Automated Certificate Management Environment
Internet-Draft
Intended status: Informational
Expires: 29 August 2025

R. Li
H. Wang
Z. Lei
Huawei Int. Pte Ltd

25 February 2025

Secure DNS RR Update for ACME DNS Based Challenges
draft-li-acme-dns-update-00

Abstract

This document outlines how ACME DNS based challenges can be performed via DNS dynamic updates.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-li-acme-dns-update/.

Discussion of this document takes place on the WG Working Group mailing list (mailto:acme@ietf.org), which is archived at https://datatracker.ietf.org/wg/acme/about/. Subscribe at https://www.ietf.org/mailman/listinfo/acme/.

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 29 August 2025.

Copyright Notice

Table of Contents

1. Introduction 3
2. Requirements Language 3
3. Terminology 3
4. General Architecture 4
5. Use Cases 4
5.1. Cloud Computing 4
5.2. 5G Core Network 5
6. Procedure Overview 5
7. Maintenance Functions 7
8. Certificate Issuance Procedure 7
8.1. Initial Authentication Key 7
8.2. Transaction Key Establishment 7
8.2.1. TSIG Transaction Key Establishment 8
8.3. Domain Control Validation 8
8.3.1. ACME Client Performs DNS Update 8
8.3.2. ACME Challenges 8
9. Access Control for Authentication Keys 8
9.1. DCV Update Permissioning 8
9.2. Transaction Key Establishment Permissioning 9
10. Security Considerations 9
11. Operational Considerations 10
12. IANA Considerations 10
13. References 10
13.1. Normative References 10
13.2. Informative References 12
Appendix A. Example DNS Authoritative Nameserver Configurations 13
A.1. BIND9 13
Authors' Addresses 14

1. Introduction

The ACME protocol [RFC8555] provides a means to automate certificate issuance that allows a CA/RA to verify that a client has control of identifiers in the requested certificate via domain control validation (DCV) challenges. For DNS [RFC1035] identifiers, dns-01 challenge specified in [RFC8555] and dns-account-01 challenges specified in [I-D.ietf-acme-dns-account-label] require the client to create a DNS resource record (RR) on the authoritative nameserver under the domain "<challenge-specific-label>.<domain-to-validate>" to prove control of the domain in the DNS identifier. However, the procedure to update DNS records is not specified.

[RFC2136] defines the DNS UPDATE message which instructs an authoritative nameserver to add or delete RRs or RRsets from a specified zone. It can further be secured using a message authentication code (MAC) in a TSIG RR [RFC8945]. To set up the shared key used for the TSIG RR, [RFC2930] specifies the TKEY RR which can be used to establish or delete this shared secret, where the message that carries the TKEY RR needs to be authenticated using TSIG with a previously established secret or SIG(0) [RFC2931].

This document outlines how an ACME client can perform DNS resource record updates to complete ACME DNS based challenges automatically, and how to do so securely via authenticated DNS update messages. The procedures defined in this document are designed to facilitate implementation and bridge the gap in [RFC8555].

[[Comment: [RFC2930] is being updated at [I-D.eastlake-dnsop-rfc2930bis-tkey]. Relevant sections in this document will be updated if this draft is accepted.]]

2. Requirements Language

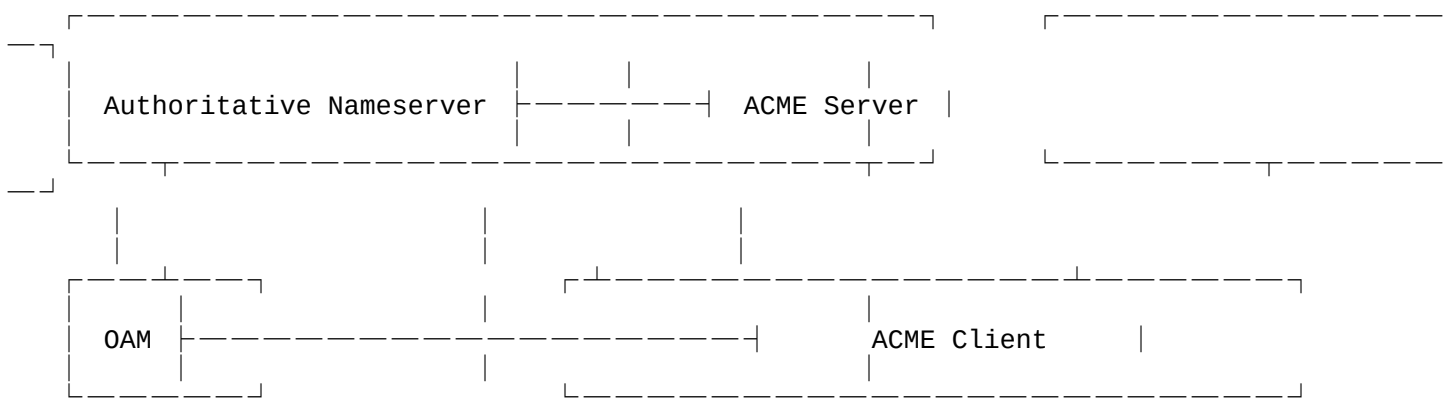
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Terminology

* *OAM* (or *O&M*): Operations and management, as per [BCP161] (RFC6291), an entity or system that is responsible for management of resources in a network.

4. General Architecture

OAM is responsible for configuration of ACME clients in a network. OAM first configures a domain name and an initial authentication key for the ACME client, and sets relevant resource records and access control settings on the authoritative nameserver [RFC9499]. The ACME client then applies for a certificate for that domain name from the ACME server through ACME protocol with DNS-based challenges that requires configuring certain DNS records. The ACME client completes a challenge by establishing a transaction key using the initial authentication key, and then provision the required resource records on the authoritative nameserver, authenticated using the transaction key. The ACME server then fetches the resource records to validate the challenge, and proceeds with certificate issuance.



It is assumed that the ACME client and the authoritative nameserver can be managed by OAM (i.e. OAM is capable of and authorized for configuring the ACME client and the authoritative nameserver).

5. Use Cases

The procedures outlined in this document provide a standardized way for ACME clients to respond to DNS based challenges. They can be applied to scenarios where clients use DNS based challenges to apply for certificates via ACME. They are especially useful if there are a large number of clients from different vendors.

5.1. Cloud Computing

In a typical cloud environment, there can be hundreds or even thousands of entities (applications, servers, etc.) that require certificates, and certificates often need to be renewed or replaced. Managing these certificates manually is error-prone, time-consuming, and can lead to security vulnerabilities and operational inefficiencies. Therefore, the cloud environment could benefit from

ACME which allows each entity to apply for its own certificate automatically. DNS based ACME Challenges cam be used for entities that do not act as web servers.

5.2. 5G Core Network

The 5G core networks are service-based and consist of network functions (NFs) that communicate with one another via TLS connections, authenticated using X.509 (PKIX) certificates [RFC5280]. Since NFs in a 5G network may come from different vendors, they could benefit from a standardized certificate management protocol such as ACME [TR33.876]. While ACME has proved to be very effective for the web, special considerations are needed if we want to deploy it in 5G networks which have more constraints. Section 5 of [TR33.776] outlines some key issues regarding application of ACME in a 5G system. Notably, 5.1 ACME initial trust framework and 5.3 Aspects of challenge validation point out that there is a need to define procedures for an NF to follow when proving its identity to ACME servers.

Similar to the cloud scenario, some 5G NFs are consumer NFs that do not expose web servers. They can therefore benefit from DNS based ACME challenges that do not require setting up a web server.

6. Procedure Overview

Assumptions:

1. OAM has pre-established trust relationship with the authoritative nameserver, so that it is able to update DNS records and configurations of the authoritative nameserver. This can be carried out through DNS UPDATE messages authenticated with TSIG [RFC8945].

2. OAM can securely perform certain maintenance operations on target ACME clients and the authoritative nameserver. See Section 7.

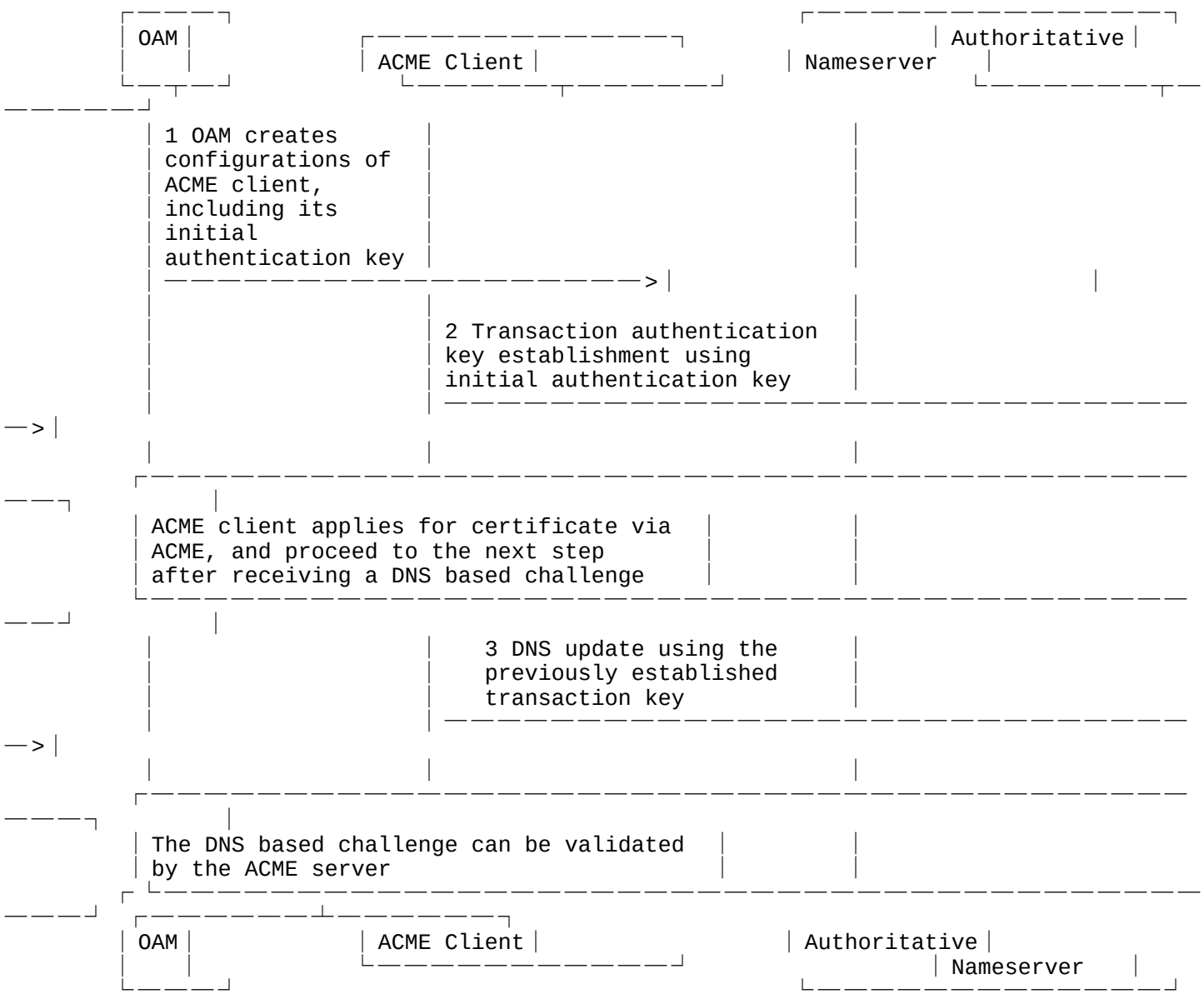
3. The authoritative nameserver is accessible by the CA/RA/ACME server.

General Procedure:

1. OAM configures an initial TSIG authentication key on the ACME client for authenticating it against the authoritative nameserver on which ACME DCV DNS records are hosted. OAM also registers the initial authentication key on the authoritative nameserver and configures its permissions.

2. The ACME client uses initial authentication parameters to establish a transaction key for TSIG [RFC8945] with the authoritative nameserver via TKEY [RFC2930]; or the ACME client uses the initial authentication key as the transaction key.

3. The ACME client uses the transaction key to authenticate its DNS UPDATE [RFC2136] message that configures an ACME DCV DNS record.



7. Maintenance Functions

In order to set up initial authentication keys for ACME clients that apply for certificates to be authenticated by the authoritative nameserver, the ACME clients and the authoritative nameserver need to support certain maintenance operations from the OAM system.

For ACME clients:

* Adjusting configurations (authoritative nameserver address, ACME server address, etc.)

* OAM to generate the symmetric TSIG key and configure it on the ACME client

For the authoritative nameserver:

* Adjusting configurations (TSIG key, etc.)

* Updating DNS records (editing zone files)

8. Certificate Issuance Procedure

8.1. Initial Authentication Key

OAM configures the target ACME client’s initial authentication key, and configures the corresponding parameters on the authoritative nameserver, so that the authoritative nameserver can verify the identity of the ACME client.

1. OAM generates a TSIG secret key for the ACME client

2. OAM configures the ACME client’s domain name and TSIG secret key

3. OAM provisions the TSIG secret key to the authoritative nameserver

8.2. Transaction Key Establishment

After setting up the initial authentication key, the ACME client possesses a key that can be used to authenticate DNS messages sent to the authoritative nameserver. However, using the same key over a long period of time may not be desirable. It is therefore RECOMMENDED to establish a separate TSIG transaction key for this purpose. The transaction key can be safely deleted after use or after a short period of time.

Although NOT RECOMMENDED, the ACME client can use the initial authentication key as the transaction key, if key establishment methods specified here or access control settings in Section 9 are not supported by the authoritative nameserver.

8.2.1. TSIG Transaction Key Establishment

The ACME client can establish a TSIG transaction key with the authoritative nameserver through a TKEY exchange [RFC2930].

Note that the TKEY RR provides an inception field and an expiration field that define a validity interval for the TSIG key to be established. It is RECOMMENDED to set a short interval (within a day) so that the key can be safely discarded afterwards.

8.3. Domain Control Validation

8.3.1. ACME Client Performs DNS Update

The ACME client updates ACME DCV DNS records using DNS UPDATE messages [RFC2136]. Transactional security is to be applied to DNS UPDATE messages via TSIG, using a key established in previous steps.

This work follows [RFC3007] to authenticate DNS UPDATE messages.

8.3.2. ACME Challenges

The DNS update method specified in this document supports dns-01 from [RFC8555], dns-account-01 from [I-D.ietf-acme-dns-account-label] and other DNS based challenges.

9. Access Control for Authentication Keys

The authoritative nameserver MUST be pre-configured for fine-grained access control for TSIG keys used for DCV and/or transaction key establishment. This section specifies how DCV update keys and transaction key establishment keys are to be configured.

9.1. DCV Update Permissioning

The authoritative nameserver SHALL implement fine-grained permissioning to only allow each ACME client’s transactional TSIG keys to be used for updating ACME DCV DNS records relevant to the ACME client’s assigned domain.

As an example, the authoritative nameserver MAY be configured to allow keys under domains with a format of _acme-dns-key.<domain-to-validate>[.<tkey-domain>] to be used to UPDATE (add or remove) one or many of the DCV DNS records below:

* TXT records under _acme-challenge.<domain-to-validate> (dns-01)

* TXT records under _*._acme-challenge.<domain-to-validate> (dns-account-01)

Note that the authoritative nameserver MAY also verify that the wildcard in the domain name above is a valid base32 encoded string.

9.2. Transaction Key Establishment Permissioning

When using TKEY RR to establish transactional TSIG keys, the key used for authenticating the key establishment SHALL only be allowed to perform key establishment for specific domains (key ids).

As an example, the authoritative nameserver MAY be configured to allow keys under domains with a format of _key-exchange-key.<key-domain>[.<tkey-domain>] to be used to establish the following transaction keys:

* TSIG key under _acme-dns-key.<key-domain>.<tkey-domain>, established via a TKEY RR

10. Security Considerations

DNS Updates via UDP messages are sent in plaintext, which may be vulnerable to eavesdropping and tampering. This can be mitigated by using DoT [RFC7858] or DoH [RFC8484].

The TSIG authentication mechanism incorporates a validity period, which is set by the client and verified by the server, to defend against replay attack. However, DNS update requests, even using TSIG for authentication, are not idempotent, and therefore a replay attack is possible within the validity period. This can be avoided by using marker RRs in the Update request, as per section 5 of [RFC2136]. Alternatively, DoT or DoH can be used so that the request can be protected by TLS.

As per Section 9, the initial authentication keys and transaction authentication keys should be configured with fine-grained permission control to prevent access to unauthorized resources.

When establishing transactional TSIG keys via TKEY, it is RECOMMENDED to set a short validity interval (e.g., within a day), and use each transactional TSIG key only once or for a short period of time.

This work follows recommendations set out in [I-D.ietf-dnsop-domain-verification-techniques] by integrating challenge types proposed in [I-D.ietf-acme-dns-account-label].

11. Operational Considerations

1. ACME clients SHOULD clean up DCV DNS records once the respective ACME challenges are completed, i.e., once the "status" field of the challenge is "valid" or "invalid".

2. ACME clients SHOULD delete transactional TSIG keys stored on the authoritative nameserver after use (via TKEY RRs).

12. IANA Considerations

This document has no IANA actions.

13. References

13.1. Normative References

[BCP161] Best Current Practice 161, <https://www.rfc-editor.org/info/bcp161>. At the time of writing, this BCP comprises the following:

Andersson, L., van Helvoort, H., Bonica, R., Romascanu, D., and S. Mansfield, "Guidelines for the Use of the "OAM" Acronym in the IETF", BCP 161, RFC 6291, DOI 10.17487/RFC6291, June 2011, <https://www.rfc-editor.org/info/rfc6291>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/rfc/rfc1035>.

[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>.

[RFC2136] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, DOI 10.17487/RFC2136, April 1997, <https://www.rfc-editor.org/rfc/rfc2136>.

[RFC2930] Eastlake 3rd, D., "Secret Key Establishment for DNS (TKEY RR)", RFC 2930, DOI 10.17487/RFC2930, September 2000, <https://www.rfc-editor.org/rfc/rfc2930>.

[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>.

[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/rfc/rfc7858>.

[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>.

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

[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/rfc/rfc8555>.

[RFC8945] Dupont, F., Morris, S., Vixie, P., Eastlake 3rd, D., Gudmundsson, O., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", STD 93, RFC 8945, DOI 10.17487/RFC8945, November 2020, <https://www.rfc-editor.org/rfc/rfc8945>.

[I-D.eastlake-dnsop-rfc2930bis-tkey] Eastlake, D. E. and M. P. Andrews, "Secret Key Agreement for DNS: The TKEY Resource Record", Work in Progress, Internet-Draft, draft-eastlake-dnsop-rfc2930bis-tkey-01, 21 October 2024, <https://datatracker.ietf.org/doc/html/draft-eastlake-dnsop-rfc2930bis-tkey-01>.

[I-D.ietf-acme-dns-account-label]
Chariton, A., Omidi, A., Kasten, J., Loukos, F., and S. A. Janikowski, "Automated Certificate Management Environment (ACME) DNS Labeled With ACME Account ID Challenge", Work in Progress, Internet-Draft, draft-ietf-acme-dns-account-label-00, 13 November 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-acme-dns-account-label-00>.

13.2. Informative References

[RFC2931] Eastlake 3rd, D., "DNS Request and Transaction Signatures (SIG(0)s)", RFC 2931, DOI 10.17487/RFC2931, September 2000, <https://www.rfc-editor.org/rfc/rfc2931>.

[RFC3007] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, DOI 10.17487/RFC3007, November 2000, <https://www.rfc-editor.org/rfc/rfc3007>.

[RFC8792] Watsen, K., Auerswald, E., Farrel, A., and Q. Wu, "Handling Long Lines in Content of Internet-Drafts and RFCs", RFC 8792, DOI 10.17487/RFC8792, June 2020, <https://www.rfc-editor.org/rfc/rfc8792>.

[RFC9499] Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219, RFC 9499, DOI 10.17487/RFC9499, March 2024, <https://www.rfc-editor.org/rfc/rfc9499>.

[I-D.ietf-dnsop-domain-verification-techniques]
Sahib, S. K., Huque, S., Wouters, P., and E. Nygren, "Domain Control Validation using DNS", Work in Progress, Internet-Draft, draft-ietf-dnsop-domain-verification-techniques-06, 21 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-domain-verification-techniques-06>.

[TR33.776] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Study of Automatic Certificate Management Environment (ACME) for the Service Based Architecture (SBA) (Release 19)", 3GPP TS:33.776 V0.3.0, May 2024, <https://www.3gpp.org/ftp/Specs/archive/33_series/33.776/33776-030.zip>.

[TR33.876] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Study on automated certificate management in Service-Based Architecture (SBA) (Release 18)", 3GPP TS:33.876 V18.0.1, July 2023, <https://www.3gpp.org/ftp/Specs/archive/33_series/33.876/33876-i01.zip>.

Appendix A. Example DNS Authoritative Nameserver Configurations

Note: '\' line wrapping per [RFC8792].

A.1. BIND9

In BIND9, TSIG keys, while not stored in DNS, also have FQDNs as key names.

In the named configuration file, a zone can be configured to support [RFC2136] updates using a key identified by an FQDN using the update-policy statement.

Note that it is not possible to configure BIND9 to support the general access control strategy specified in Section 9.1, because each zone to be updated needs to be configured explicitly.

Command to generate TSIG key for f9657a41-610c-414a-828a-fc88250f9165.amf.tsig.:

```
tsig-keygen -a HMAC-SHA512 f9657a41-610c-414a-828a-fc88250f9165.am\
f.tsig.
```

Example named configuration that grants the key permission to update TXT records for *.f9657a41-610c-414a-828a-fc88250f9165.amf.5gc.mnc001.mcc001.3gppnetwork.org.:

```
   //named.conf

   key "f9657a41-610c-414a-828a-fc88250f9165.amf.tsig." {
       algorithm hmac-sha512;
       secret "MhKYgOU+mb1nLegdky3zPydpIFlhhBD4ic9WcjbCBLHFh+Rb+my8of\
       1pGcChMBfiWrnLdn0lnmL1t4iTMb4LNw==";
   };

   zone "5gc.mnc001.mcc001.3gppnetwork.org." {
       type primary;
       update-policy {
           grant f9657a41-610c-414a-828a-fc88250f9165.amf.tsig. wildc\
           ard *.f9657a41-610c-414a-828a-fc88250f9165.amf.5gc.mnc001.\
           mcc001.3gppnetwork.org. TXT;
       };
   }
```

Authors' Addresses

Ruochen Li
Huawei Int. Pte Ltd
Singapore
Email: li.ruochen@huawei.com

Haiguang Wang
Huawei Int. Pte Ltd
Singapore
Email: wang.haiguang.shieldlab@huawei.com

Zhongding Lei
Huawei Int. Pte Ltd
Singapore
Email: lei.zhongding@huawei.com