ACME Working Group                                          R. Shoemaker
Internet-Draft                                                      ISRG
Intended status: Standards Track                        October 01, 2019
Expires: April 3, 2020

ACME IP Identifier Validation Extension
draft-ietf-acme-ip-08

Abstract

This document specifies identifiers and challenges required to enable
the Automated Certificate Management Environment (ACME) to issue
certificates for IP addresses.

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 April 3, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(https://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.
1. Introduction

The Automatic Certificate Management Environment (ACME) [RFC8555] only defines challenges for validating control of DNS host name identifiers, which limits its use to being used for issuing certificates for DNS identifiers. In order to allow validation of IPv4 and IPv6 addresses for inclusion in X.509 certificates, this document specifies how challenges defined in the original ACME specification and the TLS-ALPN extension specification [I-D.ietf-acme-tls-alpn] can be used to validate IP identifiers.

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.

3. IP Identifier

[RFC8555] only defines the identifier type "dns", which is used to refer to fully qualified domain names. If an ACME server wishes to request proof that a user controls an IPv4 or IPv6 address, it MUST create an authorization with the identifier type "ip". The value field of the identifier MUST contain the textual form of the address as defined in [RFC1123] Section 2.1 for IPv4 and in [RFC5952] Section 4 for IPv6.
An identifier for the IPv6 address 2001:db8::1 would be formatted like so:

{"type": "ip", "value": "2001:db8::1"}

4. Identifier Validation Challenges

IP identifiers MAY be used with the existing "http-01" (see Section 8.3 of [RFC8555]) and "tls-alpn-01" (see Section 3 of [I-D.ietf-acme-tls-alpn]). To use IP identifiers with these challenges, their initial DNS resolution step MUST be skipped, and the IP address used for validation MUST be the value of the identifier.

5. HTTP Challenge

For the "http-01" challenge, the Host header field MUST be set to the IP address being used for validation per [RFC7230]. The textual form of this address MUST be as defined in [RFC1123] Section 2.1 for IPv4 and in [RFC5952] Section 4 for IPv6.

6. TLS with Application Level Protocol Negotiation (TLS ALPN) Challenge

For the "tls-alpn-01" challenge, the subjectAltName extension in the validation certificate MUST contain a single iPAddress that matches the address being validated. As [RFC6066] does not permit IP addresses to be used in the SNI extension HostName field, the server MUST instead use the IN-ADDR.ARPA [RFC1034] or IP6.ARPA [RFC3596] reverse mapping of the IP address as the HostName field value instead of the IP address string representation itself. For example, if the IP address being validated is 2001:db8::1, the SNI HostName field should contain "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa".

7. DNS Challenge

The existing "dns-01" challenge MUST NOT be used to validate IP identifiers.

8. IANA Considerations

8.1. Identifier Types

Adds a new type to the "ACME Identifier Types" registry defined in Section 9.7.7 of [RFC8555] with Label "ip" and Reference "I-D.ietf-acme-ip".
8.2. Challenge Types

Adds two new entries to the "ACME Validation Methods" registry defined in Section 9.7.8 of [RFC8555]. These entries are defined below:

<table>
<thead>
<tr>
<th>Label</th>
<th>Identifier Type</th>
<th>ACME</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>http-01</td>
<td>ip</td>
<td>Y</td>
<td>I-D.ietf-acme-ip</td>
</tr>
<tr>
<td>tls-alpn-01</td>
<td>ip</td>
<td>Y</td>
<td>I-D.ietf-acme-ip</td>
</tr>
</tbody>
</table>

9. Security Considerations

The extensions to ACME described in this document do not deviate from the broader threat model described in [RFC8555] Section 10.1.

9.1. CA Policy Considerations

This document only specifies how an ACME server may validate that a certificate applicant controls a IP identifier at the time of validation. The CA may wish to perform additional checks not specified in this document. For example, if the CA believes an IP identifier belongs to an ISP or cloud service provider with short delegation periods, they may wish to impose additional restrictions on certificates requested for that identifier.

10. Acknowledgments

The author would like to thank those who contributed to this document and offered editorial and technical input, especially Jacob Hoffman-Andrews and Daniel McCarney.

11. Normative References

[I-D.ietf-acme-tls-alpn]


Author’s Address

Roland Bracewell Shoemaker
Internet Security Research Group

Email: roland@letsencrypt.org