Stream: Internet Engineering Task Force (IETF)
RFC: 8738
Category: Standards Track
Published: February 2020
ISSN: 2070-1721
Author: R.B. Shoemaker
ISRG

RFC 8738
Automated Certificate Management Environment (ACME) IP Identifier Validation Extension

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 is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8738.

Copyright Notice

Table of Contents

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 identifiers for inclusion in X.509 certificates, this document specifies how challenges defined in the original ACME specification and the TLS-ALPN extension specification [RFC8737] 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 Section 2.1 of [RFC1123] for IPv4 and in Section 4 of [RFC5952] 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 [RFC8737]). 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 Section 2.1 of [RFC1123] for IPv4 and in Section 4 of [RFC5952] for IPv6.

6. TLS with Application-Layer 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 Server Name Indication (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

Per this document, a new type has been added to the "ACME Identifier Types" registry defined in Section 9.7.7 of [RFC8555] with Label "ip" and Reference "RFC 8738".

8.2. Challenge Types

Per this document, two new entries have been added to the "ACME Validation Methods" registry defined in Section 9.7.8 of [RFC8555]. These entries are defined below:

Label	Identifier Type	ACME	Reference
http-01	ip	Y	RFC 8738
tls-alpn-01	ip	Y	RFC 8738

Table 1

9. Security Considerations

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

9.1. Certification Authority (CA) Policy Considerations

This document only specifies how an ACME server may validate that a certificate applicant controls an 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. Normative References

[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>.

[RFC5952] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, DOI 10.17487/RFC5952, August 2010, <https://www.rfc-editor.org/info/rfc5952>.

[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>.

[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/info/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/info/rfc8555>.

[RFC8737] Shoemaker, R.B., "Automated Certificate Management Environment (ACME) TLS Application-Layer Protocol Negotiation (ALPN) Challenge Extension", RFC 8737, DOI 10.17487/RFC8737, February 2020, <https://www.rfc-editor.org/info/rfc8737>.

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.

Author's Address

Roland Bracewell Shoemaker
Internet Security Research Group
Email: roland@letsencrypt.org