Workgroup:
Automated Certificate Management Environment
Internet-Draft:
draft-todo-chariton-dns-account-01-02
Published: 10 November 2022
Intended Status: Standards Track
Expires: 14 May 2023
Authors: A. A. Chariton
Google
A. A. Omidi
Google
J. Kasten
Google
F. Loukos
Google
S. A. Janikowski
Google

Automated Certificate Management Environment (ACME) DNS Labeled With ACME Account ID Challenge

Abstract

This document specifies a new challenge type for the Automated Certificate Management Environment (ACME) protocol which allows an ACME client to respond to a domain control validation challenge presented by an ACME server with a DNS resource that is keyed by the ACME account identification.

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://daknob.github.io/draft-todo-chariton-dns-account-01/. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-todo-chariton-dns-account-01/.

Discussion of this document takes place on the WG Working Group mailing list (mailto:acme@ietf.org), which is archived at https://datatracker.ietf.org/wg/acme/about/. Subscribe at https://www.ietf.org/mailman/listinfo/acme/.

Source for this draft and an issue tracker can be found at https://github.com/daknob/draft-todo-chariton-dns-account-01.

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 14 May 2023.

Table of Contents

1. Introduction

The dns-01 challenge specified in section 8.4 of [RFC8555] requires that ACME clients validate the domain under the _acme-challenge label for the TXT record. This unique label creates an impediment limiting the number of other entities domain validation can be delegated to.

This document specifies a new challenge type, dns-account-01. This challenge leverages the ACME Account Resource URL to present an account-unique stable challenge to an ACME server. This challenge allows any domain name to delegate its domain validation to more than one service through ACME account-unique DNS records.

This RFC does not intend to deprecate the dns-01 challenge specified in [RFC8555]. Since this new challenge does not modify or build on any pre-existing challenges, the ability to complete the dns-account-01 challenge requires ACME server operators to deploy new changes to their codebase. This makes adopting and using this challenge an opt-in process.

2. Conventions and Definitions

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. DNS-ACCOUNT-01 Challenge

When the identifier being validated is a domain name, the client can prove control of that domain by provisioning a TXT resource record containing a designated value for a specific validation domain name.

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

- *token (required, string): A random value that uniquely identifies the challenge. This value **MUST** have at least 128 bits of entropy. It **MUST NOT** contain any characters outside the base64url alphabet, including padding characters ("="). See [RFC4086] for additional information on additional requirements for secure randomness.

```
{
  "type": "dns-account-01",
  "url": "https://example.com/acme/chall/i00MGYwLWIx",
  "status": "pending",
  "token": "ODE4OWY4NTktYjhmYS00YmY1LTk5MDgtZTFjYTZmNjZlYTUx"
}
```

A client can fulfill this challenge by performing the following steps:

- *Construct a key authorization from the token value provided in the challenge and the client's account key

- *Compute the SHA-256 digest [FIPS180-4] of the key authorization

- *Construct the validation domain name by prepending the following label to the domain name being validated:

"_acme-challenge_" || base32(SHA-256(Account Resource URL)[0:9])

-SHA-256 is the SHA hashing operation defined in [RFC6234]

-[0:9] is the operation that selects the first ten bytes (bytes 0 through 9 inclusive) from the previous SHA256 operation

-base32 is the operation defined in [RFC4648]

-Account Resource URL is defined in [RFC8555], Section 7.3 as the value in the Location header field

-The "||" operator indicates concatenation of strings

*Provision a DNS TXT record with the base64url digest value under the constructed domain validation name

For example, if the domain name being validated is "www.example.org", and the account URL of "https://example.com/acme/acct/ExampleAccount" then the client would provision the following DNS record:

```
_acme-challenge_ujmmovf2vn55tgye.www.example.org 300 IN TXT "LoqXcYV8...
```

(In the above, "..." indicates that the token and the JWK thumbprint in the key authorization have been truncated to fit on the page.)

Respond to the ACME server with an empty object ({}) to acknowledge that the challenge can be validated by the server

```
POST /acme/chall/Rg5dV14Gh1Q
Host: example.com
Content-Type: application/jose+json

{
  "protected": base64url({
    "alg": "ES256",
    "kid": "https://example.com/acme/acct/evOfKhNU60wg",
    "nonce": "SS2sSl1PtspvFZ08kNtzKd",
    "url": "https://example.com/acme/chall/Rg5dV14Gh1Q"
  }),
  "payload": base64url({}),
  "signature": "Q1bURgJoEslbD1c5...3pYdSMLio57mQNN4"
}
```

On receiving a response, the server constructs and stores the key authorization from the challenge token value and the current client account key.

To validate the dns-account-01 challenge, the server performs the following steps:

- Compute the SHA-256 digest [FIPS180-4] of the stored key authorization
- Compute the validation domain name with the account URL of the ACME account requesting validation
- Query for TXT records for the validation domain name
- Verify that the contents of one of the TXT records match the digest value

If all the above verifications succeed, then the validation is successful. If no DNS record is found, or DNS record and response payload do not pass these checks, then the server **MUST** fail the validation and mark the challenge as invalid.

The client **SHOULD** de-provision the resource record(s) provisioned for this challenge once the challenge is complete, i.e., once the "status" field of the challenge has the value "valid" or "invalid".

4. Security Considerations

As this challenge that is introduced only differs in the left-most label of the domain name from the existing dns-01 challenge, the same security considerations apply.

In terms of the construction of the label prepended to the domain name, there is no need for a cryptographic hash. The purpose of that is to create a long-lived and statistically distinctive record of minimal size.

SHA-256 was picked due to its broad adoption, hardware support, and existing need in implementations that would likely support dns-account-01.

The first 10 bytes were picked as a tradeoff: the value needs to be short enough to not significantly impact DNS record and response size, long enough to provide sufficient probability of collision avoidance across ACME accounts, and just the right size to have Base32 require no padding. As the algorithm is used for uniform distribution of inputs, and not for integrity, we do not consider the trimming a security issue.

5. IANA Considerations

5.1. DNS Parameters

The Underscored and Globally Scoped DNS Node Names is to be updated to include the following entry:

RR Type: TXT
_NODE NAME: _acme-challenge_*
Reference: This document

Where _acme-challenge_* denotes all node names beginning with the string _acme-challenge_. It does NOT refer to a DNS wildcard specification.

5.2. ACME Validation Method

The "ACME Validation Methods" registry is to be updated to include the following entry:

label: dns-account-01
identifier-type: dns
ACME: Y
Reference: This document

6. Normative References

[FIPS180-4] National Institute of Standards and Technology, "Secure Hash Standard (SHS)", August 2015, <https://csrc.nist.gov/publications/detail/fips/180/4/final>.

[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>.

[RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, DOI 10.17487/RFC4086, June 2005, <https://www.rfc-editor.org/info/rfc4086>.

[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>.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <https://www.rfc-editor.org/info/rfc6234>.

[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>.

Acknowledgments

Authors' Addresses

Antonios A. Chariton
Google

Email: aac@google.com

Amir A. Omidi
Google

Email: aaomidi@google.com

James Kasten
Google

Email: jdkasten@google.com

Fotis Loukos
Google

Email: fotisl@google.com

Stanislaw A. Janikowski
Google

Email: stanwise@google.com