Workgroup: Network Working Group
Internet-Draft:
draft-reddy-add-delegated-credentials-03
Published: 1 December 2023
Intended Status: Standards Track
Expires: 3 June 2024
Authors: T. Reddy M. Boucadair D. Wing S. Jain
Nokia Orange Citrix McAfee

Delegated Credentials to Host Encrypted DNS Forwarders on CPEs

Abstract

An encrypted DNS server is authenticated by a certificate signed by a Certificate Authority (CA). However, for typical encrypted DNS server deployments on Customer Premise Equipment (CPEs), the signature cannot be obtained or requires excessive interactions with a Certificate Authority.

This document explores the use of TLS delegated credentials for a DNS server deployed on a CPE. This approach is meant to ease operating DNS forwarders in CPEs while allowing to make use of encrypted DNS capabilities.

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 3 June 2024.

Table of Contents

1. Introduction

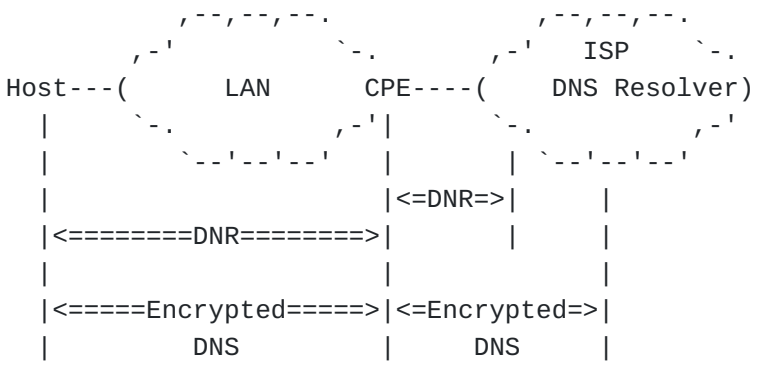
1.1. CPEs, a Critical Componenet in Home Networks.

Customer Premises Equipment (CPEs, also called Home Routers) are a critical component of the home network, and their security is essential to protecting the devices and data that are connected to them. For example, the prpl Foundation [prpl] has developed a number of initiatives to promote home router security and hardening. The prplWrt project [prplwrt] is an initiative in prpl Foundation that aims to improve the security and performance of open-source router firmware, such as OpenWrt [openwrt]. OpenWrt is an open-source operating system that is designed to run on a wide range of routers and embedded devices. It now includes support for containerization technology such as Docker, making it possible to run containerized applications on a home router. Further, DNS providers have optimized the encrypted DNS forwarder to run in a container in home routers.

1.2. Proxied DNS In Local Networks

Figure 1 shows various network setups where the CPE embeds a caching encrypted DNS forwarder. Section 1.3.1 discusses the applicability of DNR as a function of the address used by the CPE for the verification of ownership.

(a)



(b)

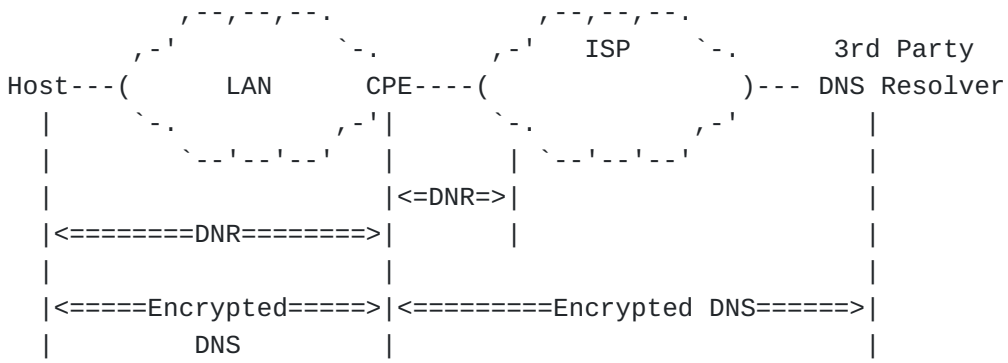


Figure 1: Proxied Encrypted DNS Sessions

For all the cases shown in Figure 1, the CPE advertises itself as the default DNS server to the hosts it serves in the LAN. The CPE relies upon DHCP or RA to advertise itself to internal hosts as the default encrypted DNS forwarder. When receiving a DNS request it cannot handle locally, the CPE forwards the request to an upstream encrypted DNS. The upstream encrypted DNS can be hosted by the ISP or provided by a third party.

Such a forwarder presence is required for IPv4 service continuity purposes (e.g., Section 3.1 of [RFC8585]) or for supporting advanced services within a local network (e.g., malware filtering, parental control, Manufacturer Usage Description (MUD) [RFC8520] to only allow intended communications to and from an IoT device, and multicast DNS proxy service for the ".local" domain [RFC6762]). When

the CPE behaves as a DNS forwarder, DNS communications can be decomposed into two legs to resolve queries:

*The leg between an internal host and the CPE.

*The leg between the CPE and an upstream DNS resolver.

1.3. Hosting Encrypted DNS Forwarder in Local Networks

This section discusses some deployment challenges to host an encrypted DNS forwarder within a local network.

1.3.1. DDR/DNR Comparison and Naming Constraints

DDR requires proving possession of an IP address, as the DDR certificate contains the server's IPv4 and IPv6 addresses and is signed by a certificate authority. DDR is constrained to public IP addresses because (WebPKI) certificate authorities will not sign special-purpose IP addresses [RFC6890], most notably IPv4 private-use [RFC1918], IPv4 shared address [RFC6598], or IPv6 Unique-Local [RFC8190] address space. A tempting solution is to use the CPE's WAN IP address for DDR and prove possession of that IP address. However, the CPE's WAN IPv4 address will not be a public IPv4 address if the CPE is behind another layer of NAT (either Carrier Grade NAT (CGN) or another on-premise NAT), reducing the success of this mechanism to CPE's WAN IPv6 address. If the ISP renumbers the subscriber's network suddenly (rather than slow IPv6 renumbering described in [RFC4192]) encrypted DNS service will be delayed until that new certificate is acquired.

DNR requires proving possession of an FQDN as the encrypted resolver's certificate contains the FQDN. The entity (e.g., ISP, network administrator) managing the CPE would assign a unique FQDN to the CPE. There are two mechanisms for the CPE to obtain the certificate for the FQDN: using one of its WAN IP addresses or requesting its signed certificate from an Internet-facing server used for remote CPE management (e.g., the Auto Configuration Server (ACS) in the CPE WAN Management Protocol [TR-069]). If using a CPE's WAN IP address, the CPE needs a public IPv4 or a global unicast IPv6 address together with DNS A or AAAA records pointing to that CPE's WAN address to prove possession of the DNS name to obtain a WebPKI CA-signed certificate (that is, the CPE fulfills the DNS or HTTP challenge discussed in ACME [RFC8555]). However, a CPE's WAN address will not be a public IPv4 address if the CPE is behind another layer of NAT (either a CGN or another on-premise NAT), reducing the success of this mechanism to a CPE's WAN IPv6 address. The mechanisms have the following limitations for certificate issuance:

*In case of large scale of CPEs (e.g., millions of devices), issuing certificate request for a large number of subdomains

could be treated as an attack by the certificate authorities to overwhelm it.

* Dependency on the CA to manage a large number of certificates.

* If the CPE uses one of its WAN IP addresses to obtain the certificate for the FQDN, the internet-facing HTTP server or a DNS authoritative server on the CPE to complete the HTTP or DNS challenge can be subjected to DDoS attacks.

1.3.2. Delegated Certificate Issuance

The encrypted DNS forwarder is hosted on a CPE and provisioned by a service (e.g., ACS) in the operator's network. Each CPE is assigned a unique FQDN (e.g., "cpe-12345.example.com" where 12345 is a unique number). It is NOT RECOMMENDED that such an FQDN carries any Personally Identifiable Information (PII) or device identification details like the customer number or device's serial number. The CPE generates a public and private key-pair, builds a certificate signing request (CSR), and sends the CSR to a service in the operator managing the CPE. Upon receipt of the CSR, the operator's service can utilize Automatic Certificate Management Environment (ACME) [RFC8555] to automate certificate management functions such as domain validation procedure, certificate issuance, and certificate revocation.

The challenge with this technique is that the service will have to communicate with the CA to issue certificates for millions of CPEs. If an external CA is unable to issue a certificate in time or replace an expired certificate, the service would no longer be able to present a valid certificate to a CPE. When the service requests certificate issuance for a large number of subdomains (e.g., millions of CPEs), it may be treated as an attacker by the CA to overwhelm it. Furthermore, the short-lived certificates (e.g., certificates that expire after 90 days) issued by the CA will have to be renewed frequently. With short-lived certificates, there is a smaller time window to renew a certificate and, therefore, a higher risk that a CA outage will negatively affect the uptime of the encrypted DNS forwarders on CPEs (and the services offered via these CPEs).

1.4. Objectives & Scope

This document discusses the use of delegated credentials [RFC9345] to host encrypted DNS resolvers, such as DoH [RFC8484], DNS-over-TLS (DoT) [RFC7858], or DNS-over-QUIC (DoQ) [RFC9250] in managed CPEs by reducing the dependency on Certification Authority (CA). The advantage of using delegated credentials on CPEs is that it completely removes the dependency on the CAs to provide a PKI

certificate for each CPE. The entity managing the CPE (e..g, ISP, CPE vendor, Security Service Provider) will provision it a with a delegated credential and renew the delegated credential before the expiry.

Scope of this document is an encrypted DNS server deployed on a managed CPEs.

2. Terminology

This document makes use of the terms defined in [RFC8499].

The following additional terms are used:

DHCP: refers to both DHCPv4 and DHCPv6.

Do53: refers to unencrypted DNS.

DNR: refers to the Discovery of Network-designated Resolvers procedure defined in [I-D.ietf-add-dnr].

DDR: refers to the Discovery of Designated Resolvers procedure defined in [I-D.ietf-add-ddr].

Encrypted DNS: refers to a scheme where DNS exchanges are transported over an encrypted channel. Examples of encrypted DNS are DoH [RFC8484], DNS-over-TLS (DoT) [RFC7858], and DNS-over-QUIC (DoQ) [RFC9250].

Managed CPE: refers to a CPE that is managed by an ISP or CPE vendor or Security Service Provider.

Unmanaged CPE: refers to a CPE that is not managed by an ISP or CPE vendor or Security Service Provider.

Delegated credential: The certificate issued by the operator as described by [RFC9345].

3. Delegated Credentials

To reduce the dependency on external CAs, this document RECOMMENDS the use of delegation credentials [RFC9345] to be added to the TLS profile of encrypted DNS client and server implementations.

A delegated credential (DC) is a digitally signed data structure with two semantic fields: a validity interval and a public key (along with its associated signature algorithm). The signature on the delegated credential indicates a delegation from the certificate that is issued to the peer.

The delegation allows a service in the operator managing the CPE to issue its own credentials within the scope of a certificate issued by an external CA. These credentials only enable the CPE who is recipient of the delegation to terminate connections for names that the CA has authorized. Furthermore, this mechanism allows the encrypted DNS forwarder on a CPE to use modern signature algorithms, such as Ed25519 [RFC8032] even if the CA does not support them.

The signature on the delegated credential indicates a delegation from the certificate that is issued to a service in an infrastrcture owned by the CPE's operator. The private key used to sign a credential corresponds to the public key of the service's X.509 end-entity certificate [RFC5280]. The delegated credential is cryptographically bound to the service's X.509 end-entity certificate with which the credential will be used. The X.509 end-entity certificate will have the KeyPurposeId set to id-kp-serverAuth for the client to identify that the certificate is issued for a server.

The basic sequence of steps involved is shown in Figure 2.

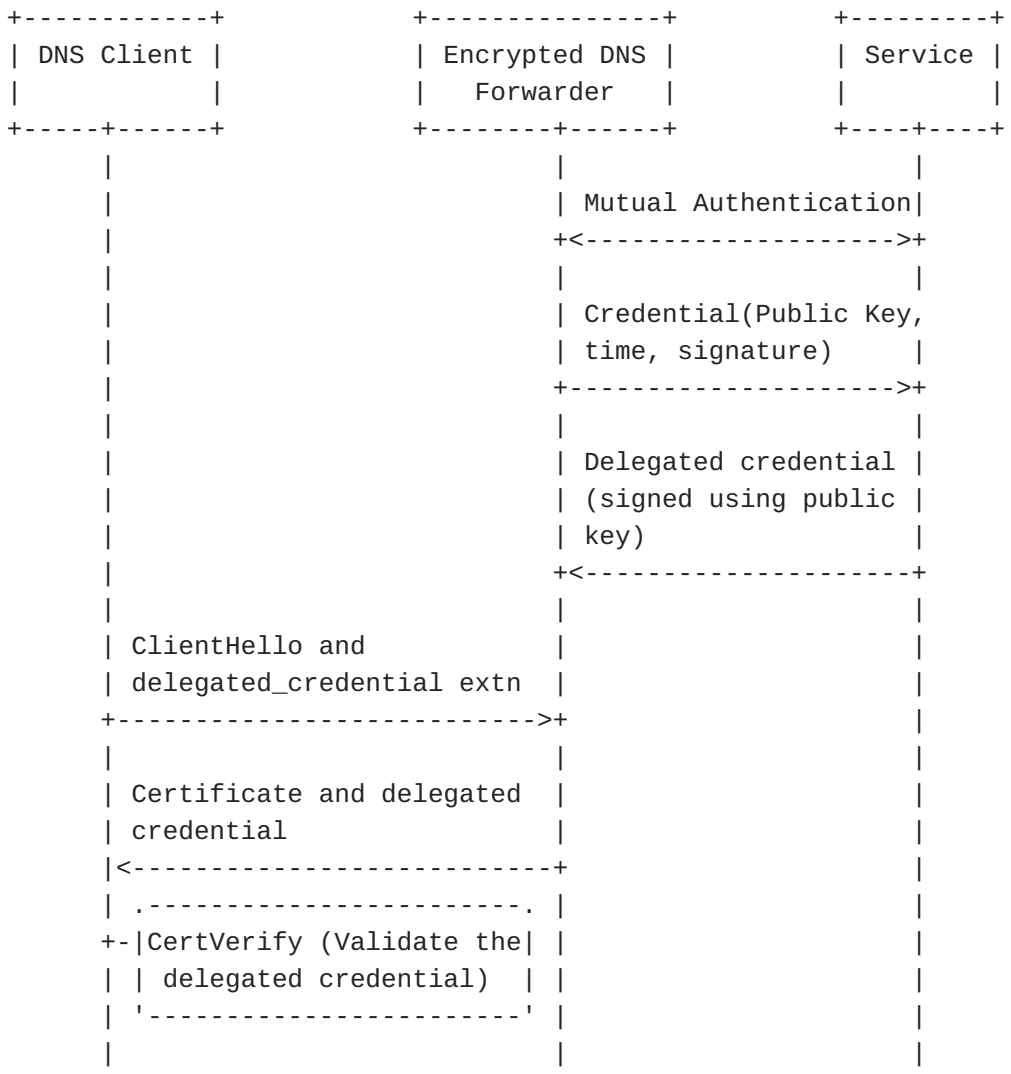


Figure 2: Typical Sequence Diagram

1. The DNS client provides an extension in its ClientHello that indicates support for delegated credentials.

2. The DNS forwarder sends the Certificate message providing both the certificate of the service as well as the delegated credential.

3. The DNS client uses information from the certificate to verify the delegated credential and that the DNS forwarder is asserting an expected identity.

For example, the operator managing the CPEs has a X.509 end-entity certificate for a domain "dnsserver.example.net" and issues each managed CPE managed a distinct delegated credential signed by the private key which orresponds to the public key of the X.509 end-entity certificate. If the operator is managing a large number of CPEs, different X.509 end-entity certificates can be used to manage

a group of CPEs (e.g., "dnsserver.group1.example.net", "dnsserver.group2.example.net" etc.). When one of the X.509 end-entity certificate is revoked, only the group of CPEs associated with that certificate need renewed delegated credentials signed by the private key which corresponds to the public key of the the replaced certificate and it reduces the burden on the operator to sign the credentails for only a subset of the CPEs.

4. Legacy DNS Clients

In order to also cover DNS clients that do not support delegation credentials or TLS 1.3 or later, server-side mechanisms that do not require changes to the client behavior are required (e.g., a PKCS#11 interface or a remote signing mechanism, [KEYLESS] being examples) as discussed in Section 3.2 of [RFC9345].

As depicted in Figure 3, a DNS forwarder may use delegated credentials for DNS clients that support them, while using a server-side mechanism to service local legacy DNS clients.

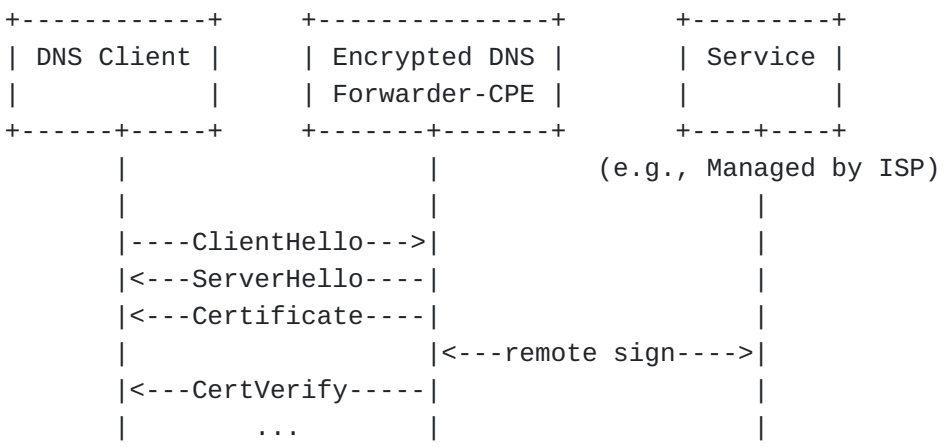


Figure 3: An Example of Remote key signing

5. The delegation SvcParamKey

For the "dns" scheme, as defined in [I-D.ietf-add-svcb-dns], the "tlsdelegation" SvcParamKey is used to indicate that a DNS server can be authenticated using delegation credentials. The DNS server must include the "tlsdelegation" parameter in the mandatory parameter list if the server is only accessible using delegation credentials. Marking the "tlsdelegation" parameter as mandatory will cause DNS clients that do not understand the parameter to ignore that SVCB record and they will not try to establish an authenticated secure connection with the DNS server. Including the "tlsdelegation" parameter without marking it mandatory advertises a DNS server that can be optionally authenticated using delegation credentials.

Both the presentation and wire format values for the "tlsdelegation" parameter MUST be empty. For example, a DoH service advertised over DNR can be annotated as only supporting delegation credentials using the following record:

```
_dns.example.net.  7200  IN SVCB 1 doh.example.net (
     alpn=h2 dohpath=/dns-query{?dns} tlsdelegation mandatory=tlsdelegat
```

6. Design Rationale

Alternate solutions and their limitations are discussed below:

* A service managing the CPEs could get a CA certificate with name constraints extension (Section 4.2.1.10 of [RFC5280]) and the service would in-turn act as an ACME server to provision end-entity certificates on CPEs.

  - Con: Name constraints extension is not yet supported by CAs, although [RFC5280] was standardized way back in 2008.

  - Pro: Avoids changing TLS client and server (e.g., stunnel or openssl).

* [RFC9115] defines a profile of the ACME protocol for generating Delegated certificates. It allows the CPEs to request from a service managing the CPEs, acting as a profiled ACME server, a certificate for a delegated identity, i.e., one belonging to the service. The service then uses the ACME protocol (with the extensions described in [RFC8739]) to request issuance of a short-term, Automatically Renewed (STAR) certificate for the same delegated identity. The generated short-term certificate is automatically renewed by the ACME CA, is periodically fetched by the CPEs, and is used to act as encrypted DNS forwarders. The service can end the delegation at any time by instructing the CA to stop the automatic renewal and letting the certificate expire shortly thereafter. Star certificates requires support by CAs but does not require changes to the deployed TLS ecosystem.

  - Con: Star certificates require support by CAs.

  - Con: A primary use case of Star certificates is that of a Content Delivery Network (CDN), the third party, terminating TLS sessions on behalf of a content provider (the holder of a domain name). The number of star certificates required for a CDN use case will be very much lower than the use case discussed in this draft. It is yet to be seen if CAs will agree to support star certificates at a scale of millions of CPEs.

  - Pro: Avoids changing TLS client and server.

In summary, Star certificates, name constraints extension, and Delegated credentials suffer from the problem of deploying a new feature to CAs, TLS clients, and servers.

7. Security Considerations

DNR-related security considerations are discussed in Section 7 of [I-D.ietf-add-dnr]. Likewise, DDR-related security considerations are discussed in Section 7 of [I-D.ietf-add-ddr]. The security considerations in [RFC9345] are to be taken into account.

The delegated credentials should be used to send a delegation only to a trusted CPE. It is meant to be used between parties that have a trust relationship with each other, for example, a managed CPE and a service managing it. The secrecy of the delegated credential's private key is thus important, and access control mechanisms must be used to protect it, including Hardware Security Modules, Trusted Execution Environment, and private key isolation (e.g., using containerization technologies or sandboxes).

If the DNS SVCB response is not DNSSEC protected, or if the client does not perform DNSSEC validation, an attacker can spoof the 'tlsdelegation' SvcParamKey in the DNS SVCB response. For instance, an attacker can spoof the DNS SVCB response to indicate that the server does not support delegate credentials. To mitigate this attack, the client can provide the extension in its ClientHello indicating support for delegated credentials, irrespective of whether the 'tlsdelegation' SvcParamKey is sent in the DNS SVCB response or not.

8. IANA Considerations

This document adds the following entry to the SVCB Service Parameters registry ([IANA-SVCB]).

```
Number: TBD
Name:   tlsdelegation
Meaning: DNS server can be authenticated using delegation
         credentails
Reference: (this document)
```

9. Acknowledgements

Thanks to Neil Cook, Martin Thomson, Tommy Pauly, Benjamin Schwartz and Michael Richardson for the discussion and comments. .

10. References

10.1. Normative References

[I-D.ietf-add-ddr]
Pauly, T., Kinnear, E., Wood, C. A., McManus, P., and T. Jensen, "Discovery of Designated Resolvers", Work in Progress, Internet-Draft, draft-ietf-add-ddr-10, 5 August 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-add-ddr-10>.

[I-D.ietf-add-dnr] Boucadair, M., Reddy.K, T., Wing, D., Cook, N., and T. Jensen, "DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)", Work in Progress, Internet-Draft, draft-ietf-add-dnr-16, 27 April 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-add-dnr-16>.

[I-D.ietf-add-svcb-dns]
Schwartz, B. M., "Service Binding Mapping for DNS Servers", Work in Progress, Internet-Draft, draft-ietf-add-svcb-dns-09, 26 June 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-add-svcb-dns-09>.

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

[RFC9345] Barnes, R., Iyengar, S., Sullivan, N., and E. Rescorla, "Delegated Credentials for TLS and DTLS", RFC 9345, DOI 10.17487/RFC9345, July 2023, <https://www.rfc-editor.org/info/rfc9345>.

10.2. Informative References

[IANA-SVCB] "IANA Service Binding (SVCB)", <https://www.iana.org/assignments/dns-svcb/dns-svcb.xhtml>.

[KEYLESS] "Sullivan, N. and D. Stebila, "An Analysis of TLS Handshake Proxying", IEEE Trustcom/BigDataSE/ISPA 2015 , 2015", December 2018.

[openwrt] "OpenWrt", <https://openwrt.org/>.

[prpl] "Prpl Foundation", <https://prplfoundation.org/>.

[prplwrt] "Prpl WRT", <https://prplfoundation.org/project/prplwrt/>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., and E. Lear, "Address Allocation for Private

Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/info/rfc1918>.

[RFC4192] Baker, F., Lear, E., and R. Droms, "Procedures for Renumbering an IPv6 Network without a Flag Day", RFC 4192, DOI 10.17487/RFC4192, September 2005, <https://www.rfc-editor.org/info/rfc4192>.

[RFC6598] Weil, J., Kuarsingh, V., Donley, C., Liljenstolpe, C., and M. Azinger, "IANA-Reserved IPv4 Prefix for Shared Address Space", BCP 153, RFC 6598, DOI 10.17487/RFC6598, April 2012, <https://www.rfc-editor.org/info/rfc6598>.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013, <https://www.rfc-editor.org/info/rfc6762>.

[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>.

[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>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/info/rfc8032>.

[RFC8190] Bonica, R., Cotton, M., Haberman, B., and L. Vegoda, "Updates to the Special-Purpose IP Address Registries", BCP 153, RFC 8190, DOI 10.17487/RFC8190, June 2017, <https://www.rfc-editor.org/info/rfc8190>.

[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>.

[RFC8520] Lear, E., Droms, R., and D. Romascanu, "Manufacturer Usage Description Specification", RFC 8520, DOI 10.17487/RFC8520, March 2019, <https://www.rfc-editor.org/info/rfc8520>.

[RFC8555] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", RFC 8555, DOI 10.17487/RFC8555, March 2019, <https://www.rfc-editor.org/info/rfc8555>.

[RFC8585] Palet Martinez, J., Liu, H. M.-H., and M. Kawashima, "Requirements for IPv6 Customer Edge Routers to Support IPv4-as-a-Service", RFC 8585, DOI 10.17487/RFC8585, May 2019, <https://www.rfc-editor.org/info/rfc8585>.

[RFC8739] Sheffer, Y., Lopez, D., Gonzalez de Dios, O., Pastor Perales, A., and T. Fossati, "Support for Short-Term, Automatically Renewed (STAR) Certificates in the Automated Certificate Management Environment (ACME)", RFC 8739, DOI 10.17487/RFC8739, March 2020, <https://www.rfc-editor.org/info/rfc8739>.

[RFC9115] Sheffer, Y., López, D., Pastor Perales, A., and T. Fossati, "An Automatic Certificate Management Environment (ACME) Profile for Generating Delegated Certificates", RFC 9115, DOI 10.17487/RFC9115, September 2021, <https://www.rfc-editor.org/info/rfc9115>.

[RFC9250] Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/RFC9250, May 2022, <https://www.rfc-editor.org/info/rfc9250>.

[TR-069] The Broadband Forum, "CPE WAN Management Protocol", December 2018, <https://www.broadband-forum.org/technical/download/TR-069.pdf>.

Authors' Addresses

Tirumaleswar Reddy
Nokia
India

Email: kondtir@gmail.com

Mohamed Boucadair
Orange
35000 Rennes
France

Email: mohamed.boucadair@orange.com

Dan Wing
Citrix Systems, Inc.

United States of America

Email: dwing-ietf@fuggles.com

Shashank Jain
McAfee
India

Email: Shashank_Jain@mcafee.com