Independent Submission
Internet-Draft
Intended status: Informational
Expires: 27 July 2026

B. Tomas
Wireless Broadband Alliance, Inc.
M. Grayson
Cisco Systems
N. Canpolat
Intel Corporation
B. A. Cockrell
Independent
S. Gundavelli
Cisco Systems
23 January 2026

WBA OpenRoaming Wireless Federation
draft-tomas-openroaming-07

Abstract

This document describes the Wireless Broadband Alliance's OpenRoaming system. The OpenRoaming architecture 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.

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.

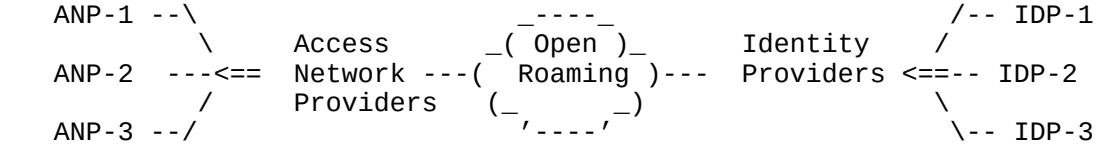


Figure 1: OpenRoaming Federation

WBA OpenRoaming recognizes the benefits that the likes of eduroam [RFC7593] provides to the education and research community. WBA OpenRoaming 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) on 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 (WBAIDs) 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, that enables Wi-Fi devices to automatically discover and authenticate to Wi-Fi hotspots that provide Internet access [PASSPOINT].

PLMN Id:

A unique identifier for a mobile network (cellular) operator. The identifier consists of a MCC (Mobile Country Code) and a MNC (Mobile Network Code). ITU-T Recommendation [E212] defines both MCC and MNC. The ITU allocates MCC values to national regulators who are then responsible for allocating MNC values to individual mobile network operators. [PASSPOINT] defines how the PLMN Id can be sent in ANQP messages.

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.

NOTE: OpenRoaming only uses 5-octet RCOIs.

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 (WRIX):

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, increasing concerns around sending Internet traffic over open, untrusted networks, together with the decreasing costs for cellular data, mean that 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 has typically been 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 on the access networks WLAN equipment enabling them to be sent in ANQP messages, 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 the 12 most significant bits of the 36-bit RCOI to embed closed access group policies.

4. Passpoint authentication that can use any suitable EAP method.

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

Example EAP methods used with Passpoint include EAP-TLS, EAP-SIM, EAP-AKA, EAP-AKA’ and EAP-TTLS with MS-CHAP-V2 that are included in Table 4 of the Passpoint specification [PASSPOINT]. In addition to these 5 EAP methods, Wi-Fi devices are available that can be configured to use different EAP type with Passpoint, including Passpoint with Protected EAP (PEAP) [PEAP], EAP-TEAP [RFC7170] and EAP-FAST [RFC4851] outer methods, together with alternative inner methods to MS-CHAP-V2 used inside EAP-TTLS, including EAP-TLS. Because OpenRoaming ANPs have no direct relationship with OpenRoaming IDPs that decide the credential type and EAP method to use when authenticating End-User devices, OpenRoaming ANPs SHOULD ensure that all EAP Methods compatible with Passpoint can be used to authenticate End-User devices.

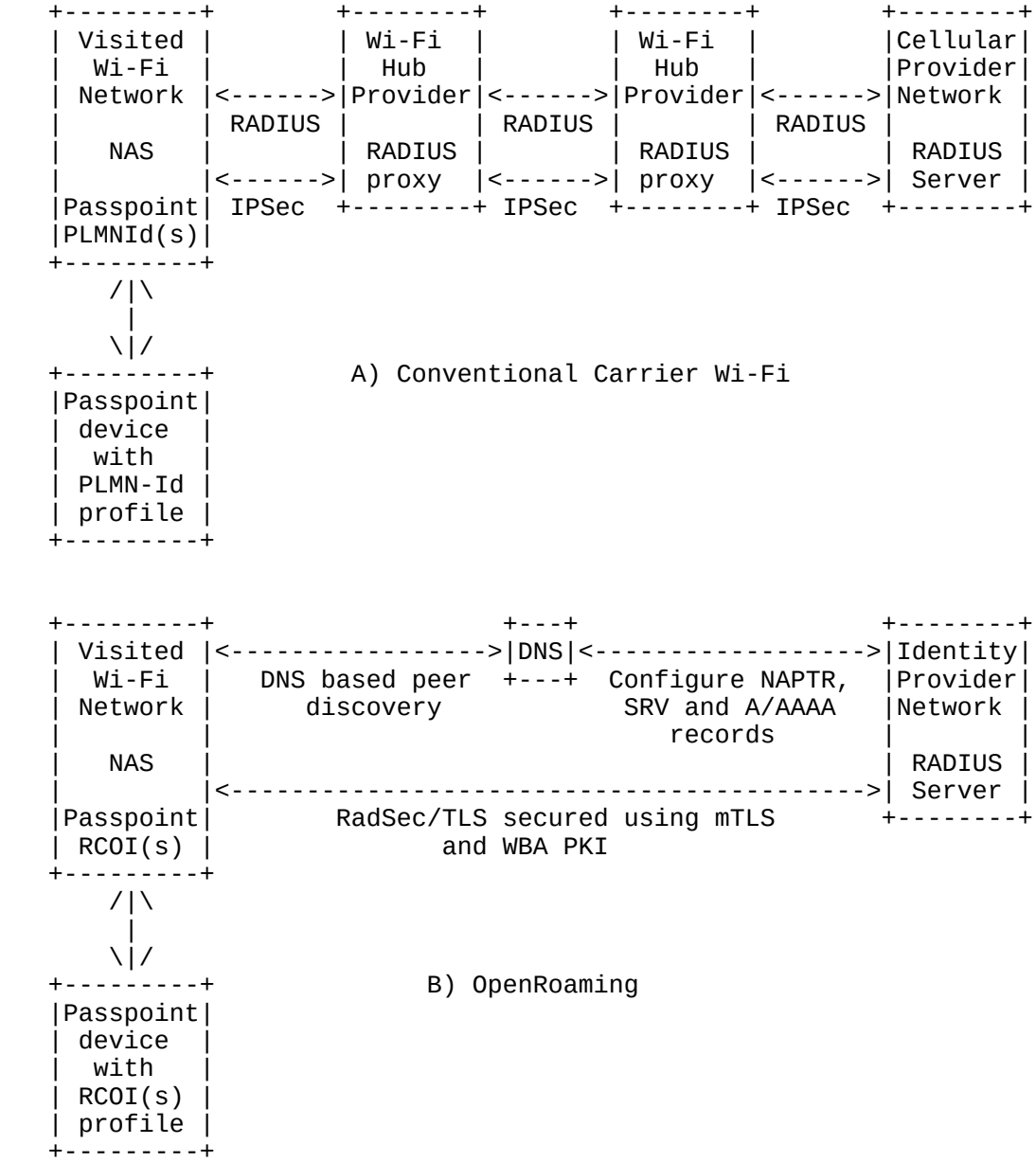


Figure 2: Contrasting Carrier Wi-Fi and OpenRoaming Architectures

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".

```
WBAID         = member-string [ ":" country-code ]

member-string = 1*( member-char )

member-char   = UPPERALPHA / DIGIT / SPECIAL

country-code  = 2UPPERALPHA

UPPERALPHA    = %x41-5A  ; "A"-"Z"
DIGIT         = %x30-39  ; "0"-"9"

; SPECIAL: permitted special characters
; excludes ":", ".", "_", "#", pound (%xA3), "*", '"'

SPECIAL       = %x21 / %x24-26 / %x28-29 / %x2B-2D /
                %x2F / %x3C-40 / %x5B-5E / %x7B-7E
```

Figure 3: ABNF definition of Primary WBAID Structure

When 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 a 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 [WBAPKICP] 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 1.3.6.1.4.1.14122.1.1.7.

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

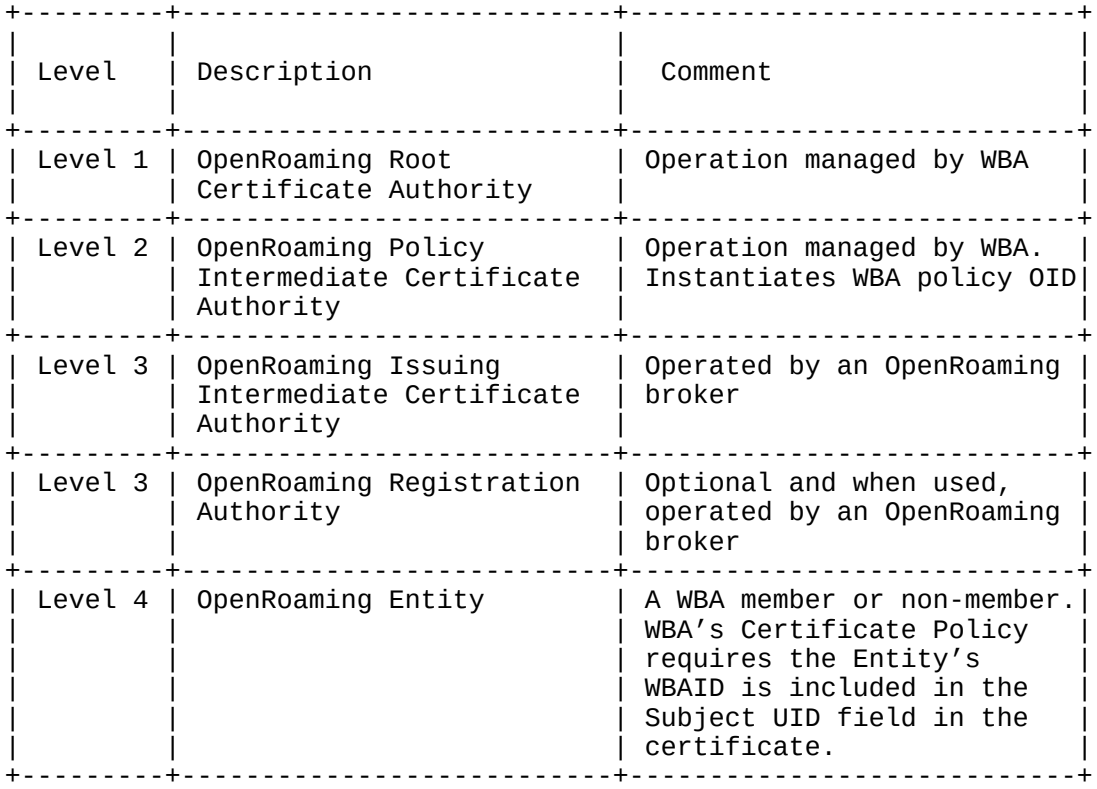


Figure 4: OpenRoaming PKI Hierarchy

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.

OpenRoaming is a distributed federation that lacks a centralized RADIUS element for identifying and troubleshooting signalling issues. Instead, the WBA operates cloud-based systems capable of verifying the correct configuration of DNS and TLS endpoints for OpenRoaming IDPs that have registered their realms with the WBA. This baseline testing by the WBA ensures that ANPs and IDPs can establish a TLS connection, such as when an end-user from an IDP roams into the coverage area of Wi-Fi networks operated by an ANP.

To provide a scalable system that enables access and identity providers to collaboratively troubleshoot and resolve issues, the WBA Certificate Practice Statement [WBAPKICPS] mandates that the Subject Alternative Name (SAN) attribute in issued end-entity certificates includes a contact email address responsible for handling issues raised by third-party providers. The OpenRoaming legal framework requires ANPs and IDPs to make reasonable efforts to support troubleshooting procedures. This includes monitoring the email address listed in the SAN attribute of the certificate and responding to any issues raised by legitimate third parties.

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/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 connected to 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 over the Internet 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 sub-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 mnc<mnc>.mcc<mcc>.pub.3gppnetwork.org sub-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 used with 3GPP's 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 discovered RadSec server is authoritative for a realm

The OpenRoaming preferred approach to dynamically discover the RadSec server IP address serving a particular realm or set of realms is to use DNS records that are protected with DNSSEC [RFC9364]. However, GSMA has not enabled DNSSEC on its 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 for a realm are not protected with DNSSEC, because the realm has been provided directly by the OpenRoaming End-User, 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) used in the dynamic peer detection in the certificate SubjectAltName.

Where the DNS records are 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 derived name(s) from the secured DNS NAPTR/SRV query in the certificate SubjectAltName.

Where the OpenRoaming IDP has offloaded the operation of RadSec termination to a third party hub-provider that is responsible for supporting a number of independent realms, the hub-provider SHOULD ensure that the discovered RadSec server(s) supporting the independent realms from its partner IDPs is/are configured with a WBA-PKI server certificate that includes the derived name(s) from the DNS NAPTR/SRV query in the certificate SubjectAltName.

6.4. Co-existence with other Federations

Other federations which want to interface to the OpenRoaming federation may use dynamic discovery with distinct NAPTR application service tags to facilitate integration. For example, an eduroam service provider can use the use the "x-eduroam" application service tag, specified in [RFC7593], to discover the home institution's RadSec peer for authentication, and OpenRoaming ANPs can use the "aaa+auth" tag to discover a separate RadSec peer that can be defined for handling all inter-domain authentications.

Where a separate inter-federation RadSec peer is not used, the other federation AAA operating as an OpenRoaming IDP needs to determine which certificate chain to return in its ServerHello message. An OpenRoaming ANP operating with TLS 1.3 SHOULD use the "certificate_authorities" extension [RFC8446] in its ClientHello message to indicate that the ANP supports the WBA PKI Certificate Authority trust anchor. Similarly, an OpenRoaming ANP operating using TLS 1.2 SHOULD use the "trusted_ca_keys" extension [RFC6066] in its ClientHello message to indicate the DistinguishedName of the WBA PKI Certificate Authority whose root keys the ANP possesses. The federation AAA operating as an OpenRoaming IDP MAY use information in the ClientHello extension to guide its certificate selection.

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 which end-users are authorized to access the service. The realization of authorization 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.

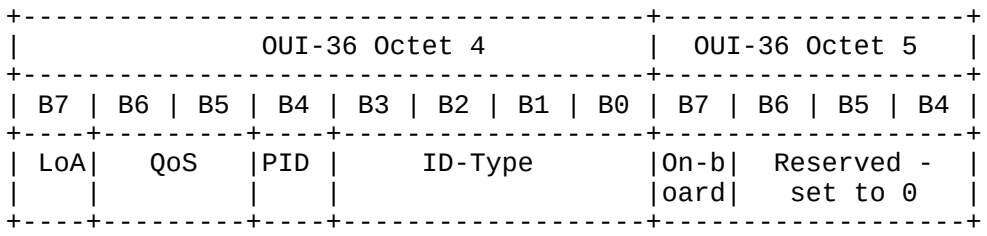


Figure 5: Extension of Octets 4 and 5 for OpenRoaming Context Dependent RCOI Field

7.2.1. Level of Assurance Policies

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

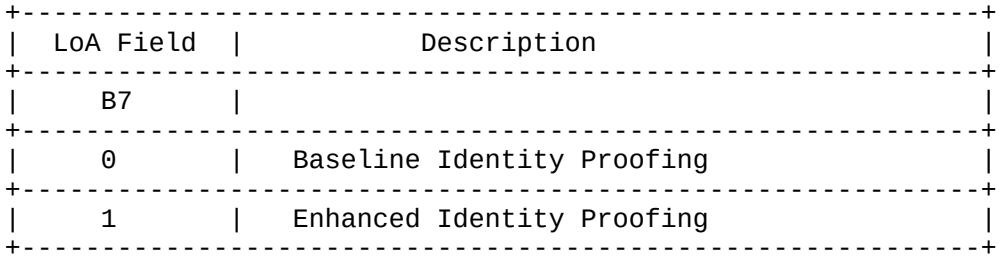


Figure 6: OpenRoaming CAG LoA Field

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

7.2.2.1. Access Network Requirements

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. This is especially the case where the Wi-Fi hotspot has been automatically selected with no user intervention. As a consequence, OpenRoaming defines specific service tiers across the federation and uses the QoS field to differentiate between different tiers. 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 ANP shall ensure that the maximum download speed that End Users can access the Internet shall be at least 50 megabits per second.

3. During the busy hour, 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 ANP shall ensure that the maximum download speed that End Users can access the Internet shall be at least 100 megabits per second.

3. During the busy hour, 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.

4. 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.

5. 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 configures 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".

Exceptionally, ANPs that operate OpenRoaming installations on moving platforms are permitted to deviate from normal OpenRoaming service level requirements. This is because such installations may necessitate use of cellular-based backhaul and/or backhaul via Non-Terrestrial Networks (NTN) which may not be able to meet the OpenRoaming minimum "bronze" service level requirements. If an ANP wants to benefit from such deviations, it MUST signal using the WLAN-Venue-Info attribute [RFC7268] that it is operating in a venue category identified using a Venue Group value of "10", which is defined in Section 8.4.1.34 of [IEEE80211] as being used for vehicular installations. In such cases, the OpenRoaming ANP MAY signal one or more WBA-Custom-SLA vendor specific attributes [WBAVSA] to indicate one or more (availability, per-user sustained bandwidth) tuples to the IDP.

7.2.2.2. Identity Provider Requirements

Irrespective of the service-levels supported by their users, the IDP shall ensure that the availability of their authentication service measured during scheduled operations shall exceed 99% over any one month period.

7.2.2.3. Rationale for busy hour sustained throughput values

The ANP requirements for sustained busy hour throughput requirements above are based on equating a notional per month consumption to a sustained busy hour throughput. The following calculation represents the mapping of sustained throughput to monthly consumption.

* Busy hour sustained throughput = 256 kilobits per second
* Busy hour consumption = 256 x 1024 x 3600 / 8 = 118 megabytes per hour
* Daily consumption, assuming 7% consumed in busy hour = 118 / 0.07 = 1.69 gigabytes
* Monthly consumption, assuming 22 busy days per month = 1.69 x 22 = 37.1 gigabytes/month

Comparing to a cellular usage, we need to use smartphone consumption figures that precludes Wi-Fi as well as broadband specific fixed wireless access subscriptions.

Using an example 10 gigabytes/month consumption per cellular subscription, it is evident that OpenRoaming bronze is dimensioned to accommodate 3.7 times the example cellular traffic, or 78% of total traffic when cellular and Wi-Fi are combined. Similarly, OpenRoaming silver is dimensioned to carry 88% of total traffic when cellular and Wi-Fi are combined.

7.2.3. Privacy Policies

The baseline privacy policy of OpenRoaming ensures the identities of end-users remain anonymous when using the service. The WBA WRIX specification specifies that where supplicants use EAP methods that support user-name privacy, i.e., which are compatible with the "@realm" (or "anonymous@realm") (outer) EAP-Identifier, then the supplicant SHOULD use the anonymized outer EAP identifier. Supplicants supporting other EAP methods SHOULD support EAP method specific techniques for masking the end-user’s permanent identifier, for example pseudonym support in EAP-AKA/AKA’ [RFC4187] and/or enhanced IMSI privacy protection [WBAEIPP]. OpenRoaming IDPs SHOULD

support and enable the corresponding server-side functionality to ensure end-user privacy is protected.

The WBA WRIX specification also recognizes that the privacy of end-users can be unintentionally weakened by the use of correlation identifiers signalled using the Chargeable-User-Identity attribute (#89) [RFC4372] and/or the Class attribute (#25) [RFC2865] in the RADIUS Access-Accept packet. The WBA WRIX Specification recommends that the default IDP policy SHOULD ensure that, when used, such correlation identifiers are unique for each combination of end-user/ANP and that the keys and/or initialization vectors used in creating such correlation identifiers SHOULD be refreshed at least every 48 hours, but not more frequently than every 2 hours.

This 2 hour limit is designed to assist the ANP in performing autonomous troubleshooting of connectivity issues from authentic users/devices that are repeatedly re-initiating connectivity to the ANP’s network and/or to assist the ANP in identifying a new session originated by an authentic user/device that has previously been identified by the ANP as having violated the OpenRoaming end-user terms and conditions. When using typical public Wi-Fi session durations, it is estimated that, with this 2 hour restriction, the ANP will be able to correlate an Access-Request/Access-Accept exchange that immediately follows an Accounting-Request stop message in over 50% of the sessions.

In contrast to this default policy, there can be scenarios where the ANP desires to derive value from its OpenRoaming settlement-free service by analysing aggregate end-user behaviour. Whereas the use of aggregated end-user information does not violate the OpenRoaming privacy policy, the derivation of such can benefit from the ANP being able to uniquely identify end-users. In order to support such scenarios, the OpenRoaming closed access group policies include the PID field.

The PID field can be used to support scenarios where the user has consented with their IDP that an immutable end-user identifier 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 MUST explicitly give their permission before an immutable end-user identity is 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	An immutable end-user ID will be returned by the IDP in the Access-Accept packet.

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(note 1)
1	0	1	1	A retail identity
other values				Reserved

NOTE 1: A manufacturer identity closed access group policy applies to IoT credentials corresponding to manufacturer installed identities as well as IoT credentials corresponding to owner installed identities.

Figure 9: OpenRoaming CAG ID-Type Field

7.2.5. On-boarding Credential Policies

The format of the on-boarding credential policy (On-board) field is as shown in Figure 10.

On-board Field	Description
B7 Octet 5	
0	A long-lived identity
1	A short-lived identity

Figure 10: OpenRoaming CAG On-board Field

The On-board field is used to identify closed access group policy aspects related to whether the identity/profile is long-lived, or whether the identity/profile is short-lived. Short-lived profiles are intended to only be used to provide connectivity such that the procedure for configuring a long-lived identity/profile can be performed.

Sessions authorized with short-lived credentials MUST have a session-timeout value of less than 300 seconds.

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 the WBA WRIX Specification which in turn are derived from [RFC3580] and [RFC3579]. All ANPs MUST support RADIUS Accounting for all OpenRoaming sessions, irrespective of which RCOIs are supported, i.e., for both settled and settlement free service. All IDPs MUST respond to any RADIUS Access-Request and Accounting-Request packet received.

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] and indicate such by including a CUI attribute in all RADIUS Access-Request packets. An ANP that has configured the OpenRoaming-Context PID Field set to "1" MAY treat a RADIUS Access-Accept received without a CUI attribute as an Access-Reject. An ANP that has configured the OpenRoaming-Context PID Field set to "0" MUST NOT treat any RADIUS Access-Accept received without a CUI attribute as an Access-Reject.

When an end-user has explicitly given their permission to share an immutable end-user identifier with third party ANPs, 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 the RADIUS Access-Request packet, where the location profile is the civic location profile that includes the country code where the ANP is located [RFC5580].

When the OpenRoaming ANP supports the OpenRoaming-Settled RCOI ("BA-A2-D0"), the RADIUS Access-Request packet MUST include the Location-Data attribute (#128) 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.

The OpenRoaming Privacy Policy [ORPRIVACY] restricts the use of all location information signalled to an IDP for either:

1. Making service authorization decisions based on the location of the ANP’s wireless network; or

2. Compliance with applicable law, or law enforcement requests.

8.4. Session-Timeout

An OpenRoaming ANP receiving a RADIUS Access Accept message including a Session-Timeout attribute MUST operate according to [RFC3580].

An IDP authenticating using a credential associated with a Passpoint profile with an RCOI where the On-board value is set to 1, as defined in Section 7.2.5, MUST set the session-timeout value to less than 300 seconds in the Access-Accept message.

8.5. Acct-Session-Id

All OpenRoaming enabled ANPs MUST support attribute Acct-Session-Id [RFC2866]. If an OpenRoaming IDP receives a RADIUS Access-Request message without an Acct-Session-Id, it should reject the Access-Request.

The Acct-Session-Id attribute SHOULD be temporally unique within an ANP’s access network.

An OpenRoaming IDP that receives an Accounting-Request message without either an Acct-Session-Id or an Acct-Multi-Session-Id corresponding to an authenticated RADIUS session SHOULD create a log of the message non-compliance, including the WBAID of the ANP.

8.6. Acct-Multi-Session-Id

All OpenRoaming enabled ANPs configured to generate multiple related accounting sessions for a single EAP-Supplicant roaming between Wi-Fi Access points MUST support attribute Acct-Multi-Session-Id [RFC2866].

The Acct-Multi-Session-Id attribute SHOULD be temporally unique within an ANP’s access network.

An OpenRoaming IDP that receives an Accounting-Request message without either an Acct-Session-Id or an Acct-Multi-Session-Id corresponding to an authenticated RADIUS session SHOULD create a log of the message non-compliance, including the WBAID of the ANP.

8.7. Event-Timestamp

All OpenRoaming ANPs MUST include the Event-Timestamp attribute [RFC2869] in all RADIUS Accounting-Request messages.

8.8. Enhanced Reply-Message

Reply-Message was originally defined in [RFC3579] as being forbidden from being included in any RADIUS message containing an EAP-Message attribute. This was to prevent earlier systems from attempting to interwork the Reply-Message text into an EAP Notification packet.

In contrast to using Reply-Message to signal a displayable text string to authenticating users, WBA's WRIX framework defines the re-use of the attribute in WRIX-based Passpoint networks to signal additional information from the IDP to the ANP, specifically regarding why a connection has been rejected. The message received MUST NOT be shown to end users.

The enhanced reply-message is encoded using UTF-8 characters. The WBA defines additional information is appended after the NUL ASCII character (0x00). The ABNF syntax of the Reply-Message is shown in Figure 11.

```
 Reply-message      = [ displayable-string ] %x00 [ wba-info ]
 displayable-string = *CHAR
 wba-info           =  "Reject-Reason=" cause-code

 cause-code =  "10" ; failed user authentication
 cause-code =/ "11" ; invalid user identity
 cause-code =/ "12" ; expired client certificate
 cause-code =/ "20" ; generic AAA failure
 cause-code =/ "21" ; backend failure
 cause-code =/ "22" ; protocol timeout
 cause-code =/ "30" ; failure due to badly formatted request
 cause-code =/ "31" ; rejected - missing charging model
 cause-code =/ "32" ; rejected - missing geospatial location
 cause-code =/ "40" ; failure due to subscription - permanent
 cause-code =/ "41" ; authorization rejected -
                    ; no service subscription
 cause-code =/ "42" ; authorization rejected -
                    ; roaming not allowed in this network
 cause-code =/ "43" ; authorization rejected -
                    ; offered charging model not acceptable
 cause-code =/ "44" ; authorization rejected -
                    ; roaming to this location not allowed
 cause-code =/ "45" ; authorization rejected -
                    ; offered service level not acceptable
 cause-code =/ "50" ; failure due to subscription -
                    ; temporary
 cause-code =/ "51" ; authorization rejected -
                    ; offered charging model not acceptable at this time
 cause-code =/ "52" ; authorization rejected -
                    ; roaming to this location not allowed at this time
 cause-code =/ "53" ; authorization rejected -
                    ; concurrency limits exceeded
 cause-code =/ "54" ; authorization rejected - insufficient credit
```

Figure 11: WBA Enhanced Reply-Message Syntax

8.9. 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.

8.10. 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].

8.11. WLAN-Venue-Info

The ANP MAY use the WLAN-Venue-Info attribute [RFC7268] to signal the category of venue hosting the WLAN.

8.12. WBA-Custom-SLA

When the ANP uses the WLAN-Venue-Info attribute to signal that the venue hosting the WLAN is a vehicular installation, the ANP MAY use the WBA-Custom-SLA vendor specific attribute [WBAVSA] to indicate one or more (availability, per-user sustained bandwidth) tuples to the IDP.

8.13. Additional attributes related to OpenRoaming settled

OpenRoaming settled defines the use of additional RADIUS attributes.

8.13.1. 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].

8.13.2. 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].

8.13.3. 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 packet.

8.13.4. OpenRoaming Session Mediation

OpenRoaming-Settled necessarily requires end-entities, which may include ANPs, IDPs and/or their respective hubs, to be able to perform session mediation between RADIUS Access-Request/Access-Accept and RADIUS Accounting-Request messages. This can be performed using RADIUS attributes Acct-Session-Id (#44) and Acct-Multi-Session-Id (#50) together with Operator-Name (#126).

To allow for possible non-uniqueness of Acct-Session-Id and/or Acct-Multi-Session-Id attributes between different Network Access Servers (NAS) within the same ANP, it is recommended to additionally use the attribute NAS-Identifier (#32) or NAS-IP-Address (#4) or NAS-IPv6-Address (#95) or Called-Station-Id (#30) in the matching process.

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 an 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 successive multiple failed authentications, the device’s supplicant SHOULD add the Access Point’s BSSID to a deny list to avoid future triggering of an authentication exchange with the unauthorized system.

9.2. ANP RadSec Connectivity

The ANP’s RadSec client connects to the IDP’s RadSec server over the public Internet. Recommended best practice for firewall deployment on public Internet facing interfaces SHOULD be followed. Firewall rules SHOULD permit outbound RadSec traffic (TCP destination port 2083) and allow return traffic for the same TCP connections while denying any TCP socket initiation from outside of the ANP’s network.

9.3. Dynamic Discovery of RadSec Peers

Whereas the dynamic discovery mechanisms specified in [RFC7585] permit the IDP to use their DNS SRV record to indicate a non-standard TCP port to be used in a RadSec connection, IDPs SHOULD recognize that ANP systems may only be configured to permit outbound connections on the standardized RadSec port of 2083.

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 MAY 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 store 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.

In order to prevent denial of service/brute force attacks, IDPs SHOULD implement intrusion prevention functionality that monitors systems to identify TLS mutual authentication failures and temporarily block source IP addresses that are the source of TLS authentication failures using firewall functionality.

9.4. 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 end-users are aware that the federation does not provide a secure end-to-end service. The end-user MUST NOT rely on the encryption delivered by OpenRoaming for providing security of services accessed using the ANP's Wi-Fi network.

9.5. ANP Inspection of End-User Traffic

All OpenRoaming ANPs MUST implement layer 2 traffic inspection and filtering, as specified in clause 5.1 of the [PASSPOINT] specification. ANPs MUST prohibit the delivery of any packet received from an OpenRoaming device directly to another OpenRoaming device.

All ANPs MUST use traffic inspection and filtering to help protect OpenRoaming users from malicious activity on the Internet as well as possible malicious activity by other authenticated OpenRoaming users. ANP traffic filtering function SHOULD NOT block ports associated with Wi-Fi calling, including UDP ports 500 and 4500 used by Internet Key Exchange (IKE), Internet Security Association and Key Management Protocol (ISAKMP) and IPSec [RFC7296]. Recommended best practice for firewall deployment on public Internet facing interfaces SHOULD be followed, including configuring the traffic inspection and filtering using information derived from reliable sources of threat intelligence.

9.6. End-User Location

The OpenRoaming legal framework (see Appendix C) ensures that the IDP has agreed to the OpenRoaming Privacy Policy [ORPRIVACY] to correctly handle the location-based personally identifiable information collected as part of providing the IDP service. Unless the IDP has agreed a separate privacy policy with the End-User, the IDP MUST only use location information signalled by an ANP for either:

1. Making service authorization decisions based on the location of the ANP’s wireless network; or

2. Compliance with applicable law, or law enforcement requests.

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/rfc/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/rfc/rfc8174>.

12.2. Informative References

[E212] ITU-T Study Group 2, "The international identification plan for public networks and subscriptions", June 2024, <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=E.212>.

[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>.

[IEEE80211] IEEE, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", n.d., <https://standards.ieee.org/ieee/802.11/5536/>.

[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>.

[PEAP] Microsoft Corporation, "Protected Extensible Authentication Protocol (PEAP)", April 2024, <https://winprotocoldocs-bhdugrdyduf5h2e4.b02.azurefd.net/MS-PEAP/%5bMS-PEAP%5d.pdf>.

[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/rfc/rfc2865>.

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, DOI 10.17487/RFC2866, June 2000, <https://www.rfc-editor.org/rfc/rfc2866>.

[RFC2869] Rigney, C., Willats, W., and P. Calhoun, "RADIUS Extensions", RFC 2869, DOI 10.17487/RFC2869, June 2000, <https://www.rfc-editor.org/rfc/rfc2869>.

[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/rfc/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/rfc/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/rfc/rfc3748>.

[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/rfc/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/rfc/rfc4372>.

[RFC4851] Cam-Winget, N., McGrew, D., Salowey, J., and H. Zhou, "The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST)", RFC 4851, DOI 10.17487/RFC4851, May 2007, <https://www.rfc-editor.org/rfc/rfc4851>.

[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/rfc/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/rfc/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/rfc/rfc5580>.

[RFC6066] Eastlake 3rd, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, DOI 10.17487/RFC6066, January 2011, <https://www.rfc-editor.org/rfc/rfc6066>.

[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/rfc/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/rfc/rfc6614>.

[RFC7170] Zhou, H., Cam-Winget, N., Salowey, J., and S. Hanna, "Tunnel Extensible Authentication Protocol (TEAP) Version 1", RFC 7170, DOI 10.17487/RFC7170, May 2014, <https://www.rfc-editor.org/rfc/rfc7170>.

[RFC7268] Aboba, B., Malinen, J., Congdon, P., Salowey, J., and M. Jones, "RADIUS Attributes for IEEE 802 Networks", RFC 7268, DOI 10.17487/RFC7268, July 2014, <https://www.rfc-editor.org/rfc/rfc7268>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/rfc/rfc7296>.

[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/rfc/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/rfc/rfc7593>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

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

[RFC9364] Hoffman, P., "DNS Security Extensions (DNSSEC)", BCP 237, RFC 9364, DOI 10.17487/RFC9364, February 2023, <https://www.rfc-editor.org/rfc/rfc9364>.

[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>.

[WBAEIPP] Wireless Broadband Alliance, "WBA Enhanced IMSI Privacy Protection", August 2022, <https://wballiancec.wpenginepowered.com/wp-content/uploads/2021/02/IMSI_Privacy_Protection_for_Wi-Fi_Technical_Specification_v1.1.0_Revision_FINAL.pdf>.

[WBAPKICP] Wireless Broadband Alliance, "WBA PKI Certificate Policy v4.0.0", April 2024, <https://wballiance.com/openroaming/pki-repository/>.

[WBAPKICPS] Wireless Broadband Alliance, "WBA PKI Certificate Practise Statement v1.0.0", September 2025, <https://wballiance.com/openroaming/pki-repository/>.

[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 12.

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 packet 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.

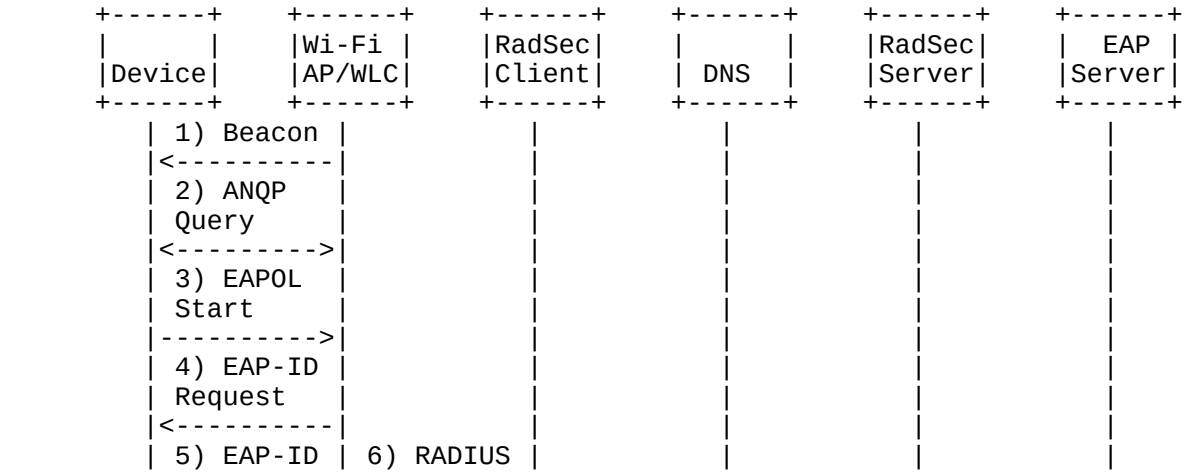
16. The keying material is used to secure the Wi-Fi interface between the device and AP/WLC.

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

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

19. The RadSec server can forward the Accounting-Request packet 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.



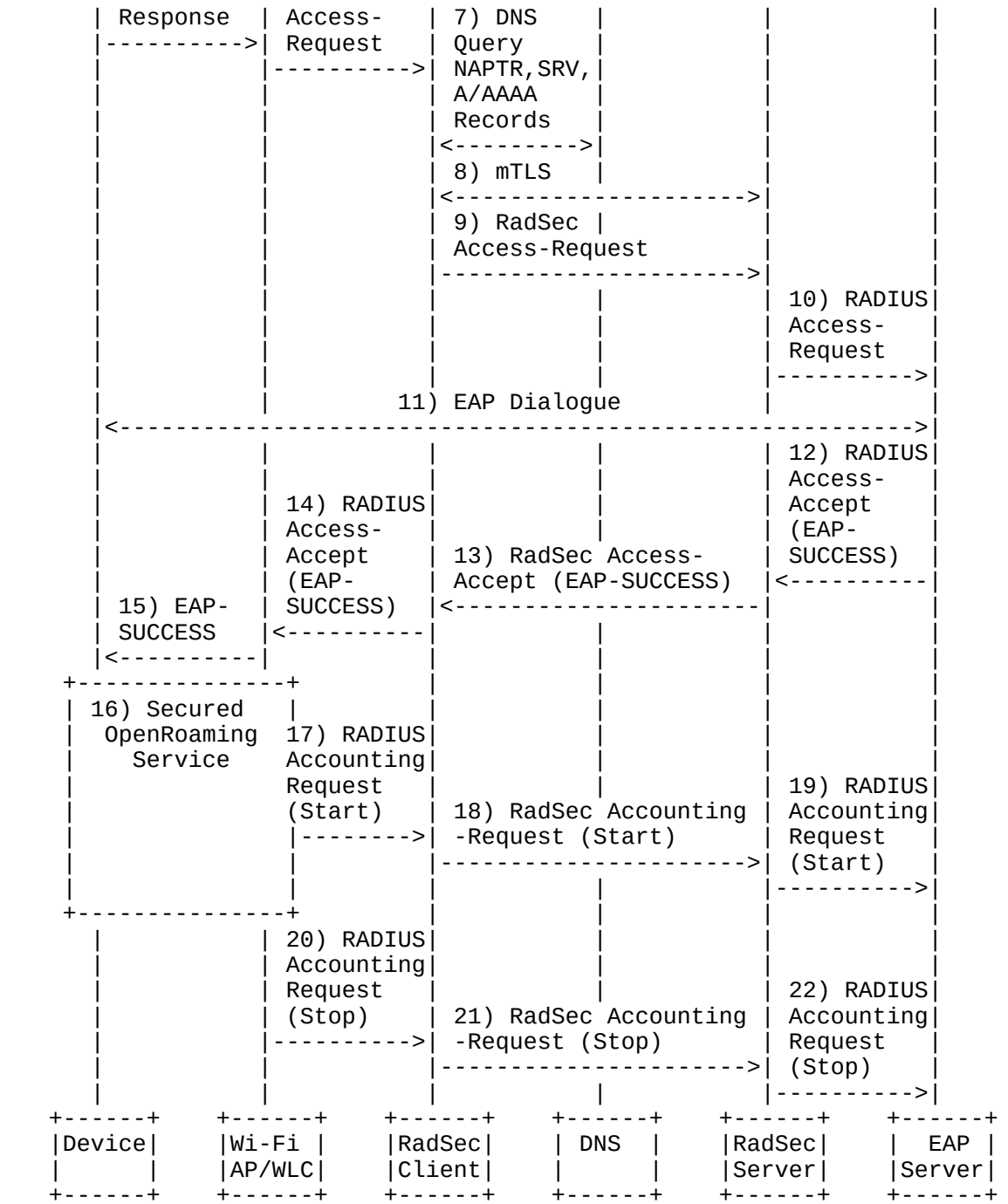

Response
Access-Request
7) DNS Query NAPTR,SRV, A/AAAA Records
8) mTLS
9) RadSec Access-Request
10) RADIUS Access-Request
11) EAP Dialogue
12) RADIUS Access-Accept (EAP-SUCCESS)
13) RadSec Access-Accept (EAP-SUCCESS)
14) RADIUS Access-Accept (EAP-SUCCESS)
15) EAP-SUCCESS
16) Secured OpenRoaming Service
17) RADIUS Accounting Request (Start)
18) RadSec Accounting -Request (Start)
19) RADIUS Accounting Request (Start)
20) RADIUS Accounting Request (Stop)
21) RadSec Accounting -Request (Stop)
22) RADIUS Accounting Request (Stop)
Device
Wi-Fi AP/WLC
RadSec Client
DNS
RadSec Server
EAP Server

Figure 12: Example OpenRoaming Signalling Flow

Appendix B. Example OpenRoaming RCOI Usage

This Annex illustrates the use of OpenRoaming RCOIs to enforce different policies in 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 policy enforcement decisions.

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

Figure 13 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.

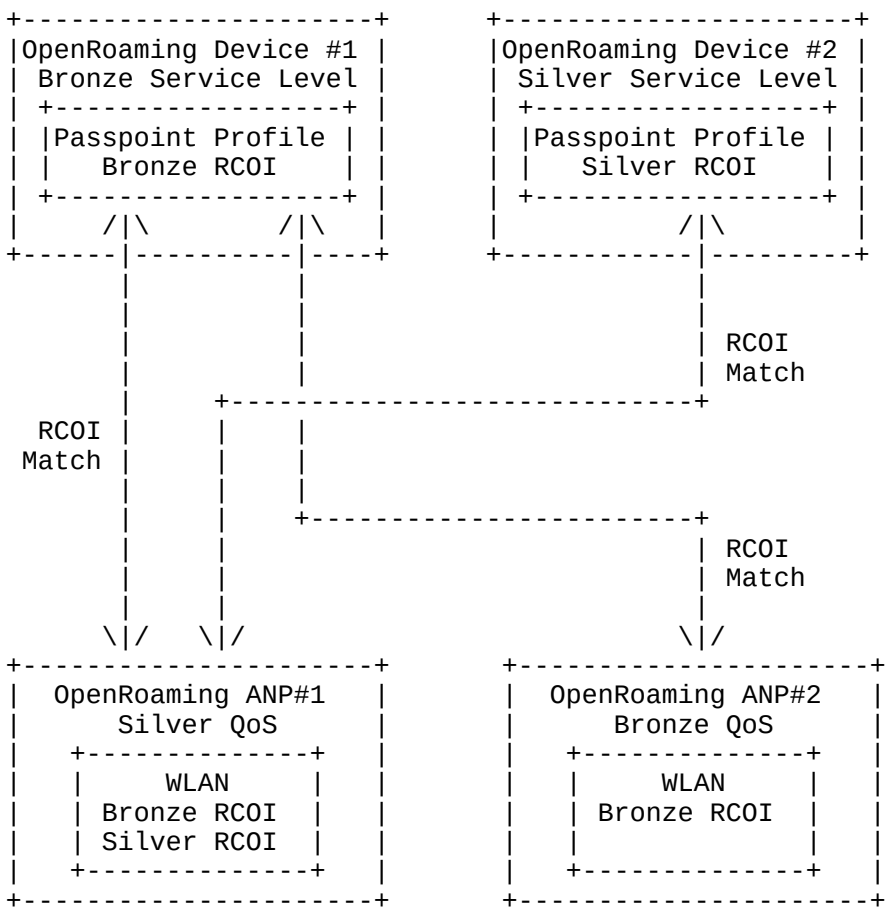


Figure 13: Use of OpenRoaming RCOIs to realize QoS policies

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

Figure 14 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.

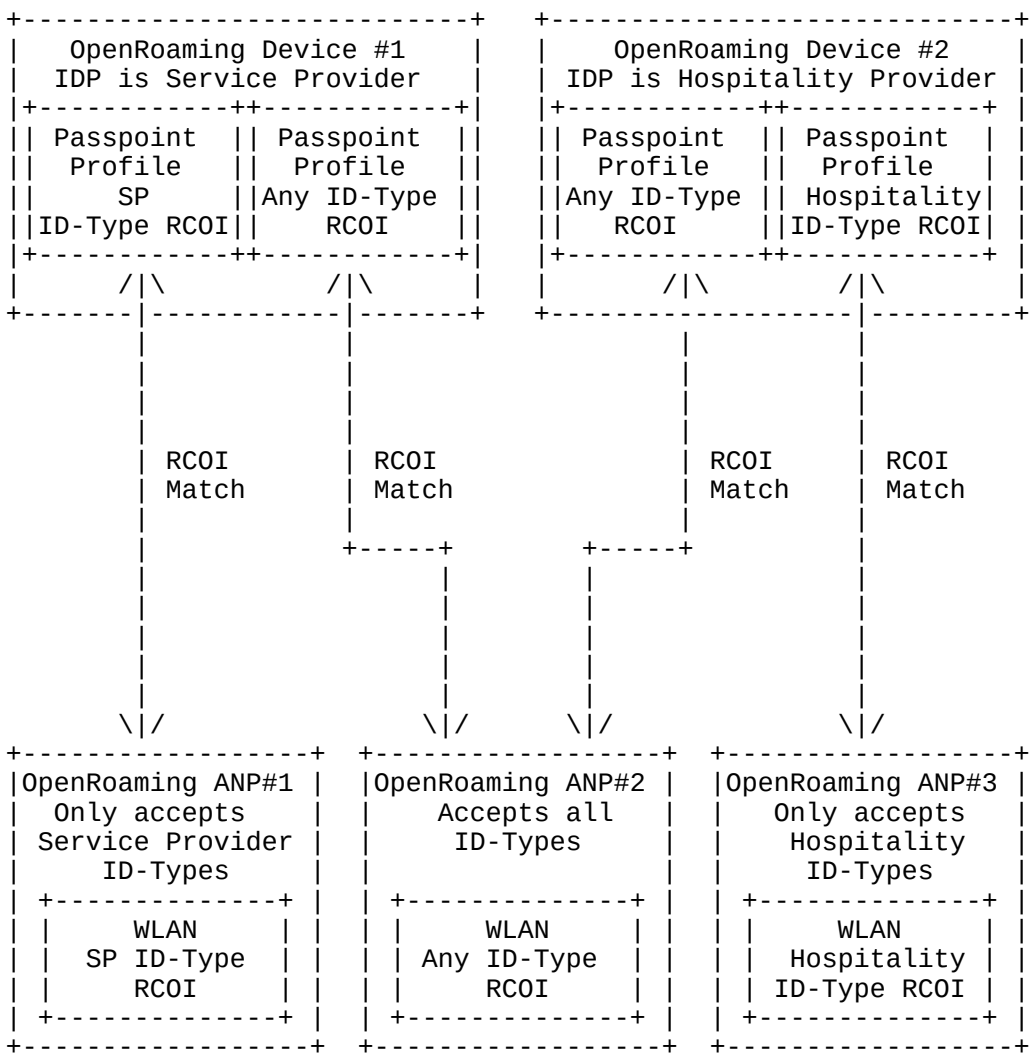


Figure 14: Use of OpenRoaming RCOIs to realize ID-Type policies

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

Figure 15 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.

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.

* ANP#2 is operated in a geography where regulations permit support of authentications with identities managed using the OpenRoaming baseline identity proofing requirements.

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.

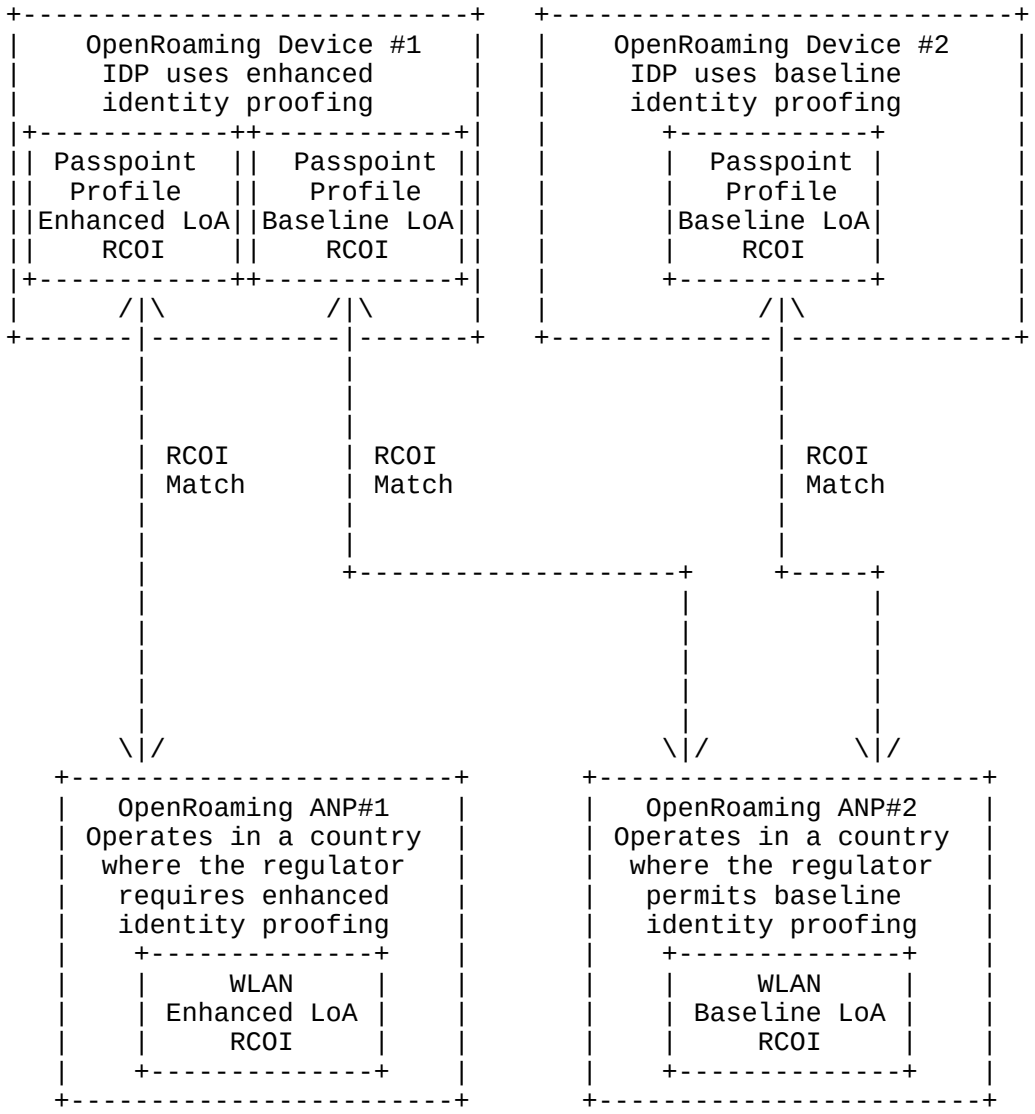


Figure 15: Use of OpenRoaming RCOIs to realize identity proofing policies

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 16 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.

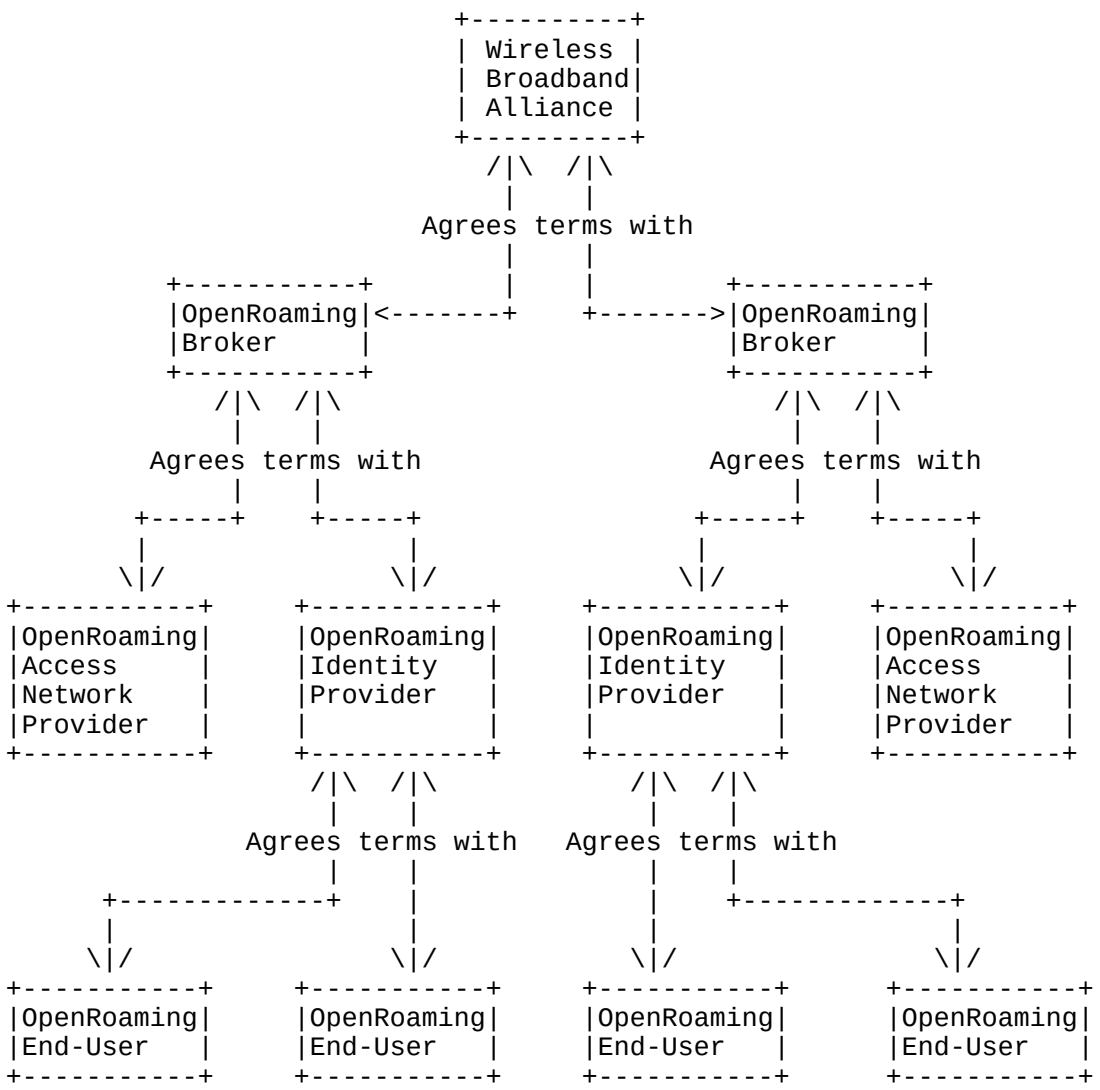


Figure 16: Organization of the OpenRoaming Federation

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].

If an ANP detects service abuse by an end-user in contravention of the end-user Terms and Conditions, the ANP SHOULD record logs relevant to the abuse and use the email address embedded in the Subject Alternative Name (SAN) attribute in IDP's issued end-entity certificate to contact the abuser's IDP, indicating the nature of the abuse together with any relevant logs. The immutable terms of OpenRoaming require IDPs to make reasonable efforts to address the service abuse experienced by the ANP, which may include the withdrawal of the OpenRoaming service from the identified abusive end-user.

Changelog

* 01 - added details of WBA-Custom-SLA for OpenRoaming ANP networks that signal using [RFC7268] that they operate on a vehicular platform. Added clarifications regarding use of direct and indirect names in certificate validation.

* 02 - added details of OpenRoaming protection of end-user privacy, including WRIX recommendations on use of correlation identifiers in RADIUS Access-Accept packet that may unintentionally weaken end-user privacy.

* 03 - updated DNSsec reference. Added section on interworking with other federations.

* 04 - updated PKI Policy OID to reflect new certificate chain. Added IDP availability requirements. Added session-timeout requirements. Added new onboarding capabilities for short lived credentials. Added text concerning OpenRoaming Privacy Policy and restrictions on location usage.

* 05 - added new section on use of Reply-Message, added new text on troubleshooting, clarified RADIUS accounting handling, clarified CUI usage in Access-Accept, clarified use of EAP types.

* 06 - corrected ePDG FQDN. Added missing enhanced Reply-Message for cause-code = 45. Added new text regarding recommended best practice for firewall deployment on public Internet facing interfaces should be followed for ANP RADSEC connections and for protecting End-Users.

* 07 - added details of service abuse handling. Added further details of RADIUS attributes. Added rationale for busy hour sustained throughput values. Introduced requirements on minimum speeds for OpenRoaming bronze and silver tiers. Corrected WBAID ABNF by adding in permitted special characters.

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
Independent
San Antonio,
United States of America
Email: bcbeti@outlook.com

Sri Gundavelli
Cisco Systems
170 West Tasman Drive
San Jose, 95134
United States of America
Email: sgundave@cisco.com