Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 24 February 2026

M. L. Bihan
August 2025

Automated Certificate Management Environment (ACME) SRV Identifier Validation Extension

draft-lebihan-srv-identifier-validation-extension-00

Abstract

This document specifies an extension to the Automated Certificate Management Environment (ACME) protocol to enable validation and issuance of certificates containing SRV-ID identifiers as defined in RFC 4985. This allows secure delegation of services where the service domain and hosting infrastructure are controlled by different entities, addressing the multi-tenancy challenges in protocols that use SRV records for service discovery.

About This Document

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

The latest revision of this draft can be found at https://mimi89999.github.io/srv-identifier-validation-extension/draft-lebihan-srv-identifier-validation-extension.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-lebihan-srv-identifier-validation-extension/.

Source for this draft and an issue tracker can be found at https://github.com/mimi89999/srv-identifier-validation-extension.

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 2 February 2026.

Table of Contents

1. Introduction

Many application protocols can use DNS SRV records [RFC2782] for service discovery and delegation to third-party hosting providers. Organizations often wish to maintain their domain identity (e.g., example.com) while delegating the actual service hosting to specialized providers.

Currently, obtaining proper PKIX certificates for such delegated services presents significant operational challenges. The hosting provider cannot easily obtain certificates for the customer's domain without either:

* Access to the customer's DNS infrastructure for validation

* Access to the customer's web server for HTTP validation

* The customer obtaining certificates and sharing private keys

These approaches are either operationally infeasible, introduce security risks, or do not scale effectively in multi-tenant environments.

This document extends ACME [RFC8555] to support SRV-ID identifiers [RFC4985], enabling hosting providers to obtain certificates that properly identify delegated services without requiring control over the source domain's infrastructure.

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 uses the following terms:

Source Domain: The domain that owns the service identity (e.g., example.com in _myservice.example.com)

Target Domain: The domain providing the actual service hosting (e.g., hosting.example.net)

SRV-ID: An identifier type defined in [RFC4985] representing a service-specific identity

3. Problem Statement

Consider an organization using example.com that wishes to delegate multiple services to different providers:

* Service A to provider-a.example

* Service B to provider-b.example

* Service C to provider-c.example

These services might be discovered via SRV records such as:

```
_service-a._tcp.example.com. 86400 IN SRV 0 5 5001 provider-a.example.
_service-b._tcp.example.com. 86400 IN SRV 0 5 5002 provider-b.example.
_service-c._tcp.example.com. 86400 IN SRV 0 5 5003 provider-c.example.
```

Without DNSSEC (which has limited deployment), these delegations are vulnerable to DNS spoofing attacks. Current ACME validation methods cannot be used by the hosting providers to obtain certificates for example.com without coordination that is often impractical.

Existing approaches have significant limitations:

* *DANE [RFC6698]*: Requires DNSSEC deployment, which remains limited across many TLDs and registrars

* *POSH [RFC7711]*: Requires placing files in .well-known on the source domain's web server. If that web server is compromised (e.g., through a CMS vulnerability), an attacker could modify the POSH files

* *dns-account-01 [I-D.ietf-acme-dns-account-label]*: While this challenge type allows multiple providers to independently validate the same domain through unique DNS labels, it ties the validation to a specific ACME account URL that includes the CA endpoint. This creates operational inflexibility: if a hosting provider needs to switch CAs (due to rate limits, outages, pricing changes, or other operational reasons), every customer would need to update their DNS records to reflect the new account URL. This requirement is impractical at scale and effectively locks providers into a single CA

* *Certificate sharing*: Requires distributing private keys between organizations, creating security and operational concerns

4. SRV Identifier Type

This document defines a new ACME identifier type "srv" for use in authorization objects.

An SRV identifier object has the following fields:

type (required, string): The string "srv"

value (required, string): The SRVName as defined in [RFC4985], in

the format "_service.domain". MUST begin with an underscore followed by the service name, then a dot, then the domain name. This format corresponds to the SRVName structure in [RFC4985] Section 2, which omits the protocol component found in DNS SRV records.

Example identifier object:

```
{
  "type": "srv",
  "value": "_myservice.example.com"
}
```

5. Identifier Validation Challenges

SRV identifiers MUST be validated using the dns-01 challenge type as defined in [RFC8555] Section 8.4, with the following modification:

When validating an SRV identifier, the challenge TXT record MUST be provisioned under the service name rather than the base domain. Specifically:

1. The client constructs the validation domain name by prepending "_acme-challenge." to the SRV identifier value.

2. For an SRV identifier "_myservice.example.com", the resulting validation domain would be: "_acme-challenge._myservice.example.com"

3. The client provisions a TXT record at this location containing the base64url encoding of the SHA-256 digest of the key authorization, as specified in the standard dns-01 challenge.

The server performs validation by:

1. Computing the SHA-256 digest of the stored key authorization

2. Querying for TXT records at the validation domain name constructed from the SRV identifier

3. Verifying that the contents of one of the TXT records matches the digest value

HTTP-01 and other challenge types MUST NOT be used for SRV identifier validation, as they cannot properly demonstrate control of a service-specific identifier.

6. Validation Process

The validation flow is:

1. Client creates a newOrder request with an SRV identifier

2. Server creates authorization with dns-01 challenge

3. Client provisions DNS TXT record at the service-specific location

4. Server validates the dns-01 challenge

5. Upon successful validation, server issues certificate containing the SRV-ID from the original identifier value

The issued certificate MUST contain the SRV-ID in the subjectAltName extension as specified in [RFC4985], using the id-on-dnsSRV form.

The issued certificate MUST NOT include a Common Name (CN) in the subject field. Placing a SRVName in the CN field could lead to interpretation issues with software interpreting the SRVName in the CN field as a standard domain name.

7. Security Considerations

7.1. DNS Security

This mechanism relies on the integrity of DNS SRV records. In the absence of DNSSEC, it is vulnerable to DNS spoofing attacks. ACME servers SHOULD:

* Use DNSSEC-validating resolvers where possible

* Perform validation from multiple network vantage points

* Apply similar mitigations as for standard DNS-based validation

7.2. Scope of Authorization

Unlike certificates with DNS-ID identifiers, certificates with SRV-ID identifiers are restricted to the specific service. This provides better isolation in multi-tenant environments where different services are hosted by different providers. A certificate for "_service-a.example.com" cannot be used to impersonate "_service-b.example.com" or the base domain example.com.

7.3. Client Support

Clients MUST properly validate SRV-ID certificates and not accept them as valid for general DNS names. Protocol specifications using this extension SHOULD clearly define certificate validation requirements.

8. IANA Considerations

8.1. ACME Identifier Types

IANA is requested to add the following entry to the "ACME Identifier Types" registry:

Label	Reference
srv	RFC XXXX

Table 1

8.2. ACME Validation Methods

IANA is requested to add the following entry to the "ACME Validation Methods" registry:

Label	Identifier Type	ACME	Reference
dns-01	srv	Y	RFC XXXX

Table 2

9. References

9.1. 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>.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, DOI 10.17487/RFC2782, February 2000, <https://www.rfc-editor.org/rfc/rfc2782>.

[RFC4985] Santesson, S., "Internet X.509 Public Key Infrastructure Subject Alternative Name for Expression of Service Name", RFC 4985, DOI 10.17487/RFC4985, August 2007, <https://www.rfc-editor.org/rfc/rfc4985>.

[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>.

[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>.

9.2. Informative References

[I-D.ietf-acme-dns-account-label] Chariton, A., "Automated Certificate Management Environment (ACME) DNS Labeled With ACME Account ID Challenge", Work in Progress, Internet-Draft, draft-ietf-acme-dns-account-label-01, May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-acme-dns-account-label-01>.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012, <https://www.rfc-editor.org/rfc/rfc6698>.

[RFC7711] Miller, M. and P. Saint-Andre, "PKIX over Secure HTTP (POSH)", RFC 7711, DOI 10.17487/RFC7711, November 2015, <https://www.rfc-editor.org/rfc/rfc7711>.

Acknowledgments

Author’s Address

Michel Le Bihan
Email: michel@lebihan.pl