opsawg
Internet-Draft
Intended status: Standards Track
Expires: December 5, 2021

M. Boucadair
Orange
T. Reddy
McAfee

June 3, 2021

RADIUS Extensions for Encrypted DNS
draft-boucadair-opsawg-add-encrypted-dns-00

Abstract

This document specifies new Remote Authentication Dial-In User Service (RADIUS) attributes that carry an authentication domain name, a list of IP addresses, and a set of service parameters of encrypted DNS resolvers.

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 December 5, 2021.

Table of Contents

1. Introduction

In the context of broadband services, ISPs traditionally provide DNS resolvers to their customers. To that aim, ISPs deploy dedicated mechanisms to advertise a list of DNS Recursive DNS server(s) to their customers (e.g., DHCP, IPv6 Router Advertisement). The information used to populate DHCP messages and/or IPv6 Router Advertisements relies upon specific Remote Authentication Dial-In User Service (RADIUS) [RFC2865] attributes such as the DNS-Server-IPv6-Address Attribute specified in [RFC6911].

With the advent of Encrypted DNS (e.g., DNS-over-HTTPS (DoH) [RFC8484], DNS-over-TLS (DoT) [RFC7858], or DNS-over-QUIC (DoQ) [I-D.ietf-dprive-dnsoquic]), additional means are required to provision hosts with network-designated Encrypted DNS. To fill that void, [I-D.ietf-add-dnr] leverages existing protocols such as DHCP and IPv6 Router Advertisement to provide hosts with the required information to connect to an Encrypted DNS server. However, there are no RADIUS attributes that can be used to populate the discovery messages discussed in [I-D.ietf-add-dnr].

This document specifies two new RADIUS attributes: IPv6-Encrypted-DNS (Section 3.1) and IPv4-Encrypted-DNS (Section 3.2) Attributes. Note that two attributes are specified in order to accommodate both IPv4

and IPv6 deployment contexts while taking into account the constraints in Section 3.4 of [RFC6158].

Typical deployment scenarios are similar to those described, for instance, in Section 2 of [RFC6911]. Some of these deployments may rely upon the mechanisms defined in [RFC4014] or [RFC7037], which allows a Network Access Server (NAS) to pass attributes obtained from a RADIUS server to a DHCP server. For illustration purposes, Figure 1 shows an example where a Customer Premises Equipment (CPE) is provided with an Encrypted DNS server. This example assumes that the NAS embeds both RADIUS client and DHCPv6 server capabilities.

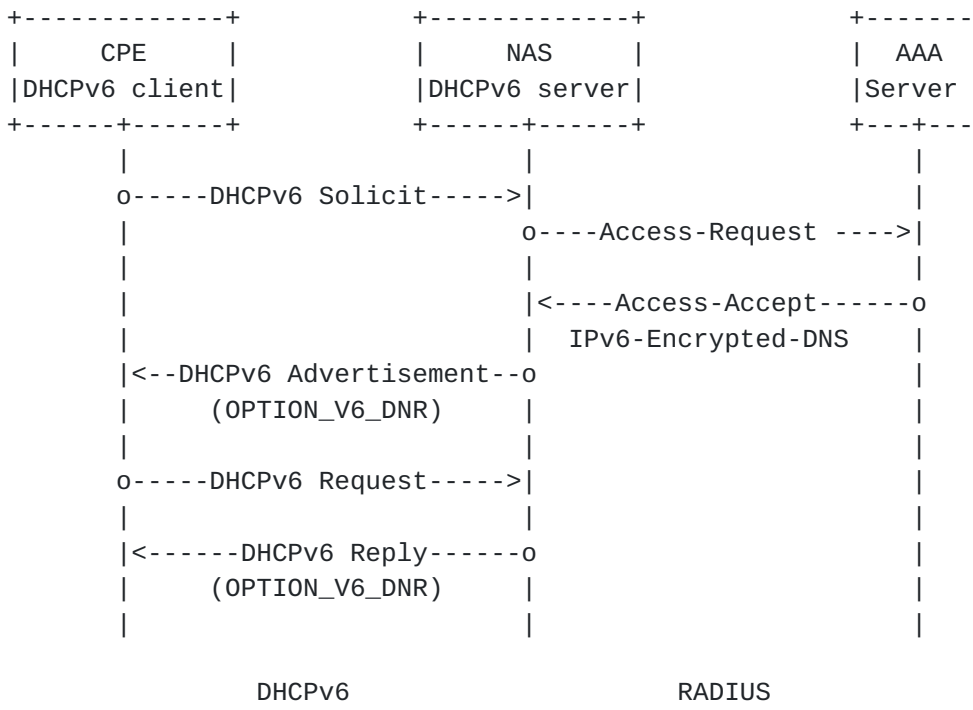

Figure 1: Example of RADIUS IPv6 Encrypted DNS

Upon receipt of the DHCPv6 Solicit message from a CPE, the NAS sends a RADIUS Access-Request message to the AAA server. Once the AAA server receives the request, it replies with an Access-Accept message (possibly after having sent a RADIUS Access-Challenge message and assuming the CPE is entitled to connect to the network) that carries a list of parameters to be used for this session, and which include the Encrypted DNS information. The content of the IPv6-Encrypted-DNS Attribute is then used by the NAS to complete the DHCPv6 procedure that the CPE initiated to retrieve information about the encrypted DNS service to use. The procedure defined in [I-D.ietf-add-dnr] is thus followed between the DHCPv6 client and the DHCPv6 server. The same procedure is followed between the DHCPv6 client on endpoints serviced by the CPE and the DHCPv6 server on CPE.

Upon change of the any Encrypted DNS-related information (e.g., ADN, IPv6 address), the RADIUS server sends a RADIUS CoA message [RFC5176] that carries the RADIUS IPv6-Encrypted-DNS Attributed to the NAS. Once that message is accepted by the NAS, it replies with a RADIUS CoA ACK message. The NAS replaces the old Encrypted DNS server information with the new one and sends a DHCPv6 Reconfigure message to cause the DHCPv6 client to initiate a Renew/Reply message exchange with the DHCPv6 server.

Figure 2 shows another example where a CPE is provided an Encrypted DNS server, but the CPE uses DHCPv4 to retrieve its encrypted DNS server.

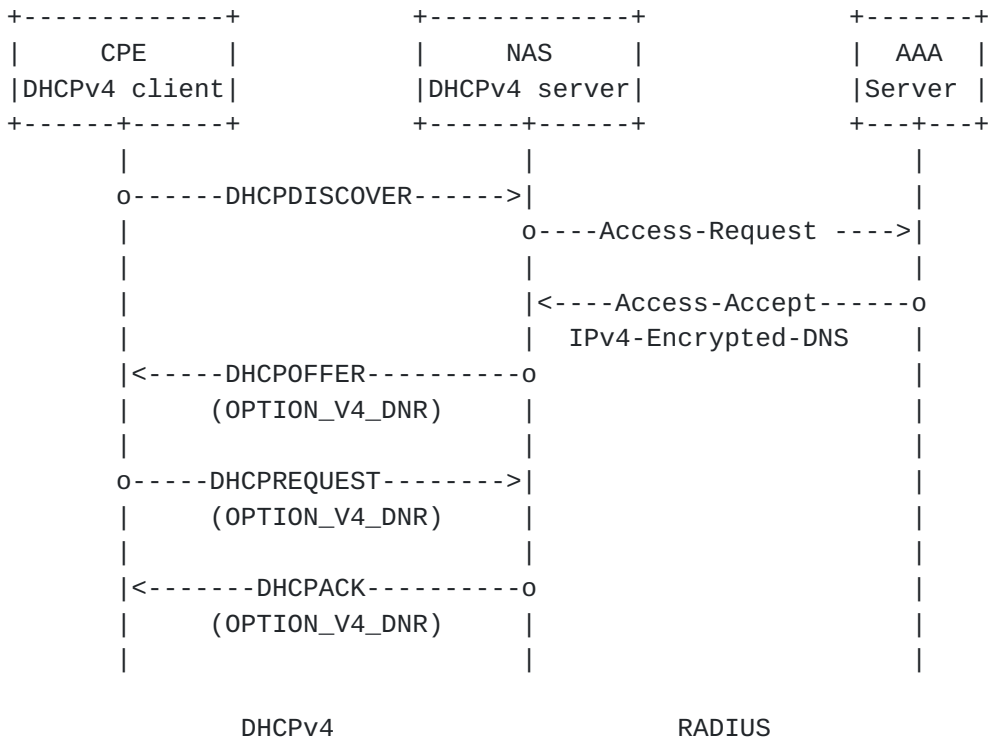

Figure 2: Example of RADIUS IPv4 Encrypted DNS

For the particular case of DoH [RFC8484], the attributes defined in Section 3 can also be used for redirection purposes. For example, a DoH server may redirect DoH clients to other DoH servers (e.g., local forwarders hosted by a CPE). To that aim, when a DoH query is received from a DoH client, the DoH servers interacts with an AAA server to check whether redirection should be enabled for this client. If such redirection is to be enabled, the AAA server returns IPv4-Encrypted-DNS and/or IPv6-Encrypted-DNS Attributes that will be used to populate the DoH redirection response that will then be sent to the DoH client. The DoH client may contact the DoH server using the information supplied in the redirection response.

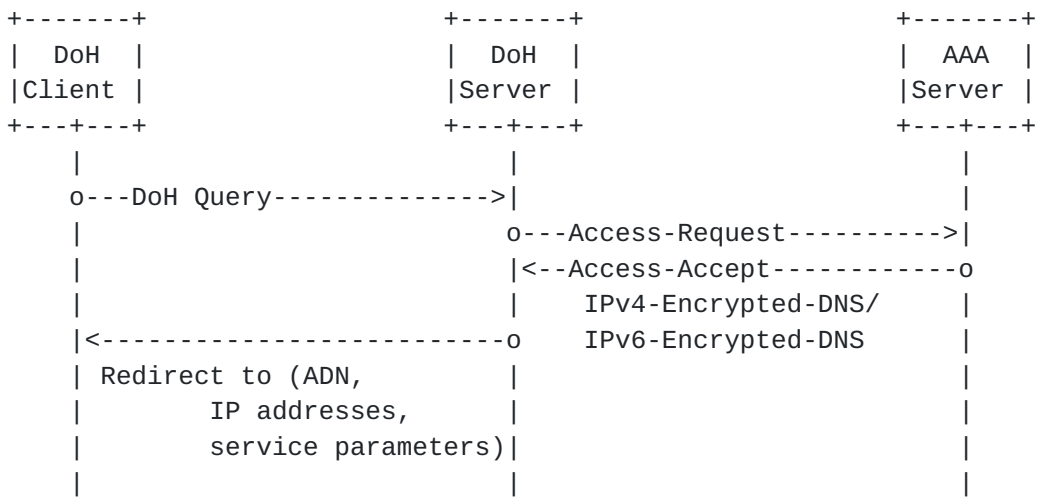

Figure 3: Example of DoH Redirection

Other deployment scenarios can be envisaged, however it is out of the scope of this document to provide a comprehensive list of those deployments.

This document adheres to [RFC8044] for defining the new attributes.

2. Terminology

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.

This document makes use of the terms defined in [RFC8499]. The following additional terms are used:

Encrypted DNS: refers to a scheme where DNS exchanges are transported over an encrypted channel. Examples of encrypted DNS are DNS-over-TLS (DoT) [RFC7858], DNS-over-HTTPS (DoH) [RFC8484], or DNS-over-QUIC (DoQ) [I-D.ietf-dprive-dnsoquic].

3. Encrypted DNS RADIUS Attributes

Both IPv6-Encrypted-DNS and IPv4-Encrypted-DNS have the same format shown in Figure 4. The description of the fields is provided in Sections 3.1 and 3.2.

These attributes and their embedded TLVs (Section 3.3) are defined with globally unique names and follow the guidelines in Section 2.7.1 of [RFC6929].

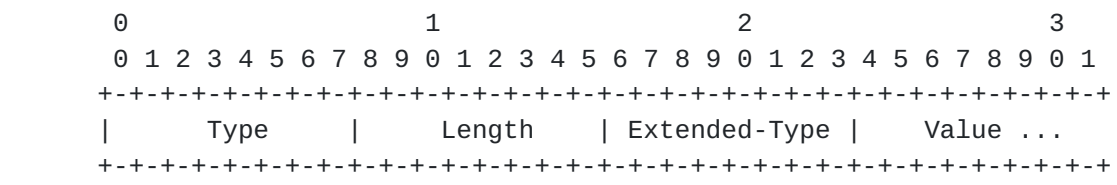

Figure 4: Format of IPv6-Encrypted-DNS and IPv4-Encrypted-DNS Attributes

3.1. IPv6-Encrypted-DNS Attribute

This attribute is of type "tlv" as defined in Section 2.3 of [RFC6929].

The IPv6-Encrypted-DNS Attribute includes the authentication domain name, a list of IPv6 addresses, and a set of service parameters of an encrypted DNS resolver.

Because multiple IPv6-Encrypted-DNS Attributes may be provisioned to a requesting host, multiple instances of the IPv6-Encrypted-DNS attribute MAY be included; each instance of the attribute carries a distinct Encrypted DNS server.

The IPv6-Encrypted-DNS Attribute MAY appear in a RADIUS Access-Accept packet. It MAY also appear in a RADIUS Access-Request packet as a hint to the RADIUS server to indicate a preference. However, the server is not required to honor such a preference.

The IPv6-Encrypted-DNS Attribute MAY appear in a RADIUS CoA-Request packet.

The IPv6-Encrypted-DNS Attribute MAY appear in a RADIUS Accounting-Request packet.

The IPv6-Encrypted-DNS Attribute MUST NOT appear in any other RADIUS packet.

The IPv6-Encrypted-DNS Attribute is structured as follows:

Type

241

Length

This field indicates the total length, in octets, of all fields of this attribute, including the Type, Length, Extended-Type, and the entire length of the embedded TLVs.

Extended-Type

TBA1 (see Section 6.1).

Value

This field contains a set of TLVs as follows:

Encrypted-DNS-ADN TLV: The IPv6-Encrypted-DNS Attribute MUST include exactly one instance of Encrypted-DNS-ADN TLV (Section 3.3.1).

Encrypted-DNS-IPv6-Address TLV: The IPv6-Encrypted-DNS Attribute MUST include one or multiple instances of Encrypted-DNS-IPv6-Address TLV (Section 3.3.2).

Encrypted-DNS-SvcParams TLV: The IPv6-Encrypted-DNS Attribute SHOULD include one instance of Encrypted-DNS-SvcParams TLV (Section 3.3.4).

The IPv6-Encrypted-DNS Attribute is associated with the following identifier: 241.TBA1.

3.2. IPv4-Encrypted-DNS Attribute

This attribute is of type "tlv" as defined in Section 2.3 of [RFC6929].

The IPv4-Encrypted-DNS Attribute includes the authentication domain name, a list of IPv4 addresses, and a set of service parameters of an encrypted DNS resolver.

Because multiple IPv4-Encrypted-DNS attributes may be provisioned to a requesting host, multiple instances of the IPv4-Encrypted-DNS attribute MAY be included; each instance of the attribute carries a distinct Encrypted DNS server.

The IPv4-Encrypted-DNS Attribute MAY appear in a RADIUS Access-Accept packet. It MAY also appear in a RADIUS Access-Request packet as a hint to the RADIUS server to indicate a preference. However, the server is not required to honor such a preference.

The IPv4-Encrypted-DNS Attribute MAY appear in a RADIUS CoA-Request packet.

The IPv4-Encrypted-DNS Attribute MAY appear in a RADIUS Accounting-Request packet.

The IPv4-Encrypted-DNS Attribute MUST NOT appear in any other RADIUS packet.

The IPv4-Encrypted-DNS Attribute is structured as follows:

Type

241

Length

This field indicates the total length, in octets, of all fields of this attribute, including the Type, Length, Extended-Type, and the entire length of the embedded TLVs.

Extended-Type

TBA2 (see Section 6.1).

Value

This field contains a set of TLVs as follows:

Encrypted-DNS-ADN TLV: The IPv4-Encrypted-DNS Attribute MUST include exactly one instance of Encrypted-DNS-ADN TLV (Section 3.3.1).

Encrypted-DNS-IPv4-Address TLV: The IPv4-Encrypted-DNS Attribute MUST include one or multiple instances of Encrypted-DNS-IPv4-Address TLV (Section 3.3.3).

Encrypted-DNS-SvcParams TLV: The IPv4-Encrypted-DNS Attribute SHOULD include one instance of Encrypted-DNS-SvcParams TLV (Section 3.3.4).

The IPv4-Encrypted-DNS Attribute is associated with the following identifier: 241.TBA2.

3.3. RADIUS TLVs for Encrypted DNS

The TLVs defined in the following subsections use the format defined in [RFC6929]. These TLVs have the same name and number when encapsulated in any of the parent attributes defined in Sections 3.1 and 3.2.

The encoding of the "Value" field of these TLVs follows the recommendation of [RFC6158].

3.3.1. Encrypted-DNS-ADN TLV

TLV-Type

TBA3 (see Section 6.2).

TLV-Length

Length of included ADN + 2 octets.

Data Type

The Encrypted-DNS-ADN TLV is of type text (Section 3.4 of [RFC8044]).

TLV-Value

This field includes a fully qualified domain name of the Encrypted DNS server. This field is formatted as specified in Section 10 of [RFC8415].

This TLV is identified as 241.TBA1.TBA3 when included in the IPv6-Encrypted-DNS Attribute (Section 3.1) and as 241.TBA2.TBA3 when included in the IPv4-Encrypted-DNS Attribute (Section 3.2).

3.3.2. Encrypted-DNS-IPv6-Address TLV

TLV-Type

TBA4 (see Section 6.2).

TLV-Length

18

Data Type

The Encrypted-DNS-IPv6-Address TLV is of type ip6addr (Section 3.9 of [RFC8044]).

TLV-Value

This field includes an IPv6 address (128 bits) of the Encrypted DNS server.

The Encrypted-DNS-IPv6-Address attribute MUST NOT include multicast and host loopback addresses [RFC6890].

This TLV is identified as 241.TBA1.TBA4 as part of the IPv6-Encrypted-DNS Attribute (Section 3.1).

3.3.3. Encrypted-DNS-IPv4-Address TLV

TLV-Type

TBA5 (see Section 6.2).

TLV-Length

6

Data Type

The Encrypted-DNS-IPv4-Address TLV is of type ip4addr (Section 3.8 of [RFC8044]).

TLV-Value

This field includes an IPv4 address (32 bits) of the Encrypted DNS server.

The Encrypted-DNS-IPv4-Address attribute MUST NOT include multicast and host loopback addresses.

This TLV is identified as 241.TBA1.TBA5 as part of the IPv4-Encrypted-DNS Attribute (Section 3.2).

3.3.4. Encrypted-DNS-SvcParams TLV

TLV-Type

TBA6 (see Section 6.2).

TLV-Length

Length of included service parameters + 2 octets.

Data Type

The Encrypted-DNS-SvcParams TLV is of type text (Section 3.4 of [RFC8044]).

TLV-Value

Specifies a set of service parameters that are encoded following the rules in [I-D.ietf-add-dnr]. Service parameters may include,

for example, a list of ALPN protocol identifiers or alternate port numbers.

The service parameters MUST NOT include "ipv4hint" or "ipv6hint" SvcParams as they are superseded by the included IP addresses.

This TLV is identified as 241.TBA1.TBA6 when included in the IPv6-Encrypted-DNS Attribute (Section 3.1) and as 241.TBA2.TBA6 when included in the IPv4-Encrypted-DNS Attribute (Section 3.2).

4. Security Considerations

RADIUS-related security considerations are discussed in [RFC2865].

Security considerations (including traffic theft) are discussed in [I-D.ietf-add-dnr].

5. Table of Attributes

The following table provides a guide as what type of RADIUS packets that may contain these attributes, and in what quantity.

Access-Request	Access-Accept	Access-Reject	Challenge	Acct. Request	# Attribute
0+	0+	0	0	0+	TBA1 IPv6-Encrypted-DNS
0+	0+	0	0	0+	TBA2 IPv4-Encrypted-DNS

CoA-Request	CoA-ACK	CoA-NACK	# Attribute
0+	0	0	TBA1 IPv6-Encrypted-DNS
0+	0	0	TBA1 IPv4-Encrypted-DNS

The following table defines the meaning of the above table entries:

0 This attribute MUST NOT be present in packet.
0+ Zero or more instances of this attribute MAY be present in packet.

6. IANA Considerations

6.1. New RADIUS Attributes

IANA is requested to assign two new RADIUS attribute types from the IANA registry "Radius Attribute Types" located at http://www.iana.org/assignments/radius-types:

IPv6-Encrypted-DNS (241.TBA1)

IPv4-Encrypted-DNS (241.TBA2)

Type	Description	Data Type	Reference
241.TBA1	IPv6-Encrypted-DNS	tlv	This-Document
241.TBA2	IPv4-Encrypted-DNS	tlv	This-Document

6.2. New RADIUS TLVs

IANA is requested to create a new registry called "RADIUS Encrypted DNS TLVs". The registry is initillay populated as follows:

Value	Description	Data Type	Reference
0	Reserved		
1	Encrypted-DNS-ADN	text	Section 3.3.1
2	Encrypted-DNS-IPv6-Address	ipv6addr	Section 3.3.2
3	Encrypted-DNS-IPv4-Address	ipv4addr	Section 3.3.3
4	Encrypted-DNS-SvcParams	text	Section 3.3.4
5-255	Unassigned		

7. Acknowledgements

Thanks to Christian Jacquenet for the review.

8. References

8.1. Normative References

[I-D.ietf-add-dnr] Boucadair, M., Reddy, T., Wing, D., Cook, N., and T. Jensen, "DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)", draft-ietf-add-dnr-00 (work in progress), February 2021.

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

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

[RFC6158] DeKok, A., Ed. and G. Weber, "RADIUS Design Guidelines", BCP 158, RFC 6158, DOI 10.17487/RFC6158, March 2011, <https://www.rfc-editor.org/info/rfc6158>.

[RFC6890] Cotton, M., Vegoda, L., Bonica, R., Ed., and B. Haberman, "Special-Purpose IP Address Registries", BCP 153, RFC 6890, DOI 10.17487/RFC6890, April 2013, <https://www.rfc-editor.org/info/rfc6890>.

[RFC6929] DeKok, A. and A. Lior, "Remote Authentication Dial In User Service (RADIUS) Protocol Extensions", RFC 6929, DOI 10.17487/RFC6929, April 2013, <https://www.rfc-editor.org/info/rfc6929>.

[RFC8044] DeKok, A., "Data Types in RADIUS", RFC 8044, DOI 10.17487/RFC8044, January 2017, <https://www.rfc-editor.org/info/rfc8044>.

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

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

8.2. Informative References

[I-D.ietf-dprive-dnsoquic] Huitema, C., Mankin, A., and S. Dickinson, "Specification of DNS over Dedicated QUIC Connections", draft-ietf-dprive-dnsoquic-02 (work in progress), February 2021.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <https://www.rfc-editor.org/info/rfc2131>.

[RFC4014] Droms, R. and J. Schnizlein, "Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option", RFC 4014, DOI 10.17487/RFC4014, February 2005, <https://www.rfc-editor.org/info/rfc4014>.

[RFC5176] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 5176, DOI 10.17487/RFC5176, January 2008, <https://www.rfc-editor.org/info/rfc5176>.

[RFC6911] Dec, W., Ed., Sarikaya, B., Zorn, G., Ed., Miles, D., and B. Lourdelet, "RADIUS Attributes for IPv6 Access Networks", RFC 6911, DOI 10.17487/RFC6911, April 2013, <https://www.rfc-editor.org/info/rfc6911>.

[RFC7037] Yeh, L. and M. Boucadair, "RADIUS Option for the DHCPv6 Relay Agent", RFC 7037, DOI 10.17487/RFC7037, October 2013, <https://www.rfc-editor.org/info/rfc7037>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

Authors' Addresses

Mohamed Boucadair
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Tirumaleswar Reddy
McAfee, Inc.
Embassy Golf Link Business Park
Bangalore, Karnataka 560071
India

Email: kondtir@gmail.com