [ISO3166] e.g., "WBAMEMBER:US".

```
upper-case-char = %x41-5a
member-id       = 1*upper-case-char
wbaid           = member-id [ %x3a 2*2upper-case-char]
```

Figure 3: ABNF definition of Primary WBAID Structure

Operating as an OpenRoaming broker, the WBA Member is able to allocate subordinate identities to OpenRoaming providers who are not WBA members by pre-pending a subordinate identity , plus "." (%x2e) to the Member's WBAID, e.g., OPENROAMINGPROVIDER.WBAMEMBER:US. In this way, any receiving entity of a WBAID can identify the WBA Member who is acting as an OpenRoaming broker to the provider by assigning it an identity.

5. Scaling Secured Signalling

As described in Appendix C, the OpenRoaming legal framework does not assume any direct relationship between ANP and IDP. In order to scale the secured signalling between providers, the federation makes use of Public Key Infrastructure using a private Certificate Authority specifically designed to secure the operations of the roaming federation. WBA and its members have published the WBA Certificate Policy that defines the policies which govern the operations of the PKI components by all individuals and entities within the infrastructure. The OID for Wireless Broadband Alliance is:

{ iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) The Wireless Broadband Alliance(14122) }

The Wireless Broadband Alliance organizes its OID arcs for the Certificates Policy Documents using the object identifier 1.3.6.1.4.1.14122.1.1. At the time of writing, the current certificate policy is 1.3.6.1.4.1.14122.1.1.6.

This Certificate Policy is based on a 4-level hierarchy, as illustrated below.

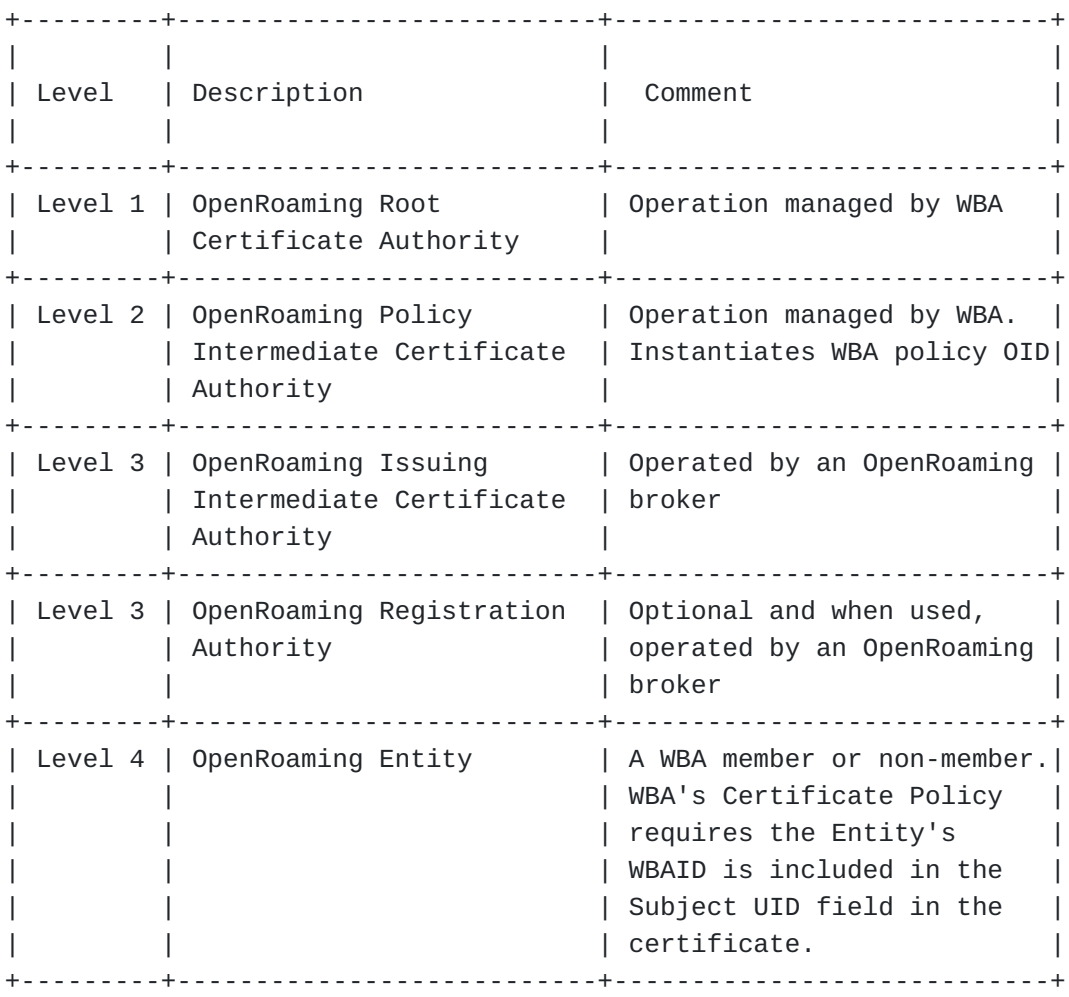


Figure 4: OpenRoaming PKI Hierarchy

Certificates issued under the WBA PKI are used by Entities to perform mutual authentication with other Entities and to secure RadSec signalling [RFC6614] that carries EAP-based Passpoint authentication. This is typically between a RadSec client in the OpenRoaming ANPs network and an RadSec Server in the OpenRoaming IDPs network, although a provider can decide to outsource the operation of the RadSec endpoint to a third party provider.

6. IDP Discovery

6.1. Dynamic Discovery

OpenRoaming defines the use of dynamic discover [RFC7585] by which an ANP discovers the IP address of the IDP's RadSec server.

6.2. Discovery of EAP-AKA Servers

Passpoint defines the use of EAP-AKA' based authentication [RFC5448] which uses the 3GPP 23.003 [TS23003] defined realm of wlan.mnc<mnc>.mcc<mcc>.3gppnetwork.org, where <mcc> represent an E. 212 Mobile Country Code and <mnc> represents the E.212 Mobile Network Code allocated to the IDP. GSMA is responsible for operating the 3gppnetwork.org domain and GSMA IR.67 [GSMAIR67] limits access to the DNS systems supporting such records to those systems on the inter-PLMN IP backbone (known as "GRX/IPX"). As OpenRoaming ANPs do not connect to this inter-PLMN backbone, then conventional realm based lookup cannot be used to discover the RadSec server supporting EAP-AKA' authentication.

GSMA IR.67 does allow systems to be discoverable from the public Internet, specifically calling out the use of the pub. 3gppnetwork.org domain name for such procedures. In order for ANPs to dynamically discover the RadSec server supporting EAP-AKA' authentication, GSMA has defined the use of the wlan.mnc<mnc>.mcc<mcc>.pub.3gppnetwork.org by OpenRoaming systems. This means that whenever a RadSec client receives a user-name containing an NAI formatted as user@wlan.mnc<mnc>.mcc<mcc>. 3gppnetwork.org, the dynamic peer detection functionality MUST insert "pub" into the realm and perform DNS based dynamic discovery using the wlan.mnc<mnc>.mcc<mcc>.pub.3gppnetwork.org domain name. The RADIUS user-name attribute MUST NOT be similarly modified.

IR.67 defines the procedure by which a cellular operator can request the delegation of their wlan.mnc<mnc>.mcc<mcc>.pub.3gppnetwork.org domain. GSMA PRD IR.67 also allows an MNO to delegate the entire mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org sub-domain which could have already occurred, e.g., to enable use of the epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org for Wi-Fi calling service. Using this approach, a cellular operator operating as an OpenRoaming IDP can authenticate their end-users on third party ANP Wi-Fi networks.

6.3. Proving a server is authoritative for a realm

The OpenRoaming preferred approach by which a dynamically discovered RadSec server can prove that it is authoritative for a particular realm or set of realms is to use DNS records that are protected with DNSSEC [RFC4035]. However, GSMA have not enabled DNSSEC on their 3gppnetwork.org domain, meaning that DNSSEC cannot be applied on the publicly resolvable domains under pub.3gppnetwork.org. Because of this situation, OpenRoaming does not currently mandate operation of DNSSEC.

If the DNS records are not protected with DNSSEC, the IDP SHOULD ensure that the discovered RadSec server(s) supporting its realm(s) is/are configured with a WBA-PKI server certificate that includes the realm(s) in the certificate SubjectAltName. The SubjectAltName field(s) is/are used to prove that the RadSec server is authoritative for a particular realm, or set of realms.

7. OpenRoaming Passpoint Profile

7.1. OpenRoaming Policy Controls

In order to avoid possible fragmentation of roaming federations, OpenRoaming recognizes that there is a need to permit OpenRoaming to be integrated into a variety of different use-cases and value propositions. These use-cases include scenarios where providers are able to enforce policy controls of end-users accessing the service. The realization of policy controls in the OpenRoaming federation is a balance between the requirements for fine grain policy enforcement versus the potential impact of policy enforcement on the user experience.

Such a level of control is realized using Closed Access Group (CAG) based policies. A Closed Access Group identifies a group of OpenRoaming users who are permitted to access one or more OpenRoaming access networks configured with a particular CAG policy. These Closed Access Group policies are encoded using one or more Roaming Consortium Organization Identifiers (RCOIs), first defined in Passpoint Release 1.0, and well supported across the smartphone device ecosystem.

Note, encoding CAG policies in OpenRoaming using one or more RCOIs is aimed at delivering an equivalent functionality to the CAG policies encoded in 3GPP using one or more CAG-IDs.

7.2. OpenRoaming Closed Access Group Policies

OpenRoaming defines the use of multiple RCOIs to facilitate the implementation of closed access group policies across the federation. The currently defined RCOIs are:

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

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

Figure 5 shows how the 24-bit length OpenRoaming RCOIs are further extended into 36-bit length OUI-36s with additional context dependent identifiers used to encode specific closed access group policies. Following Passpoint Release 1.0 specification, only when there is a bitwise match of all 36 bits of the configured RCOI in

the WLAN equipment and the Passpoint profile configured in the end-user device will an EAP authentication be triggered.

The encoding of closed access group policies is defined so that the "no-restrictions" policy is encoded using the 12-bit value "00-0", i.e., 54-03-BA-00-0 represents a policy that accepts all OpenRoaming settlement-free users onto a particular ANP installation.

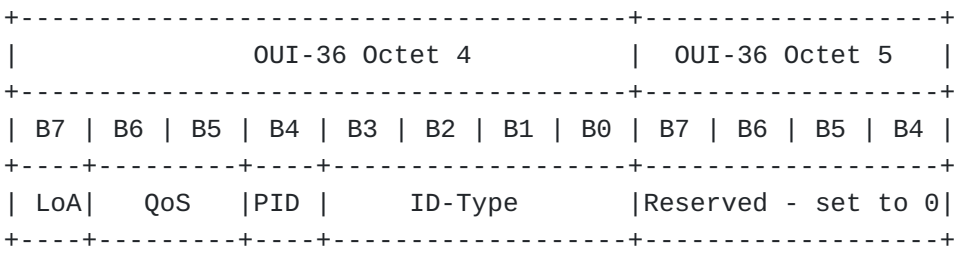


Figure 5: Extension of Octets 4 and 5 for OpenRoaming Context Dependent RCOI Field

7.2.1. Level of Assurance Policies

The format of the Level of Assurance (LoA) field is as shown in Figure 6.

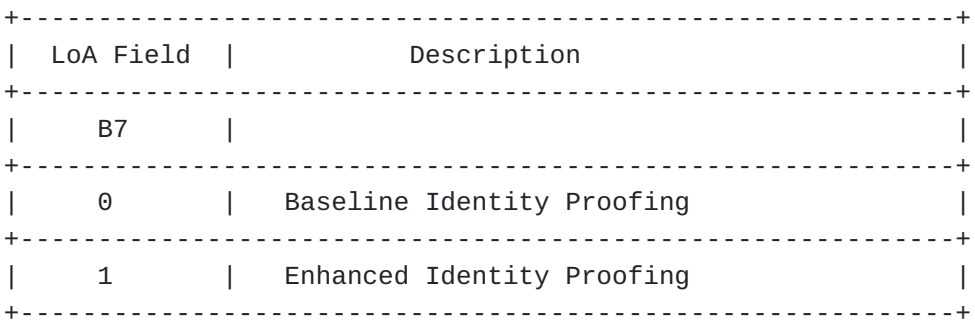


Figure 6: OpenRoaming CAG LoA Field

The baseline identity proofing requirement on IDPs ensures that all OpenRoaming identities are managed with at least a medium level of assurance (LoA level 2) for end-user enrollment, credential management and authentication, as specified in ISO/IEC 29115 [ISO29115].

Any IDP that manages its identities according to ISO/IEC 29115 LoA level 2 MUST NOT configure any RCOI in their end-users' Passpoint profile with the LoA field set to "1". Conversely, an IDP that manages its identities according to ISO/IEC 29115 LoA level 3 MAY

configure multiple RCOIs in their end-users' Passpoint profile, including RCOIs with the LoA field set to "0" and RCOIs with the LoA field set to "1".

The LoA field is used to support ANPs which operate in regulatory regimes that require enhanced identity proofing to be used in the provision of credentials on OpenRoaming devices, equivalent to LoA level 3 in ISO/IEC29115 [ISO29115]. In such a scenario, the ANP can set the LoA bit field to 1 in all configured RCOIs to ensure that only identities provisioned using enhanced LoA 3 procedures can access via the ANP's network.

7.2.2. Quality of Service Policies

One of the challenges faced by users of Wi-Fi hotspots is when the Wi-Fi network is configured sub-optimally and results in a poor user experience. Often the only remedy open to a user it to disable the Wi-Fi interface on their smartphone and continue to use cellular data. As a consequence, OpenRoaming defines specific service tiers across the federation using the QoS field. The format of the QoS field is shown in Figure 7.

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

Figure 7: OpenRoaming CAG QoS Field

The "Bronze" and "Silver" values of QoS field are used to identify specific quality of service policy aspects.

The bronze service tier corresponds to the following:

1. The availability of OpenRoaming service when used to access the Internet measured during scheduled operations across the ANP's network exceeds 90% over any one month period.

2. The aggregate bandwidth used to receive Internet service on the ANP's network is sufficient to enable each and every

authenticated and authorized OpenRoaming end-user to simultaneously receive a sustained 256 kilobits per second connection.

The silver service tier corresponds to the following:

1. The availability of OpenRoaming service when used to access the Internet measured during scheduled operations across the ANP's network exceeds 95% over any one month period.

2. The aggregate bandwidth used to receive Internet service on the ANP's network is be sufficient to enable each and every authenticated and authorized end-user to receive a sustained 512 kilobits per second connection.

3. At least 10% of authenticated and authorized users are able to stream video content at a downlink rate of at least 5 megabits per second (when measured over a one-minute interval) over all of the ANP's OpenRoaming enabled Wi-Fi networks.

4. The authenticated and authorized end-users are able to stream video from one or more third party content distribution networks with an end-to-end latency of less than 150ms from all of the ANP's OpenRoaming enabled Wi-Fi networks.

The QoS field can be used by those IDPs that are only interested in providing their end-users with a higher quality service level when automatically authenticated onto an OpenRoaming network. For example, an IDP configures the QoS field as bronze in a Passpoint profile that uses the "5A-03-BA" settlement free RCOI and configure the QoS field as silver in a Passpoint profile that uses the "BA-A2-D0" OpenRoaming-settled paid service.

ANPs that only support the bronze service tier MUST set the QoS Field to "00" in all RCOIs configured on their WLAN equipment. ANPs that support the silver service tier MAY configure multiple RCOIs on their WLAN equipment that include values where the QoS field is set to "01" and values where the QoS field is set to "00".

7.2.3. Privacy Policies

The baseline privacy policy of OpenRoaming ensures the identities of end-users remain anonymous when using the service. The PID field can be used to support scenarios where the user has consented with their IDP that their permanent ID can be signalled to the ANP in the RADIUS Access-Accept. The format of the PID field is illustrated in Figure 8. The PID field can be configured to "1" in the RCOIs used by those ANPs that want to be be able to account for unique OpenRoaming end-users.

The OpenRoaming IDP terms ensure subscribers explicitly give their permission for their permanent identity to be shared with a third party ANP. When such permission has not been granted, an IDP MUST NOT set the PID field to "1" in any of the RCOIs in its end-user Passpoint profiles. When such permission has been granted, an IDP MAY configure multiple RCOIs in their end-users' Passpoint profile, including RCOIs with the PID field set to "0" and RCOIs with the PID field set to "1".

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

Figure 8: OpenRoaming CAG PID Field

7.2.4. ID-Type Policies

The ID-Type field can be used to realize policies which are based on the business sector associated with the identity used by the IDP. The format of the ID-Type field is illustrated in Figure 9.

All IDPs configure at least one RCOI in their end-user's Passpoint profile with ID-Type set to "0000" (Any identity type is permitted). An IDP MAY configure additional RCOIs in their end-users' Passpoint profile with an ID-Type representing the sector type of IDP.

An ANP what wants to serve all end-users, irrespective of sector, configures RCOIs in the WLAN equipment with ID-Type set to "0000". Alternatively, an ANP which operates a sector specific business that only desires to serve a subset of OpenRoaming end-users MAY set the ID-Type to their desired sector in all configured RCOIs.

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

Figure 9: OpenRoaming CAG ID-Type Field

7.3. Prioritizing Policies

The definition of OpenRoaming closed access group policies assumes the configuration of multiple RCOIs in ANP WLAN equipment and IDP end-user devices.

When a device has multiple Passpoint profiles matching the ANP's RCOI policy, an OpenRoaming ANP may want to prefer OpenRoaming subscribers use a particular IDP's profile when attaching to its access network. Such a preference can be because the OpenRoaming ANP has a preferential relationship with certain OpenRoaming IDPs.

The OpenRoaming ANP is able to use the Home SP preference functionality defined in Passpoint [PASSPOINT] to prioritize the use of a particular profile by a Passpoint enabled device. In such a scenario, the ANP configures the Domain Name list to include the FQDN(s) associated with the profile(s) to be prioritized.

8. OpenRoaming RADIUS Profile

The OpenRoaming RADIUS profile is based on WBA WRIX Specifications which in turn are derived from [RFC3580] and [RFC3579].

Additionally, OpenRoaming defines the use of the following RADIUS attributes.

8.1. Operator-Name

As described in Section 4, OpenRoaming uses the Operator-Name (#126) [RFC5580] attribute to signal the WBAID of the OpenRoaming ANP. All ANPs MUST support the Operator-Name attribute and use it to signal the WBAID of the OpenRoaming ANP.

8.2. Chargeable-User-Identity

All OpenRoaming ANPs MUST support the Chargeable-User-Identity attribute (#89) [RFC4372]. When an end-user has consented to sharing a permanent identity with the ANP, the CUI returned by the IDP is invariant over subsequent end-user authentication exchanges between the IDP and the ANP.

8.3. Location-Data/Location-Information

All OpenRoaming ANPs MUST support signalling of location information using [RFC5580]. As a minimum, all OpenRoaming IDPs need to be able to determine the country in which the OpenRoaming ANP operates. The OpenRoaming legal framework described in Appendix C serves as an "out-of-band agreement" as specified in clause 3.1 of [RFC5580]. Hence, all OpenRoaming ANPs MUST include the Location-Data attribute (#128) in RADIUS Access-Request messages where the location profile is the civic location profile that includes the country code where the ANP is located in all Access-Request messages [RFC5580].

When the OpenRoaming ANP supports the OpenRoaming-Settled RCOI ("BA-A2-D0"), the Location-Data attribute (#128) MUST be included where the location profile is the civic location profile containing Civic Address Type information that is sufficient to identify the financial regulatory regime that defines the taxable rates associated with consumption of the ANP's service.

OpenRoaming also defines the optional use the geospatial location profile as specified in [RFC5580]. ANPs MAY signal coordinate-based

geographic location of the NAS or end-user device and this information MAY be used by IDPs, e.g., in their authorization decisions.

8.4. WBA-Identity-Provider

The Operator-Name attribute allows the WBAID of the ANP to be signalled to the IDP. In the reverse direction, the IDP MUST use the WBA-Identity-Provider vendor specific attribute [WBAVSA] to signal the WBAID of the IDP back to the ANP.

8.5. WBA-Offered-Service

The ANP MAY use the WBA-Offered-Service vendor specific attribute to signal the highest OpenRoaming service tier supported on its network [WBAVSA].

8.6. Additional attributes related to OpenRoaming settled

OpenRoaming settled defines the use of additional RADIUS attributes.

8.6.1. WBA-Financial-Clearing-Provider

All OpenRoaming ANPs and IDPs that support the OpenRoaming settled service MUST use the WBA-Financial-Clearing-Provider vendor specific attribute to signal the identity of the provider of financial clearing services [WBAVSA].

8.6.2. WBA-Data-Clearing-Provider

All OpenRoaming ANPs and IDPs that support the OpenRoaming settled service MAY use the WBA-Data-Clearing-Provider vendor specific attribute to signal the identity of the provider of data clearing services [WBAVSA].

8.6.3. WBA-Linear-Volume-Rate

In cellular roaming, inter-operator tariff information is exchanged in the roaming agreements between operators. In OpenRoaming, as there is no direct agreement between ANPs and IDPs, the tariff information is exchanged in RADIUS messages. All OpenRoaming ANPs that support the OpenRoaming settled service MUST use the WBA-Linear-Volume-Rate vendor specific attribute to signal the charging model being offered by the ANP [WBAVSA]. An IDP that authorizes an offered charging model MUST include the agreed WBA-Linear-Volume-Rate in the Access-Accept message.

9. Security Considerations

9.1. Network Selection and Triggering Authentication

OpenRoaming defines the use of Passpoint with Roaming Consortium Organization Identifiers. A bit-wise match between an RCOI configured in the Passpoint profile of an end-user's device and the RCOI signalled by WLAN equipment will trigger a Passpoint defined EAP-based authentication exchange. The security associated with the Passpoint RCOI information element is identical to other PLMN-ID and Realm information elements, allowing an unauthorized system to configure the OpenRoaming RCOI with the aim of triggering a Passpoint authentication. Because such unauthorized system will not have been issued with a certificate using WBA's PKI, the unauthorized system is unable to communicate with any other OpenRoaming provider. In such a scenario, after repeated failed authentication attempts, the device's supplicant can add the Access Point's BSSID to a deny list to avoid future triggering of an authentication with the unauthorized system.

9.2. Dynamic Discovery of RadSec Peers

OpenRoaming recommends the use of DNSSEC to ensure a dynamically discovered RadSec server is authoritative for a particular realm or set of realms. Where this is not possible, e.g., when using dynamic resolution with the pub.3gppnetwork.org sub-domain, the OpenRoaming certificate policy permits the configuration of supported realm(s) in the SubjectAltName of the certificate(s) issued to the IDP.

An ANP can decide to continue with the RadSec establishment, even if a server cannot prove it is authoritative for a realm. As the ANP's RadSec client uses a dedicated trust anchor corresponding to the WBA's private Certificate Authority, if DNS is hijacked by a third-party non-federation member who has not been issued a certificate under WBA's PKI, the subsequent TLS establishment will fail.

9.3. End-User Traffic

The OpenRoaming federation ensures RADIUS traffic is secured between ANP and IDP and ensures Wi-Fi traffic is protected between the end-user device and the WLAN equipment of the ANP. The ANP is therefore able to observe IP traffic to/from end-users who have performed a successful authentication with their IDP. The OpenRoaming legal framework (see Appendix C) ensures that the ANP has agreed to the OpenRoaming Privacy Policy [ORPRIVACY] to correctly handle the personally identifiable information collected as part of providing the ANP service.

The Open-Roaming end-user terms and conditions [ORTERMS] ensure that users are aware that the federation does not provide a secure end-

to-end service. The end-user should not rely on the encryption delivered by OpenRoaming for providing security of services accessed using the ANP's Wi-Fi network.

10. Future Enhancements

WBA announced the launch of its OpenRoaming Federation in June 2020. Since then, WBA members have continued to enhance the technical framework to address new market requirements that are reflected in the Closed Access Group policies described in Section 7.2 and the RADIUS profile described in Section 8. WBA encourages those parties interested in adapting OpenRoaming to address new requirements to join the Alliance and help drive the definition of OpenRoaming forward.

11. IANA Considerations

This document has no IANA actions.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

12.2. Informative References

[GSMAIR67] GSMA, "GSMA IR.67: DNS Guidelines for Service Providers and GRX and IPX Providers", 25 November 2022, <https://www.gsma.com/newsroom/wp-content/uploads//IR.67-v21.0.pdf>.

[ISO29115] ISO/IEC 29115, "Information technology - Security techniques: Entity authentication assurance framework", April 2013.

[ISO3166] ISO 3166-2:2020, "Codes for the representation of names of countries and their subdivisions", August 2020, <https://www.iso.org/standard/72483.html>.

[ORPRIVACY] Wireless Broadband Alliance, "OpenRoaming End-User Privacy Policy", n.d., <https://wballiance.com/openroaming/privacy-policy/>.

[ORTERMS] Wireless Broadband Alliance, "OpenRoaming End User Terms and Conditions", n.d., <https://wballiance.com/openroaming/toc/>.

[PASSPOINT] Wi-Fi Alliance, "Wi-Fi Alliance Passpoint", n.d., <https://www.wi-fi.org/discover-wi-fi/passpoint>.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <https://www.rfc-editor.org/info/rfc2865>.

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, DOI 10.17487/RFC3579, September 2003, <https://www.rfc-editor.org/info/rfc3579>.

[RFC3580] Congdon, P., Aboba, B., Smith, A., Zorn, G., and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC 3580, DOI 10.17487/RFC3580, September 2003, <https://www.rfc-editor.org/info/rfc3580>.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC 3748, DOI 10.17487/RFC3748, June 2004, <https://www.rfc-editor.org/info/rfc3748>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <https://www.rfc-editor.org/info/rfc4035>.

[RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, DOI 10.17487/RFC4187, January 2006, <https://www.rfc-editor.org/info/rfc4187>.

[RFC4372] Adrangi, F., Lior, A., Korhonen, J., and J. Loughney, "Chargeable User Identity", RFC 4372, DOI 10.17487/RFC4372, January 2006, <https://www.rfc-editor.org/info/rfc4372>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC5448] Arkko, J., Lehtovirta, V., and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')", RFC 5448, DOI 10.17487/RFC5448, May 2009, <https://www.rfc-editor.org/info/rfc5448>.

[RFC5580] Tschofenig, H., Ed., Adrangi, F., Jones, M., Lior, A., and B. Aboba, "Carrying Location Objects in RADIUS and Diameter", RFC 5580, DOI 10.17487/RFC5580, August 2009, <https://www.rfc-editor.org/info/rfc5580>.

[RFC6071] Frankel, S. and S. Krishnan, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap", RFC 6071, DOI 10.17487/RFC6071, February 2011, <https://www.rfc-editor.org/info/rfc6071>.

[RFC6614] Winter, S., McCauley, M., Venaas, S., and K. Wierenga, "Transport Layer Security (TLS) Encryption for RADIUS", RFC 6614, DOI 10.17487/RFC6614, May 2012, <https://www.rfc-editor.org/info/rfc6614>.

[RFC7585] Winter, S. and M. McCauley, "Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI)", RFC 7585, DOI 10.17487/RFC7585, October 2015, <https://www.rfc-editor.org/info/rfc7585>.

[RFC7593] Wierenga, K., Winter, S., and T. Wolniewicz, "The eduroam Architecture for Network Roaming", RFC 7593, DOI 10.17487/RFC7593, September 2015, <https://www.rfc-editor.org/info/rfc7593>.

[RFC8952] Larose, K., Dolson, D., and H. Liu, "Captive Portal Architecture", RFC 8952, DOI 10.17487/RFC8952, November 2020, <https://www.rfc-editor.org/info/rfc8952>.

[TS23003] 3GPP, "3GPP 23.003: Numbering, addressing and identification v18.1.0", 28 March 2023, <https://www.3gpp.org/ftp/Specs/archive/23_series/23.003/23003-i10.zip>.

[WBAVSA] Wireless Broadband Alliance, "Vendor Specific Attributes", n.d., <https://github.com/wireless-broadband-alliance/RADIUS-VSA>.

Appendix A. Example OpenRoaming Signalling Flow

An example signalling flow for OpenRoaming is illustrated in Figure 10.

1. In step 1, the WLAN is configured with Passpoint information and includes configured RCOIs in its beacon.

2. The beacon can only contain 3 RCOIs and so if none of the RCOIs match a profile provisioned in the device, the device queries for the list of RCOIs supported.

3. If the list includes an RCOI that matches a configured profile in the device, then device sends an EAPOL Start message to the authenticator.

4. The authenticator in the AP/WLC requests the EAP-Identity of the device.

5. The device responds with its EAP-Identity, which is a user@realm Network Access Identifier (NAI)

6. The NAS in the WLC/AP embeds the NAI in the user-name attribute in a RADIUS Access-Request message and forwards to the configured RadSec client.

7. The RadSec client recovers the realm from the NAI/user-name attribute and performs a DNS-based dynamic peer discovery.

8. The RadSec client established an mTLS authenticated TLS session with the discovered peer using certificates issued by the WBA PKI.

9. Once TLS is established, the RadSec client forwards the Access-Request to the RadSec server.

10. If the EAP Server is not co-located with the RadSec server, the RadSec server proxies the Access-Request to the EAP-Server.

11. The EAP-Server continues the EAP dialogue with the EAP Supplicant in the device using a Passpoint defined EAP method.

12. Following successful authentication, the EAP-Server responds with an Access-Accept packet containing the EAP-SUCCESS message and the keying material generated through the EAP method to secure the Wi-Fi session.

13. The Access-Accept packet is forwarded back to the RadSec client.

14. The RadSec client forwards the Access-Accept packet to the NAS in the AP/WLC.

15. The AP/WLC recovers the keying material from the Access-Accept packet and forwards the EAP-SUCCESS message to the device.

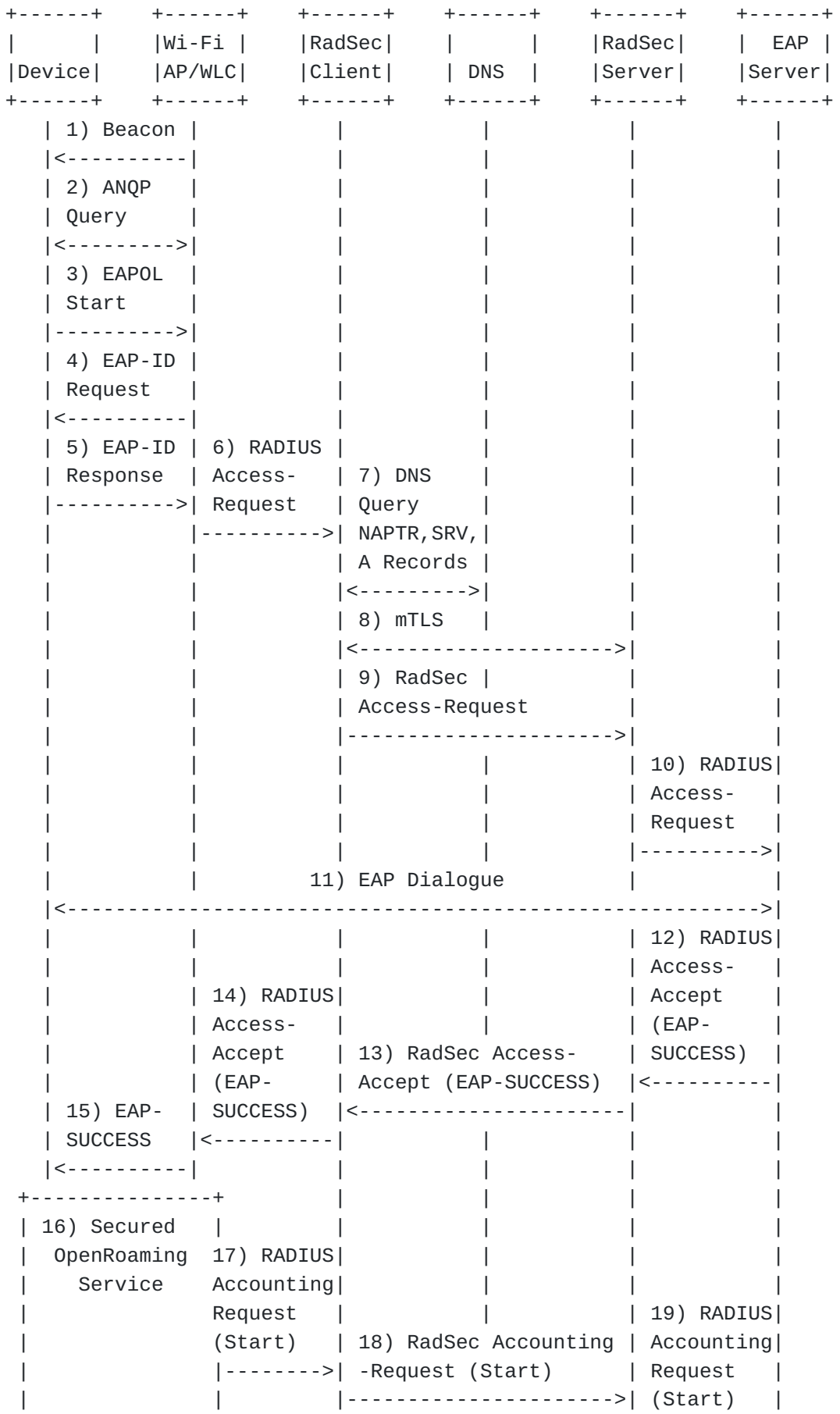
16. The keying material is used to secure the Wi-Fi interface between the device and AP/WLC.

17. The AP/WLC generates a RADIUS Accounting-Request message with Acct-Status-Type Start which is forwarded to the RadSec client.

18. The RadSec client forwards the Accounting-Request message over the TLS tunnel to the RadSec server.

19. The RadSec server can forward the Accounting-Request message to the EAP-Server.

20-22. After the Wi-Fi session terminates, an Accounting-Request message with Acct-Status-Type Stop is proxied towards the RadSec Server.


Device
Wi-Fi AP/WLC
RadSec Client
DNS
RadSec Server
EAP Server
1) Beacon
2) ANQP Query
3) EAPOL Start
4) EAP-ID Request
5) EAP-ID Response
6) RADIUS Access-Request
7) DNS Query NAPTR,SRV, A Records
8) mTLS
9) RadSec Access-Request
10) RADIUS Access-Request
11) EAP Dialogue
12) RADIUS Access-Accept (EAP-SUCCESS)
13) RadSec Access-Accept (EAP-SUCCESS)
14) RADIUS Access-Accept (EAP-SUCCESS)
15) EAP-SUCCESS
16) Secured OpenRoaming Service
17) RADIUS Accounting Request (Start)
18) RadSec Accounting -Request (Start)
19) RADIUS Accounting Request (Start)

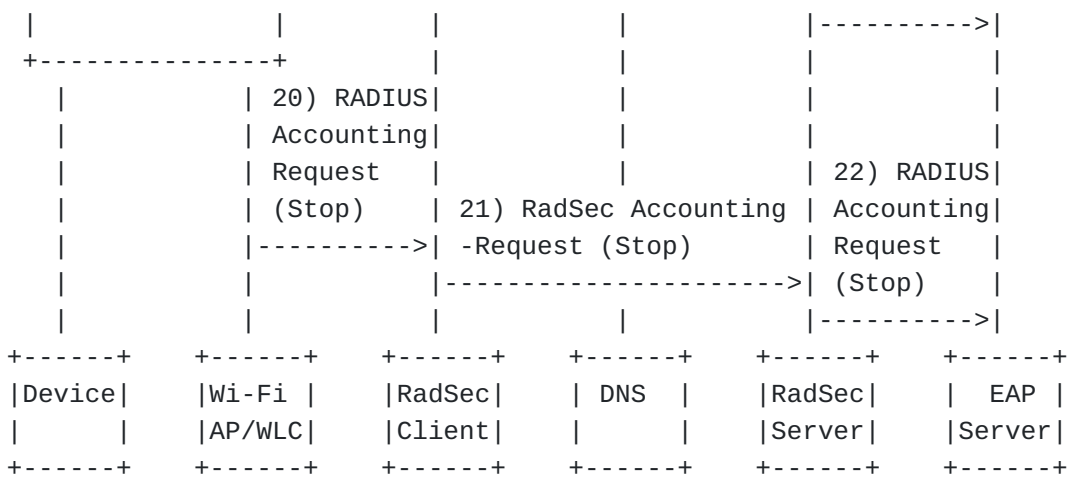


Figure 10: Example OpenRoaming Signalling Flow

Appendix B. Example OpenRoaming RCOI Usage

This Annex illustrates the use of OpenRoaming RCOIs to enforce different policies across the OpenRoaming federation, ensuring that when there is a policy mismatch between the device and access network, that the device will avoid triggering an authentication exchange that would subsequently have to be rejected because of a policy enforcement decision.

B.1. OpenRoaming RCOI based policy for supporting QoS tiers

Figure 11 illustrates the use of OpenRoaming RCOIs for supporting the standard (bronze) and silver QoS tiers across the federation. The figure shows two different devices:

- Device 1 has been provisioned by its IDP to require the basic bronze QoS policy.
- Device 2 has been provisioned by its IDP to require the silver tier of QoS handling.

The figure also shows illustrates the RCOI configuration of two ANP Access Networks:

- ANP#1 is configured to support the silver tier of QoS handling corresponding to the silver RCOI. Because the network requirements associated with the silver tier are a superset of the bronze QoS tier, the ANP also configures the bronze RCOI on its Wi-Fi access network.
- ANP#2 is only configured to support the standard (bronze) QoS tier and as such only configures the RCOI corresponding to the bronze QoS tier on its Wi-Fi access network.

The figure shows how normal Passpoint RCOI matching rules can be used to ensure that devices only trigger authentication with ANP access networks which support the required QoS tier according to the device's policy.

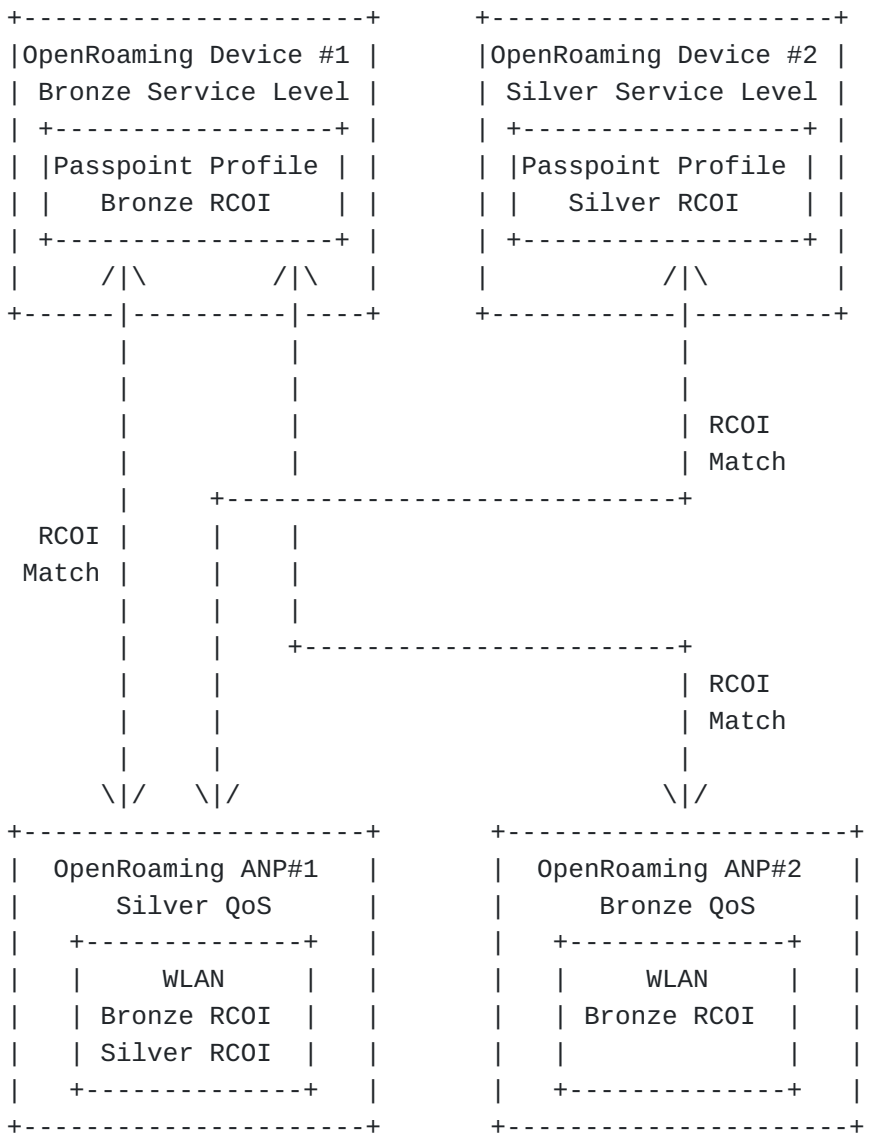


Figure 11: Use of OpenRoaming RCOIs to realize QoS policies

B.2. OpenRoaming RCOI based policy for supporting identity type policies

Figure 12 illustrates the use of OpenRoaming RCOIs for supporting different identity type policies across the federation. The figure shows two different devices:

- Device#1 has been provisioned by an IDP corresponding to a service provider. It provisions the device's Passpoint profile with the RCOI policy identifying the service provider ID-type policy as well as the "any ID-type" RCOI policy.

- Device 2 has been provisioned by a IDP corresponding to a hospitality provider. It provisions the device's Passpoint profile with the RCOI policy identifying the hospitality ID-type policy as well as the "any ID-type" RCOI policy.

The figure also shows the RCOI configuration of three different ANP Access Networks:

- ANP#1 only supports access using service provider type-IDs and so has configured the service provider ID-type policy RCOI.

- ANP#2 supports access from all identity types and so has configured the any ID-type policy RCOI.

- ANP#3 only supports access using hospitality type IDs and so has configured the hospitality ID-type policy RCOI.

The figure shows how normal Passpoint RCOI matching rules can be used to ensure that devices only trigger authentication with ANP access networks which support the required identity types according to the ANP's policy.

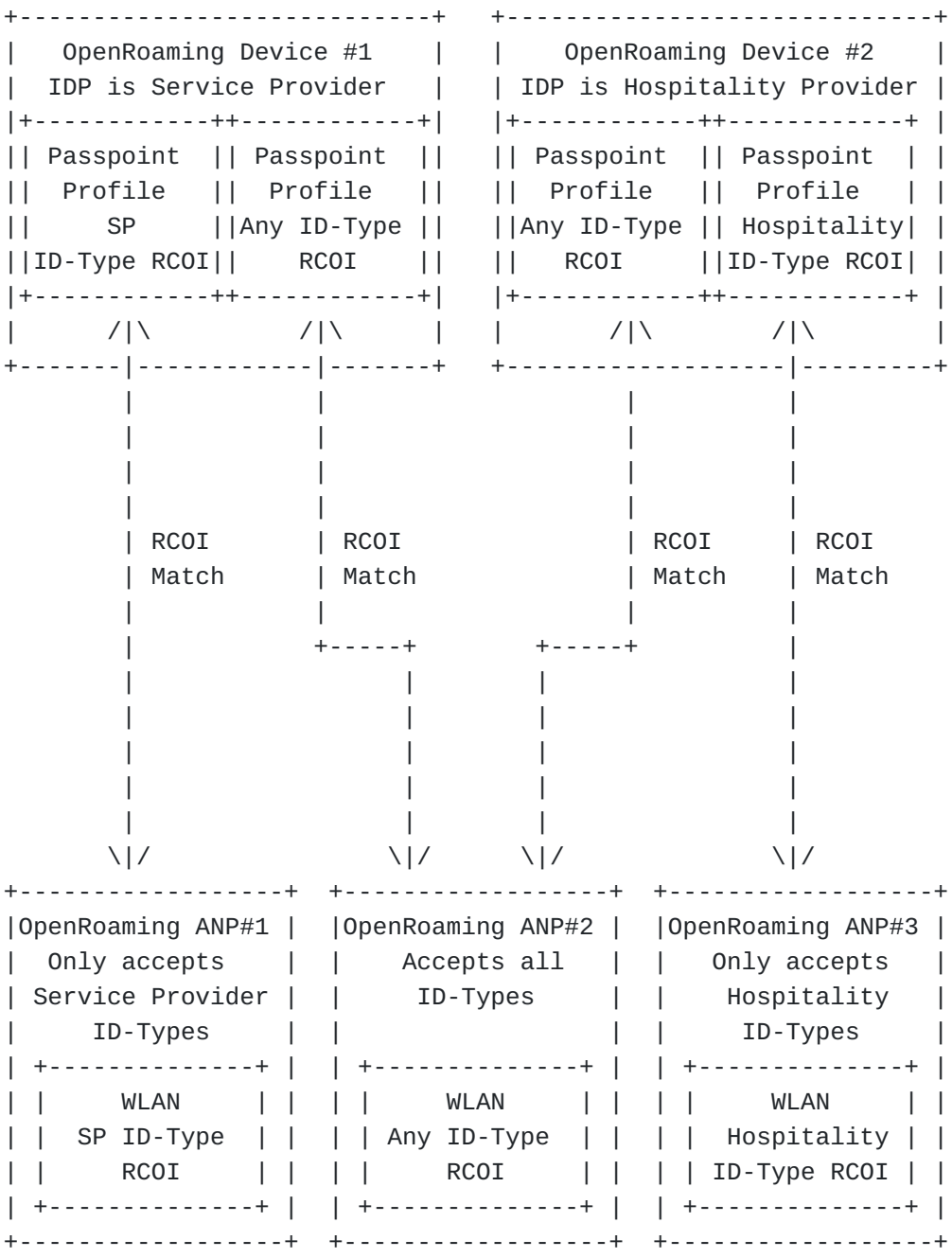


Figure 12: Use of OpenRoaming RCOIs to realize ID-Type policies

B.3. OpenRoaming RCOI based policy for supporting different identity proofing policies

Figure 13 illustrates the use of OpenRoaming RCOIs for supporting different identity proofing policies across the federation. The figure shows two different devices:

* Device 1 has been provisioned by an IDP that uses enhanced identity proofing controls that meet the enhanced OpenRoaming requirements, equivalent to LoA 3 in [ISO29115]. Because the enhanced identity proofing requirements are a superset of the requirements of the baseline identity proofing policy, the IDP also configures the use of the RCOI with baseline identity proofing.

* Device 2 has been provisioned by an IDP that uses identity proofing with controls that meet the baseline OpenRoaming requirements. It provisions the device's Passpoint profile with the RCOI policy identifying the baelien identity-proofing policy.

The figure also shows the RCOI configuration of two ANP Access Networks:

* ANP#1 is operated in a geography where regulations require support of enhanced identity proofing and so has configured its RCOI(s) with the enhanced identity-proofing policy.

* ANP#2 is operated in a geography where regulations permit support of authentications with identities managed using the OpenRoaming baseline identity proofing requirements and so has configured its RCOI(s) with the baseline identity-proofing policy.

The figure shows how normal Passpoint RCOI matching rules can be used to ensure that devices only trigger authentication with ANP access networks which support the required identity proofing according to the ANP's policy.

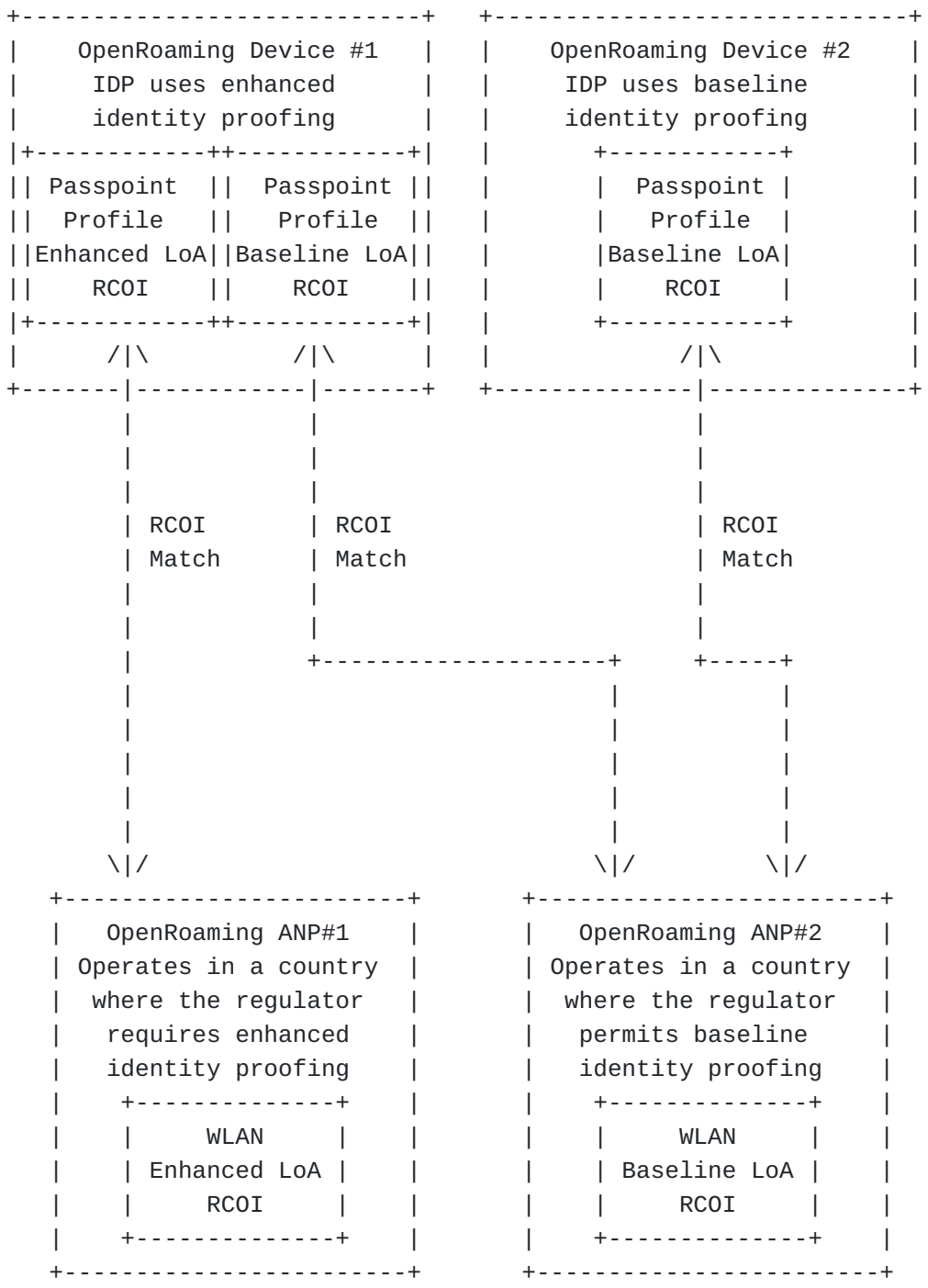


Figure 13: Use of OpenRoaming RCOIs to realize identity proofing policies

Appendix C. OpenRoaming legal framework

C.1. Seamless experience

In order for OpenRoaming to avoid the need for end-users to be presented with and accept legal terms and conditions covering their use of the Wi-Fi hotspot service, there needs to be a legal framework in place.

C.2. OpenRoaming Organization

The federation is based on a legal framework that comprises a set of policies, templated agreements and immutable terms as agreed to by the WBA and its membership. The framework defines a hierarchy of roles, responsibilities and relationships that are designed to enable the federation to scale to millions of Wi-Fi access networks.

Figure 14 shows the relationships between WBA, OpenRoaming Brokers, who are members of the WBA that have agreed terms with WBA to perform the OpenRoaming broker role and the OpenRoaming providers. OpenRoaming brokers agree terms with OpenRoaming Providers that can act as Access Network Providers (ANPs) and/or Identity Providers (IDPs). OpenRoaming providers do not have to be members of the WBA to provide OpenRoaming services. Finally, OpenRoaming IDPs agree terms with OpenRoaming end-users who then benefit from seamless authentication onto the Wi-Fi networks deployed by the different OpenRoaming ANPs.

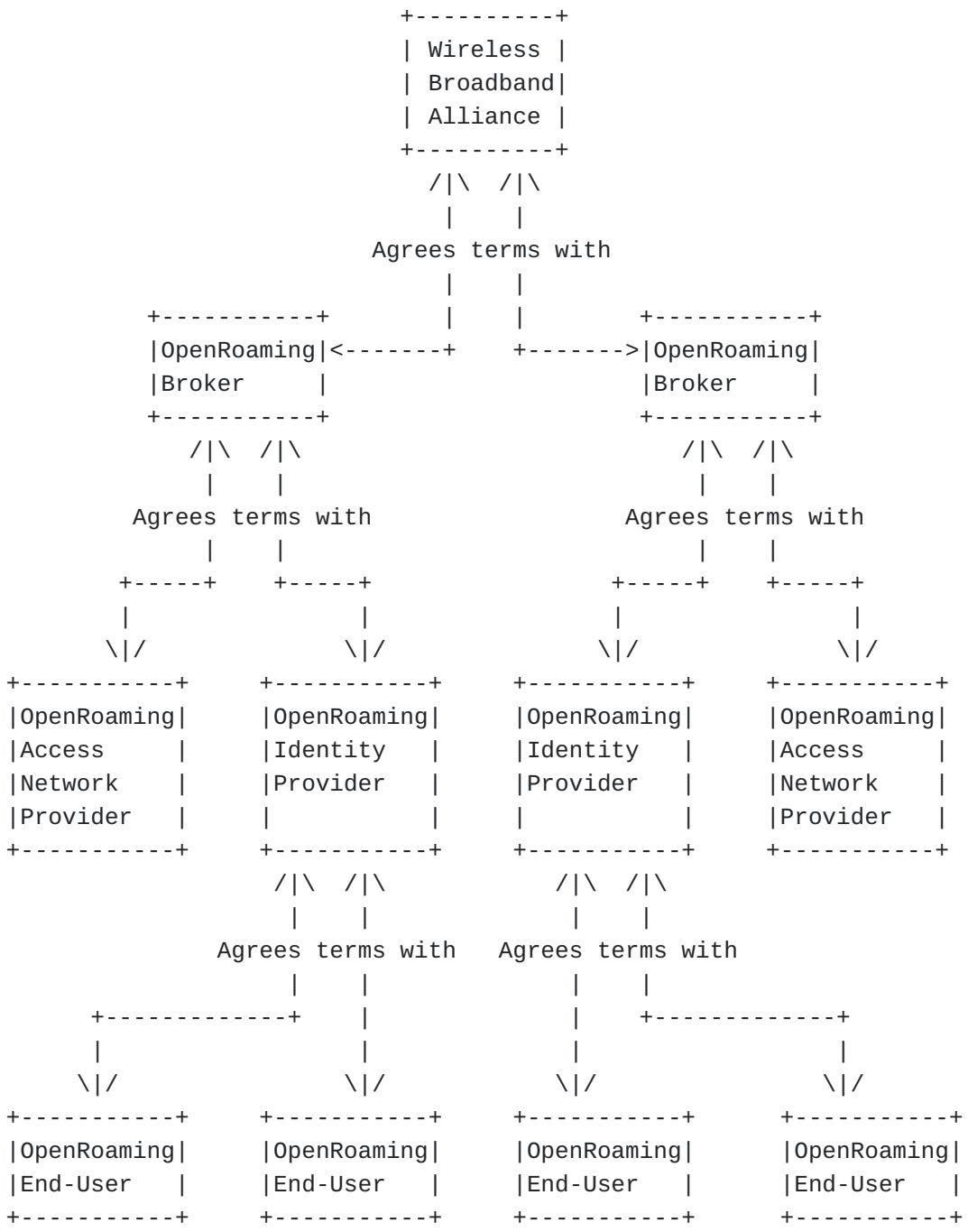


Figure 14: Organization of the OpenRoaming Federation

C.3. OpenRoaming legal terms

In OpenRoaming there is no direct agreement between individual ANPs and individual IDPs or between end-users and ANPs. As a consequence, OpenRoaming brokers agree to use certain federation-specific terms in their agreements with OpenRoaming providers.

This arrangement ensures that all ANPs agree to abide by the OpenRoaming privacy policy [ORPRIVACY] and all end-users agree to abide by the OpenRoaming end-user Terms and Conditions [ORTERMS].

Acknowledgements

The authors would like to thank all the members of the WBA's OpenRoaming Workgroup who help define the OpenRoaming specifications.

Authors' Addresses

Bruno Tomas
Wireless Broadband Alliance, Inc.
5000 Executive Parkway, Suite 302
San Ramon, 94583
United States of America

Email: bruno@wballiance.com

Mark Grayson
Cisco Systems
10 New Square Park
Feltham
TW14 8HA
United Kingdom

Email: mgrayson@cisco.com

Necati Canpolat
Intel Corporation
2111 NE. 25th Ave
Hillsboro, 97124
United States of America

Email: necati.canpolat@intel.com

Betty A. Cockrell
SingleDigits
San Antonio,
United States of America

Email: bcockrell@singledigits.com

Sri Gundavelli
Cisco Systems
170 West Tasman Drive
San Jose, 95134
United States of America

Email: sgundave@cisco.com