Automated Certificate Management Environment A. Gable
Internet-Draft Internet Security Research Group
Intended status: Standards Track 2 March 2026
Expires: 3 September 2026

Automated Certificate Management Environment (ACME) Profiles Extension
draft-ietf-acme-profiles-01

Abstract

This document defines how an ACME Server may offer a selection of different certificate profiles to ACME Clients, and how those clients may indicate which profile they want.

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://aarongable.github.io/draft-acme-profiles/draft-ietf-acme-profiles.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-acme-profiles/.

Discussion of this document takes place on the Automated Certificate Management Environment Working Group mailing list (mailto:acme@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/acme/. Subscribe at https://www.ietf.org/mailman/listinfo/acme/.

Source for this draft and an issue tracker can be found at https://github.com/aarongable/draft-acme-profiles.

Current Implementations

This note is to be removed before publishing as an RFC.

This document is implemented by at least two ACME Servers (Boulder (https://github.com/letsencrypt/boulder/issues/7309) and Pebble (https://github.com/letsencrypt/pebble/pull/473)), and at least seven ACME Clients (Certbot (https://github.com/certbot/certbot/issues/10194), Lego (https://github.com/go-acme/lego/pull/2415), eggsampler/acme (https://github.com/eggsampler/acme/pull/25), caddy (https://github.com/caddyserver/caddy/commit/2c4295ee48f494bc8dda5fa09b37612d520c8b3b), certifytheweb (https://docs.certifytheweb.com/blog/acme-profiles-draft/), poshacme (https://github.com/rmbolger/Posh-ACME/releases/tag/v4.28.0), and dehydrated (https://github.com/dehydrated-io/dehydrated/pull/956)).

It is deployed by the Let's Encrypt CA (https://letsencrypt.org/docs/profiles/), and is being actively used to manage migrations away from the tlsClientAuth EKU (https://letsencrypt.org/2025/05/14/ending-tls-client-authentication) and towards shorter-lived certificates (https://letsencrypt.org/2025/12/02/from-90-to-45).

Status of This Memo

This Internet-Draft will expire on 3 September 2026.

Copyright Notice

Table of Contents

1. Introduction

Throughout the history of the WebPKI, Certificate Authorities have used "profiles" to describe the kinds of certificates they issue. For example, an "S/MIME" profile might indicate that the resulting certificate will contain the id-kp-emailProtection Extended Key Usage and use a Certificate Policy OID to assert compliance with the CA/Browser Forum S/MIME Baseline Requirements; or a "Constrained Sub-CA" profile might indicate the inclusion of the Basic Constraints extension, the keyCertSign Key Usage, and a Name Constraints extension. Subscribers generally select a profile as part of their certificate ordering process or negotiations with the CA, depending on their needs (and sometimes their budget).

The ACME protocol only allows clients to customize their certificate in two ways: the newOrder request allows selection of the identifiers (generally Subject Alternative Names) and validity period; and the finalize request contains a CSR in which the client can theoretically include any combination of fields and extensions that they desire. But requesting certificate features via the CSR is onerous, error-prone, and dangerous. Numerous compliance incidents across the WebPKI have been caused by CAs trusting values included in a CSR and copying them directly into the issued certificate. It requires clients to know how to construct a valid CSR, provides no mechanism for servers to advertise what CSR fields they’re willing to accept, and means that CAs have to evaluate on a case-by-case basis which combinations of requested features they’re willing to issue.

This document provides a mechanism for ACME Servers to advertise what certificate profiles they offer, and for ACME Clients to select a profile when creating a new Order. This allows site operators to make informed decisions about the kind of certificate they request, without placing an undue burden on ACME Clients or Servers to transmit such information in the form of a CSR. It also encourages the evolution of the WebPKI by allowing CAs to more easily offer new and improved profiles while maintaining backwards compatibility for old subscribers.

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. Extensions to the Directory Resource

An ACME Server which wishes to allow Clients to select profiles MUST include a new field, profiles, in the meta field of its Directory object.

profiles (optional, object): A map of profile names to human-readable descriptions of those profiles.

The contents of these human-readable descriptions are up to the CA; for example, they might be prose descriptions of the properties of the profile, or the might be URLs pointing at a documentation site. ACME Clients SHOULD present these profile names and descriptions to their operator during initial setup and at appropriate times thereafter.

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "newNonce": "https://acme.example.com/new-nonce",
  "newAccount": "https://acme.example.com/new-account",
  "newOrder": "https://acme.example.com/new-order",
  "newAuthz": "https://acme.example.com/new-authz",
  "revokeCert": "https://acme.example.com/revoke-cert",
  "keyChange": "https://acme.example.com/key-change",
  "meta": {
    "termsOfService": "https://example.com/acme/terms",
    "website": "https://example.com/acme/docs",
    "caaIdentities": ["example.com"],
    "externalAccountRequired": false,
    "profiles": {
      "profile1": "https://example.com/acme/docs/profiles#profile1",
      "profile2": "https://example.com/acme/docs/profiles#profile2",
    }
  }
}
```

4. Extensions to the Order Resource

In order to convey information about the profile associated with an Order, a new field is added to the Order object:

profile (string, optional): A string uniquely identifying the profile which will be used to affect issuance of the certificate requested by this Order.

To select a profile, the client includes the desired profile name in the profile field of the Order object they supply to the newOrder request. The client SHOULD NOT request a profile name that is not advertised in the server's Directory metadata object.

```
POST /acme/new-order HTTP/1.1
Host: acme.example.com
Content-Type: application/jose+json

{
  "protected": base64url({
    "alg": "ES256",
    "kid": "https://acme.example.com/acct/evOfKhNU60wg",
    "nonce": "5XJ1L3lEkMG7tR6pA00clA",
    "url": "https://acme.example.com/new-order"
  }),
  "payload": base64url({
    "identifiers": [{"type": "dns", "value": "example.org"}],
    "profile": "profile1"
  }),
  "signature": "H6ZXtGjTZyUnPeKn...wEA4TklBdh3e454g"
}
```

The server MUST reject all newOrder requests which specify a profile that is incompatible with the rest of the contents of the request (e.g. a "tls-server-auth" profile alongside an identifier of type "email", or a "super-special" profile requested by an account which is not on the appropriate allowlist). In such cases, the server MUST respond with a problem document of type "invalidProfile" (see Section 6.3).

The server SHOULD reject all newOrder requests which specify a profile that the server is not advertising, but MAY accept them in extenuating circumstances. For example, when a private profile name has been agreed upon with the client via out-of-band mechanisms, or when replacing a certificate during a mass revocation event that was originally issued under a now-deprecated profile.

If it accepts the request, the server responds with an Order object including the selected profile.

```
HTTP/1.1 201 Created
Replay-Nonce: MYAuvOpaoIiywTezizk5vw
Link: <https://acme.example.com/directory>;rel="index"
Location: https://acme.example.com/order/TOlocE8rfgo

{
  "status": "valid",
  "expires": "2025-01-01T12:00:00Z",
  "identifiers": [{"type": "dns", "value": "example.org"}],
  "profile": "profile1",
  "authorizations": ["https://acme.example.com/authz/PAniVnsZcis"],
  "finalize": "https://acme.example.com/order/TOlocE8rfgo/finalize",
}
```

If the server is advertizing profiles and receives a newOrder request which does not identify a specific profile, it is RECOMMENDED that the server select a profile and associate it with the new Order object.

If a server receives a request to finalize an Order whose profile the CA is no longer willing to issue under, it MUST respond with a problem document of type "invalidProfile". The server SHOULD attempt to avoid this situation, e.g. by ensuring that all Orders for a profile have expired before it stops issuing under that profile.

5. Security Considerations

The extensions to the ACME protocol described in this document build upon the Security Considerations and threat model defined in Section 10.1 of [RFC8555]. It does not change the account management or identifier validation flows, so the security considerations are largely unchanged.

The one exception is in regards to CA Policy Considerations. RFC 8555 did not address how a server should determine whether it is willing to issue the certificate as requested by the finalize CSR. This document greatly simplifies this determination by making the contents of the CSR (beyond the Subject Alternative Names and Subject Public Key) irrelevant to the decision-making process.

Additionally, by moving profile selection out of the finalize CSR and into the Order resource itself, this document reduces the need for ACME Clients and Servers to parse and process x509 ASN.1. This increases the security and stability of the WebPKI as a whole by reducing the incidence of parsing errors and the likelihood of values being copied directly from the CSR into the resulting certificate.

6. IANA Considerations

6.1. ACME Directory Metadata Fields

IANA will add the following entry to the "ACME Directory Metadata Fields" registry within the "Automated Certificate Management Environment (ACME) Protocol" registry group at https://www.iana.org/assignments/acme (https://www.iana.org/assignments/acme):

Field Name	Field Type	Reference
profiles	object	This document

Table 1

6.2. ACME Order Object Fields

IANA will add the following entry to the "ACME Order Object Fields" registry within the "Automated Certificate Management Environment (ACME) Protocol" registry group at https://www.iana.org/assignments/acme (https://www.iana.org/assignments/acme):

Field Name	Field Type	Configurable	Reference
profile	string	true	This document

Table 2

6.3. ACME Error Types

IANA will add the following entry to the "ACME Error Types" registry within the "Automated Certificate Management Environment (ACME) Protocol" registry group at https://www.iana.org/assignments/acme (https://www.iana.org/assignments/acme):

Type	Description	Reference
invalidProfile	The request specified a profile which this server does not support	This document

Table 3

7. Normative References

[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/rfc/rfc2119>.

[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/rfc/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/rfc/rfc8555>.

Acknowledgments

My thanks to Phil Porada for spearheading the implementation of this protocol in the Boulder software. Thanks also to Jacob Hoffman-Andrews, Samantha Frank, James Kasten, and Jason Baker for discussions and brainstorming on what this protocol should look like.

Author’s Address

Aaron Gable
Internet Security Research Group
Email: aaron@letsencrypt.org