ACME Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 17, 2018

R. Shoemaker
ISRG

July 16, 2017

ACME IP Identifier Validation Extension
draft-ietf-acme-ip-00

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 http://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 17, 2018.

Table of Contents

1. Introduction 2
2. Terminology 2
3. IP Identifier 2
4. Identifier Validation Challenges 3
4.1. Reverse DNS 3
4.2. Existing Challenges 5
5. IANA Considerations 5
5.1. Identifier Types 5
5.2. Challenge Types 5
6. Security Considerations 5
6.1. Certificate Lifetime 5
7. Normative References 6
Author's Address 7

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 these identifiers. In order to allow validation of IPv4 and IPv6 identifiers for inclusion in X.509 certificates this document defines a new challenge type and specifies how challenges defined in the original ACME specification 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, RFC 2119 [RFC2119] and indicate requirement levels for compliant ACME-Wildcard implementations.

3. IP Identifier

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 RFC 1123 [RFC1123] Section 2.1 for IPv4 and in RFC 4291 [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

When creating an authorization for a identifier with the type "ip" the following challenge types MAY be used to perform validation.

4.1. Reverse DNS

With Reverse DNS validation the client proves control of an IP address by provisioning a TXT resource record containing a designated value for a specific validation domain name constructed using the value of the PTR record for the reverse mapping of the address.

type (required, string): The string "reverse-dns-01".

token (required, string): A random value that uniquely identifies the challenge. This value MUST have at least 128 bits of entropy, in order to prevent an attacker from guessing it. It MUST NOT contain any characters outside the base64url [RFC4648] alphabet, including padding characters ("=").

```
GET /acme/authz/1234/2 HTTP/1.1
Host: example.com

HTTP/1.1 200 OK
{
  "type": "reverse-dns-01",
  "url": "https://example.com/acme/authz/1234/2",
  "status": "pending",
  "token": "evaGxfADs6pSRb2LAv9IZf17Dt3juxGJ-PCt92wr-oA"
}
```

A client responds to this challenge by constructing a key authorization from the "token" value provided in the challenge and the client's ACME account key. The client then computes the SHA-256 digest [FIPS180-4] of the key authorization. The record provisioned to the authoritative DNS server is the base64url encoding of this digest.

The client constructs the validation domain name by prepending the label "_acme-challenge" to the domain name referenced in the PTR resource record for the IN-ADDR.ARPA [RFC1034] or IP6.ARPA [RFC3596] reverse mapping of the IP address. The client then provisions a TXT record with the digest for this name.

For example, if the IP address being validated is 2001:db8::1 and its IP6.ARPA mapping had the following PTR record:

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa. 300 IN PTR example.com

then the client would provision the following DNS record:

_acme-challenge.example.com. 300 IN TXT "gfj9Xq...Rg85nM"

The response to the Reverse DNS challenge provides the computed key authorization to acknowledge that the client is ready to fulfill this challenge.

keyAuthorization (required, string): The key authorization for this challenge.

```
POST /acme/authz/1234/2
Host: example.com
Content-Type: application/jose+json

{
  "protected": base64url({
    "alg": "ES256",
    "kid": "https://example.com/acme/acct/1",
    "nonce": "JHb54aT_KTXBWQOzGYkt9A",
    "url": "https://example.com/acme/authz/1234/2"
  }),
  "payload": base64url({
    "keyAuthorization": "evaGxfADs...62jcerQ"
  }),
  "signature": "Q1bURgJoEslbD1c5...3pYdSMLio57mQNN4"
}
```

On receiving a response, the server MUST verify that the key authorization in the response matches the "token" value in the challenge and the client's ACME account key. If they do not match, then the server MUST return an HTTP error in response to the POST request in which the client sent the challenge.

To validate a DNS challenge, the server performs the following steps:

1. Compute the SHA-256 digest of the key authorization

2. Query for a PTR record for the IP identifiers relevant reverse mapping based on its version

3. Query for TXT records for the computed validation domain name

4. Verify that the contents of one of the TXT records matches the digest value

If all of the above verifications succeed, then the validation is successful. If no PTR or TXT DNS records are found, or the returned TXT records do not contain the expected key authorization digest, then the validation fails.

4.2. Existing Challenges

IP identifiers MAY be used with the existing "http-01" and "tls-sni-02" challenges from RFC XXXX Sections XXX and XXX respectively. To use IP identifiers with these challenges their initial DNS resolution step MUST be skipped and the address used for validation MUST be the value of the identifier. For the "http-01" challenge the Host header should be set to the IP address being used for validation per RFC 7230.

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 XXX of RFC XXXX with the label "ip" and reference RFC XXXX.

5.2. Challenge Types

Adds a new type to the Challenge list defined in Section XXX of RFC XXXX with the label "reverse-dns-01", identifier type "ip", and reference RFC XXXX.

Add the value "ip" to the identifier type column for the "http-01" and "tls-sni-02" challenges.

6. Security Considerations

6.1. Certificate Lifetime

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. 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., and J. Kasten, "Automatic Certificate Management Environment (ACME)", draft-ietf-acme-acme-07 (work in progress), June 2017.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <http://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, <http://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, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc4291>.

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

[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, <http://www.rfc-editor.org/info/rfc7230>.

Author's Address

Roland Bracewell Shoemaker
Internet Security Research Group

Email: roland@letsencrypt.org