RADEXT Working Group
Internet-Draft
Intended status: Standards Track
Expires: 22 January 2026

S. Gundavelli
Cisco Systems
S. Das
Peraton Labs
M. Grayson
Cisco Systems
M. Dolly
AT&T
A. Nguyen
US DHS/CISA
21 July 2025

RADIUS attributes for National Security and Emergency Preparedness Service
draft-gundavelli-radepcs-01

Abstract

This document describes RADIUS attributes for supporting authorization of Emergency Preparedness Communication Service (EPCS), enabling authorized users to benefit from preferential access to Wi-Fi network resources during congestion.

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 22 January 2026.

Copyright Notice

Table of Contents

1. Introduction

Priority Services (PS) communications in support of National Security/Emergency Preparedness (NS/EP) services are operational in various countries around the world. While these have traditionally only been supported over cellular networks [TS.22153], the recent addition of Emergency Preparedness Communications Service (EPCS) functionality into Wi-Fi 7 [IEEE80211BE] means that Wi-Fi now supports preferred or prioritized channel access (PCA) to authorized users that can be used for Multimedia Priority Services (MPS) communications over public/private Wi-Fi networks in emergency service (ES) scenarios.

Whereas Wi-Fi 7 defines the interactions between the Wi-Fi Access Point (AP) and the Wi-Fi Station (STA) device for prioritized channel access, it does not provide an end-to-end architecture for enabling EPCS authorization capability on a per device basis.

CISRCVIII WG4 recommendations for FCC highlight the opportunities for regulatory bodies, like the FCC, to assess and promote Wi-Fi's role in emergency services [CSRC8-WG4].

Earlier deliverables from CISRCV WG8 have provided recommendations for the role of the network within the priority services platform and to enforce priority levels on traffic associated with priority users [CSRC5-WG8]. There are number of factors critical to this enforcement function:

* The priority user must be authenticated and authorized to receive priority treatment.

* The network must be able to uniquely identify priority user traffic and associate the authorized level of priority to that traffic.

* The network must then have the means to apply prioritization to the identified traffic.

* For cases where networks interconnect, traffic prioritization indicators must be securely passed to interconnected networks for downstream prioritization.

This document specifies an extension to the Remote Authentication Dial-In User Service (RADIUS) protocol [RFC2865] that enables a Wi-Fi Network Access Server (NAS) to indicate to a RADIUS server that it is EPCS capable, as well as enabling a RADIUS server to indicate to a NAS that an authenticated user is authorized to receive the EPCS service.

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

Authorizing Entity:

Refers to the Authority (e.g., Government entity) responsible for vetting and assigning priority privileges and user priority levels to an individual or organization.

Priority Services:

A feature designed to enable NS (National Security) or EP (Emergency Preparedness) subscribers to make priority calls or data sessions on a Service Providers network, particularly at times of congestion.

Service user:

Means an individual or organization to whom or which a priority access assignment has been made.

Wireless service provider:

Refers to a provider of a wireless communications service or Internet Protocol-based service, including commercial or private mobile service. The term includes agents of the licensed provider and resellers of wireless service.

2. Overview of EPCS Provisioning

This section first provides background on how MPS service is currently provisioned and authorized. The section then describes how this can be adapted for EPCS to support Wi-Fi use cases.

The service user engages with an authorizing entity to request the provision of Multimedia Priority Service for a device that has a subscription with a service provider. If the request is successful, the service provider, such as a cellular operator, will receive an indication from the authorizing entity, by an out of band mechanism, that a subscriber has been authorized for priority services. The service provider will store such an indication as part of the subscription profile of the subscriber (e.g., in the cellular network defined Home Subscriber Server (HSS)).

Figure 1 illustrates the scenario where the service provider is a cellular operator that is also operating as a Wi-Fi Identity Provider, e.g., using SIM card credentials to authenticate users onto third-party Wi-Fi networks. In such cases, the cellular operator can mirror the priority service subscription profile information in their Wi-Fi Authentication, Authorization and Accounting (AAA) system.

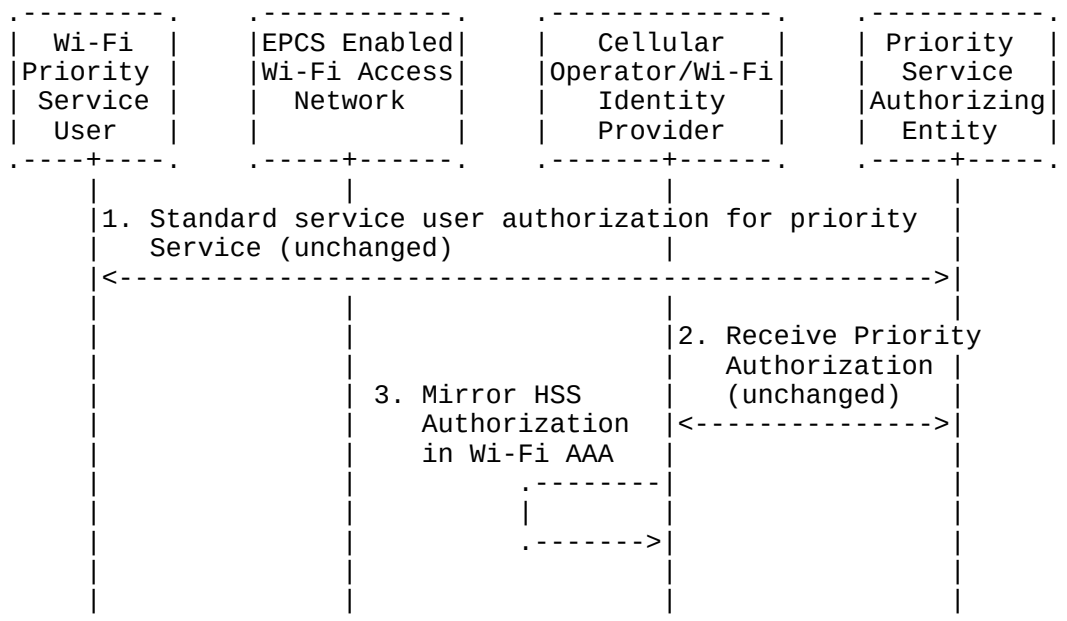


Figure 1: Provisioning Priority Services over Wi-Fi Networks

3. EPCS Authorization RADIUS Exchange

The top level RADIUS Authorization flow for an EPCS Service User is illustrated in Figure 2.

1. In step 1, the EPCS enabled Wi-Fi Access Network provider configures the defined EPCS Roaming Consortium on its Wi-Fi access network.

2. In step 2, the Wi-Fi Priority Service User enables an EPCS Passpoint profile on their device. This enables normal Passpoint automatic network selection.

3. In step 3, the Wi-Fi Priority Service User’s device matches the EPCS Roaming Consortium in the Wi-Fi beacon, probe response or Access Network Query Protocol (ANQP) response with the Roaming Consortium Organizational Indicator (RCOI) included in its Passpoint profile.

4. In steps 4 and 5, the Wi-Fi device triggers an association with the Wi-Fi Access Point/Wireless LAN Controller (AP/WLC). The device includes the EPCS Passpoint RCOI in the Roaming Consortium Selection element [PASSPOINT] and receives an association response.

5. In steps 6 and 7, the AP/WLC performs the Extensible Authentication Protocol (EAP) exchange over the LAN using EAPOL frames exchanged with the device, requesting the device's EAP identity and receives the corresponding identity associated with the EPCS Passpoint profile in the EAP response.

6. In step 8, the AP/WLC extracts the EAP identity and includes this in a RADIUS Access-Request that is sent to the Identity Provider. In this example, the identity realm corresponds to a Cellular operator as defined in [TS.23003], e.g., wlan.mnc100.mcc313.3gppnetwork.org. The AP/WLC adds the Civic-Location attribute [RFC5580] to the RADIUS Access-Request, indicating the country code and optional subdivision (using CAType 1) that identify the regulatory regime in which it is operating, the HS2.0-Roaming-Consortium attribute [PASSPOINT] indicating the EPCS Passpoint RCOI signaled by the device in step 4, and the EPCS-Capable-Indication attribute, as specified in Section 4.1. If the Wi-Fi AP/WLC is expecting to receive payment for handling the priority service traffic, the AP/WLC can include additional attributes related to charging, for example the offered WBA-Linear-Volume-Rate [WBAVSAS].

7. In step 9. the EAP dialogue completes between the supplicant in the Wi-Fi device and the Cellular Operator's EAP server.

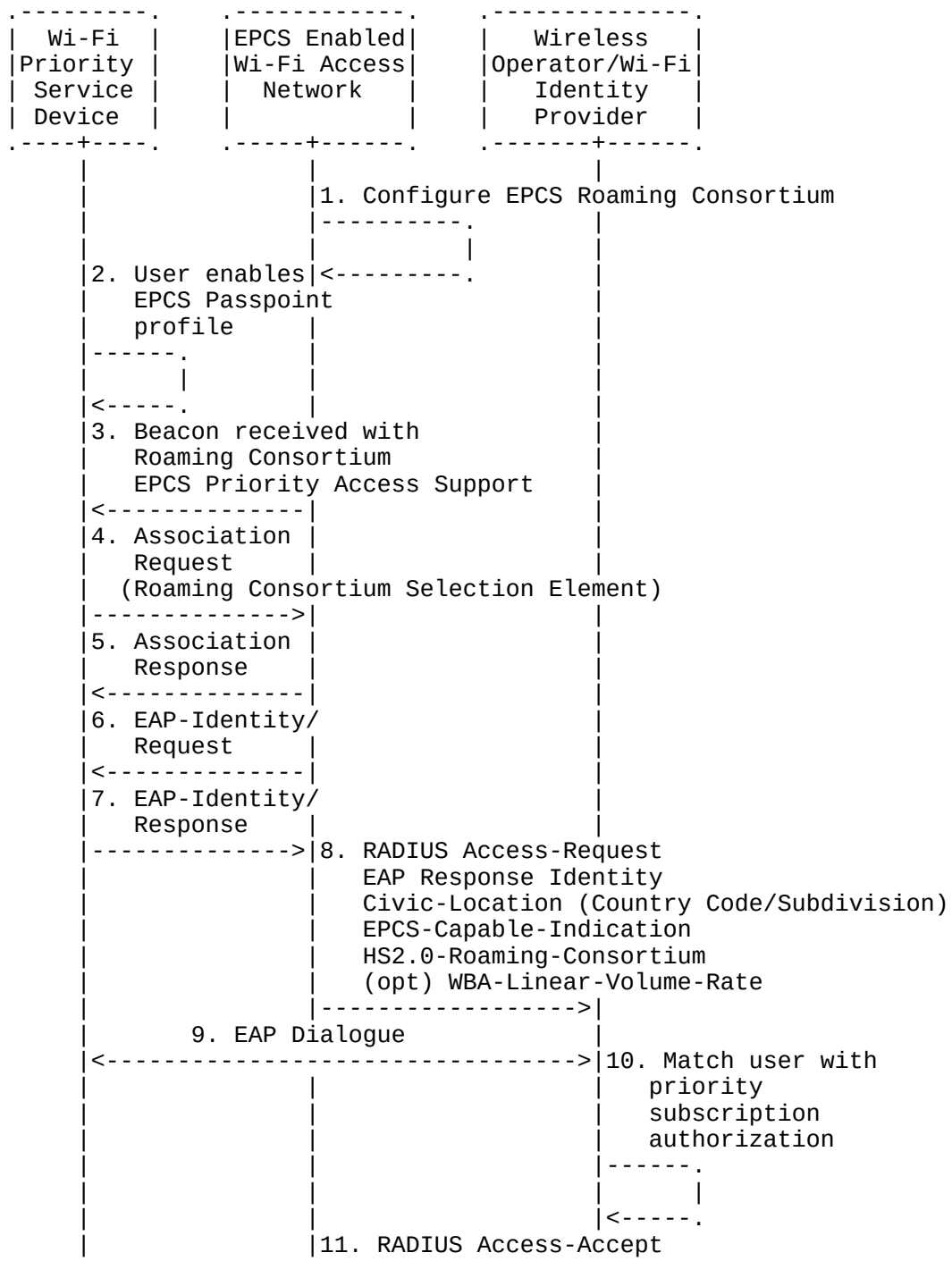
8. In step 10, the authenticated device is matched against the priority subscription profile. The provider MAY use the country code signalled in step 6 and compare that with the regulatory regimes in which priority service is authorized.

9. In step 11, assuming the user is authorized, the cellular operator replies with a RADIUS Access-Accept including the EAP-SUCCESS message and the EPCS-Subscription-Info attribute defined in Section 4.3.

10. In step 12, the AP/WLC recovers the keying material from the Access-Accept packet and forwards the EAP-SUCCESS message to the device.

11. In step 13 and 14, the AP/WLC enables EPCS priority access by sending the EPCS Priority Access Enable Request frame to the device. The device (i.e., STA) responds with an EPCS Priority Access Enable Response frame in step 14. (Note: These steps assume the AP/WLC is configured or triggered to automatically enable EPCS for the device.)

12. In step 15, the device receives EPCS Priority Access.


Wi-Fi Priority Service Device
EPCS Enabled Wi-Fi Access Network
Wireless Operator/Wi-Fi Identity Provider
1. Configure EPCS Roaming Consortium
2. User enables EPCS Passpoint profile
3. Beacon received with Roaming Consortium EPCS Priority Access Support
4. Association Request (Roaming Consortium Selection Element)
5. Association Response
6. EAP-Identity/ Request
7. EAP-Identity/ Response
8. RADIUS Access-Request
EAP Response Identity
Civic-Location (Country Code/Subdivision)
EPCS-Capable-Indication
HS2.0-Roaming-Consortium
(opt) WBA-Linear-Volume-Rate
9. EAP Dialogue
10. Match user with priority subscription authorization
11. RADIUS Access-Accept

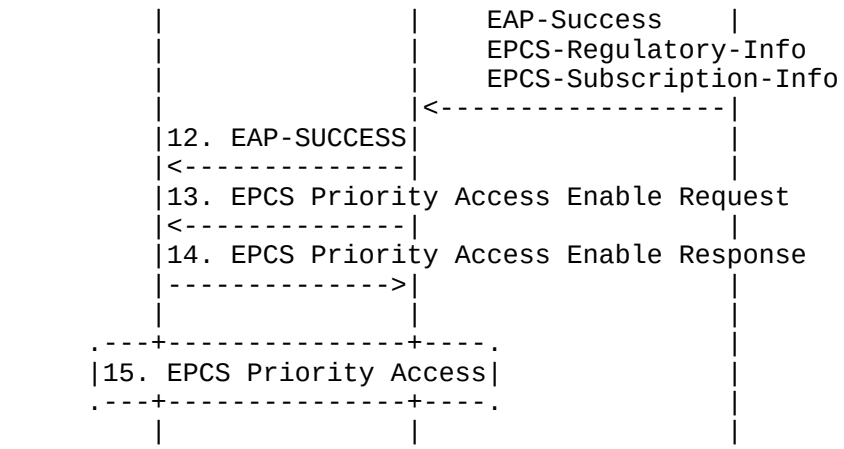


Figure 2: Authorizing Priority Services over Wi-fi

4. RADIUS EPCS Attributes

The current RADIUS protocol does not have the support for the flow described in the previous section and therefore, the following attributes are defined in this document.

4.1. EPCS-Capable-Indication

Description

The EPCS-Capable-Indication (TBA1) Attribute allows a RADIUS NAS to indicate to a RADIUS server that it is EPCS capable.

One EPCS-Capable-Indication Attribute MAY be included in an Access-Request packet.

A summary of the EPCS-Capable-Indication Attribute format is shown in Figure 3. The fields are transmitted from left to right.

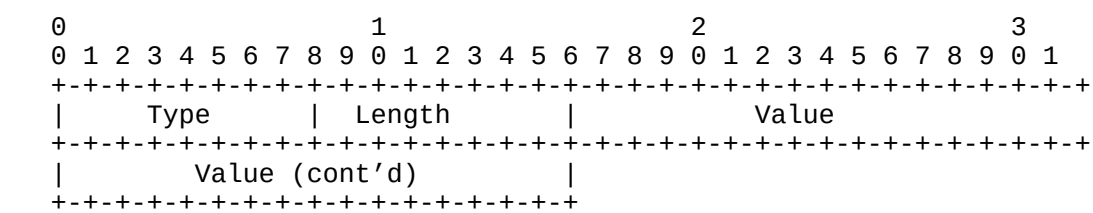


Figure 3: Encoding EPCS-Capable-Indication Attribute

Type

TBA1

Length

6 octet

Data Type

Integer

Value

The field encodes a 32-bit unsigned integer that represents whether the NAS and the device support the EPCS capability and what capabilities the NAS has to handle the traffic to the authorized EPCS users. This document defines two such values used with the EPCS-Capable-Indication attribute:

0 EPCS Priority Access is supported by the NAS, irrespective of EPCS support by the authorized EPCS user device [FCC]. When the authorized EPCS user's device does not support EPCS, the NAS may prioritize downlink traffic. When the authorized EPCS user's device supports EPCS, the NAS prioritizes both uplink and downlink traffic.

1 EPCS Priority Access is only supported by the NAS for EPCS supporting devices. The NAS will prioritize uplink and downlink traffic for EPCS priority access to authorized EPCS users. Flows from non-EPCS supporting devices will not be prioritized.

Note: How the NAS prioritizes the traffic is vendor specific implementation and is outside the scope of this document.

4.2. EPCS-Regulatory-Info

Description

The EPCS-Regulatory-Info (TBA2) Attribute allows a RADIUS Server that is authorizing a user to receive priority channel access to indicate the regulatory regime under which the RADIUS Server operates.

One EPCS-Regulatory-Info Attribute MAY be included in an Access-Accept packet.

A summary of the EPCS-Regulatory-Info Attribute format is shown in Figure 4. The fields are transmitted from left to right.

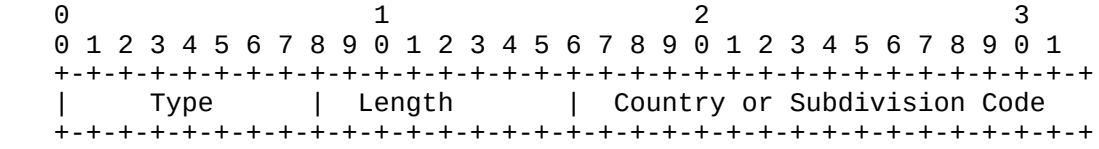


Figure 4: Encoding EPCS-Regulatory-Info Attribute

Type

TBA2

Length

Variable

Data Type

String

Value

The field is a variable length string that encodes either an ISO 3166-1 two-letter country code in capital ASCII letters, e.g., US or FR, or an ISO 3166-2 sub-division code, e.g., US-NY or FR-NC [ISO3166].

4.3. EPCS-Subscription-Info

Description

The EPCS-Subscription-Info (TBA3) Attribute allows a RADIUS Server to indicate to a NAS that a user is authorized to receive priority service.

One EPCS-Subscription-Info Attribute MAY be included in an Access-Accept packet and its presence indicates the authenticated user is authorized to receive priority service together with the priority level associated with the user’s subscription. .

A summary of the EPCS-Subscription-Info Attribute format is shown in Figure 5. The fields are transmitted from left to right.

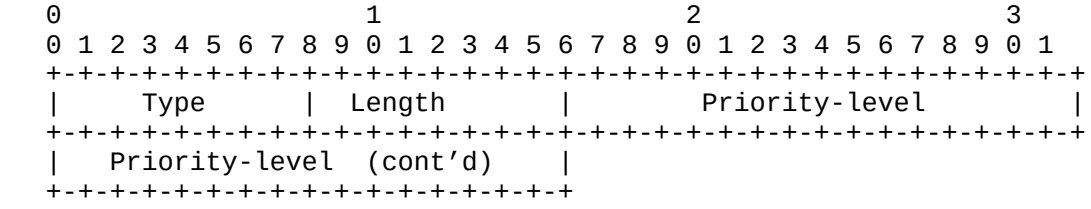


Figure 5: Encoding EPCS-Subscription-Info Attribute

Type

TBA3

Length

6 octet

Data Type

Integer

Value

The field encodes a 32-bit unsigned integer that represents the priority level associated with the user's subscription. Priority levels are administered by the regulatory regime identified by the EPCS-Regulatory-Info attribute, specified in Section 4.2.

5. Security Considerations

All systems which send RADIUS packets outside of secure networks MUST use either IPsec, RADIUS/TLS, or RADIUS/DTLS [I-D.ietf-radext-deprecating-radius].

6. IANA Considerations

This document creates three new RADIUS message types.

7. References

7.1. 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>.

7.2. Informative References

[CSRC5-WG8]
WG8, C. S. R. A. I. C. V., "PRIORITY SERVICES", March 2017, <https://www.fcc.gov/sites/default/files/CSRIC5-WG8-FinalReport031517.pdf>.

[CSRC8-WG4]
COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL VIII WG4, "REPORT ON 911 SERVICE OVER WI-FI", March 2023, <https://www.fcc.gov/sites/default/files/CSRIC8-Report-911overWi-Fi032123.pdf>.

[FCC] Federal Communications Commission, "Review of Rules and Requirements For Priority Services", May 2022, <https://docs.fcc.gov/public/attachments/FCC-22-36A1_Rcd.pdf>.

[I-D.ietf-radext-deprecating-radius]
DeKok, A., "Deprecating Insecure Practices in RADIUS", Work in Progress, Internet-Draft, draft-ietf-radext-deprecating-radius-06, 25 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-radext-deprecating-radius-06>.

[IEEE80211BE]
IEEE, "Enhancements for Extremely High Throughput (EHT)", IEEE 802.11be-2024 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment , October 2024.

[ISO3166] ISO, "The International Standard for country codes and codes for their subdivisions", n.d., <https://www.iso.org/iso-3166-country-codes.html>.

[PASSPOINT]
Wi-Fi Alliance, "Passpoint Specification, v3.3.7", February 2024, <https://www.wi-fi.org/file/passpoint-specification-package>.

[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>.

[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>.

[TS.22153] 3GPP, "Multimedia priority service", 3GPP TS 22.153 20.0.0 , January 2025.

[TS.23003] 3GPP, "Numbering, addressing and identification", 3GPP TS 23.003 19.0.0 , September 2024.

[WBAVSAS] Wireless Broadband Alliance, "Wireless Broadband Alliance Defined Vendor Specific Attributes", May 2023, <https://github.com/wireless-broadband-alliance/RADIUS-VSA>.

Changelog

* 01 - switched all integers to unit32. Updated regulatory info attribute to support both ISO 3166-1 two-letter country code as well as ISO 3166-2 subdivision code as well as corresponding support with RFC5580 CAType.

Acknowledgements

The authors would like to thank all the members of the Wireless Broadband Alliance’s Mission Critical & Emergency Services (e911) project.

Authors’ Addresses

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

Subir Das
Peraton Labs
150 Mount Airy Road
Basking Ridge, 07920
United States of America
Email: sdas@peratonlabs.com

Mark Grayson
Cisco Systems
10 New Square Park
Feltham
TW14 8HA
United Kingdom
Email: mgrayson@cisco.com

Martin C Dolly
AT&T
200 Laurel Avenue
Middletown, 07748
United States of America
Email: Md3135@att.com

An Nguyen
US DHS/CISA
245 Murray Lane SW, MS0123
Washington, DC, 20528-0123
United States of America
Email: an.p.nguyen@cisa.dhs.gov