ACME Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 28, 2019

R. Shoemaker
ISRG

July 27, 2018

ACME IP Identifier Validation Extension
draft-ietf-acme-ip-04

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 January 28, 2019.

Copyright Notice

Copyright (c) 2018 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.

Table of Contents

1. Introduction

The Automatic Certificate Management Environment (ACME) [I-D.ietf-acme-acme] 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 identifiers 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

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, [RFC2119].

3. IP Identifier

[I-D.ietf-acme-acme] only defines the identifier type "dns" which is used to refer to fully qualified domain names. If a ACME server wishes to request proof that a user controls a 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 [RFC4291] Section 2.2 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" and "tls-alpn-01" challenges from [I-D.ietf-acme-acme] Section 8.3 and [I-D.ietf-acme-tls-alpn] Section 3 respectively. 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.

For the "http-01" challenge the Host header MUST be set to the IP address being used for validation per [RFC7230].

For the "tls-alpn-01" the subjectAltName extension in the validation certificate MUST contain a single iPAddress which matches the address being validated. As [RFC6066] does not permit IP addresses to be used in the SNI extension the server MUST instead use the IN-ADDR.ARPA [RFC1034] or IP6.ARPA [RFC3596] reverse mapping of the IP address as the SNI value instead of the literal IP address.

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

5. IANA Considerations

5.1. Identifier Types

Adds a new type to the Identifier list defined in Section 9.7.7 of [I-D.ietf-acme-acme] with the label "ip" and reference I-D.ietf-acme-ip.

5.2. Challenge Types

Adds the value "ip" to the Identifier Type column in the Validation Methods list defined in Section 9.7.8 of [I-D.ietf-acme-acme] for the "http-01" and "tls-alpn-01" challenges.

6. Security Considerations

Given the often short delegation periods for IP addresses provided by various service providers CAs MAY want to impose shorter lifetimes for certificates which contain IP identifiers. They MAY also impose restrictions on IP identifiers which are in CIDRs known to be assigned to service providers who dynamically assign addresses to users for indeterminate periods of time.

7. 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.

8. Normative References

[FIPS180-4] Department of Commerce, National., "NIST FIPS 180-4, Secure Hash Standard", March 2012, <http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf>.

[I-D.ietf-acme-acme] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", draft-ietf-acme-acme-13 (work in progress), July 2018.

[I-D.ietf-acme-tls-alpn] Shoemaker, R., "ACME TLS ALPN Challenge Extension", draft-ietf-acme-tls-alpn-01 (work in progress), May 2018.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[RFC1123] Braden, R., Ed., "Requirements for Internet Hosts - Application and Support", STD 3, RFC 1123, DOI 10.17487/RFC1123, October 1989, <https://www.rfc-editor.org/info/rfc1123>.

[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>.

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", STD 88, RFC 3596, DOI 10.17487/RFC3596, October 2003, <https://www.rfc-editor.org/info/rfc3596>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/info/rfc4648>.

[RFC6066] Eastlake 3rd, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, DOI 10.17487/RFC6066, January 2011, <https://www.rfc-editor.org/info/rfc6066>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <https://www.rfc-editor.org/info/rfc7230>.

Author's Address

Roland Bracewell Shoemaker
Internet Security Research Group

Email: roland@letsencrypt.org