Automated Certificate Management Environment
Internet-Draft
Intended status: Standards Track
Expires: 23 April 2026

D. Benjamin
Google LLC

20 October 2025

Automated Certificate Management Environment (ACME) Profile Sets
draft-davidben-acme-profile-sets-00

Abstract

This document defines how an ACME Server may indicate collections of related certificate profiles to ACME Clients.

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 23 April 2026.

Copyright Notice

Table of Contents

1. Introduction

As PKIs evolve, an application that authenticates with certificates may need to support a wide range of relying parties, both before and after some change. For example:

* When transitioning to post-quantum cryptography, newer relying parties may expect post-quantum trust anchors, while older, unupdated relying parties still only support classical ones.

* When a certification authority (CA) is found untrustworthy, or its keys rotated or compromised, newer relying parties may expect a newer CA instance, while older, unupdated relying parties may only support the older CA.

As the furthest relying parties diverge, using a single certificate may not be feasible. Applications may then need to obtain multiple certificates, presenting different certificates to different relying parties.

[I-D.ietf-acme-profiles] defines ACME profiles, a mechanism for ACME Clients to choose between different certificate profiles from a single ACME Server. However, in applications that require certificates from multiple profiles, an ACME Client must know which profiles are needed, and be updated over time.

This document extends ACME profiles with _profile sets_. A profile set is a set of related profiles, defined by the ACME Server. As PKIs evolve, the ACME Server can update its profile sets to reflect relying party needs. In particular, if satisfying all relying parties with a single profile would be infeasible or inefficient, the ACME Server can add a profile to the profile set.

An ACME Client configured with a profile set requests a certificate for each profile, automatically incorporating updates to the profile set as part of certificate renewal. This allows the ACME Server to aid ACME Clients in handling PKI evolution.

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 that wishes for clients to combine multiple certificate profiles MUST include a new field, profileSets, in the meta field of its Directory object. The field is defined as follows:

profileSets (optional, object): A map of profile set names to objects describing profile sets. Profile and profile set names MUST NOT overlap.

Each profile set is described by a JSON object with the following fields:

description (required, string): A human-readable description of the profile set.

profiles (required, array of string): An array of strings, containing the names of the profiles in the profile set.

The human-readable descriptions are analogous to those of the profiles map defined in [I-D.ietf-acme-profiles]. Their contents are up to the CA; for example, they might be prose descriptions of the properties of the profile, or they might be URLs pointing at a documentation site. ACME Clients SHOULD present these profile set names and descriptions to their operator during initial setup and at appropriate times thereafter.

Profile sets MAY contain overlapping profiles.

Together, the profiles and profileSets maps indicate the choices available to the ACME Client operator. An individual profile in a profile set MAY appear in the profiles map if the ACME Server intends it to be a standalone choice for the ACME Client operator. It MAY also be omitted from the profiles map if the ACME Server intends it to be used only in a profile set.

For example, the following Directory object defines two profile sets, profile1Ext and profile2, alongside standalone profile1. An ACME Client might interpret this by offering three choices to the operator, profile1, profile1Ext, and profile2, with their corresponding human-readable descriptions.

The profile1Ext profile set consists of profile1, which is also a standalone profile, and profileExt, which is a profile-set-only profile. The profile2 profile set consists of three profile-set-only profiles, profile2a, profile2b, and profileExt.

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

{
  "newNonce": "https://example.com/acme/new-nonce",
  "newAccount": "https://example.com/acme/new-account",
  "newOrder": "https://example.com/acme/new-order",
  "newAuthz": "https://example.com/acme/new-authz",
  "revokeCert": "https://example.com/acme/revoke-cert",
  "keyChange": "https://example.com/acme/key-change",
  "meta": {
    "termsOfService": "https://example.com/acme/terms/2021-10-05",
    "website": "https://www.example.com/",
    "caaIdentities": ["example.com"],
    "externalAccountRequired": false,
    "profiles": {
      "profile1": "https://example.com/docs/profiles#profile1",
    },
    "profileSets": {
      "profile1Ext": {
        "description":
            "https://example.com/docs/profiles#profile1Ext",
        "profiles": ["profile1", "profileExt"]
      },
      "profile2": {
        "description":
            "https://example.com/docs/profiles#profile2",
        "profiles": ["profile2a", "profile2b", "profileExt"]
      }
    }
  }
}
```

4. Client Behavior

An ACME Client that supports profile sets MAY be configured to obtain certificates according to a profile set, rather than an individual profile.

If configured with a profile set, the ACME Client SHOULD request certificates from each profile in the profile set, creating independent, parallel orders for each. Each profile MAY spend different amounts of time in the "processing" state, so the ACME Client SHOULD support multiple orders in the "processing" state in parallel. Each profile MAY produce certificates with different lifetimes, so the ACME Client SHOULD evaluate each certificate for renewal independently.

The ACME Client SHOULD periodically re-fetch the Directory object to discover updated profile set definitions. For example, the client MAY re-fetch the Directory when it periodically evaluates its certificates for renewal. If the profile set definition has since changed, the ACME Client SHOULD request certificates for any newly-added profiles. Certificates for newly-removed profiles SHOULD NOT be removed until the ACME Client has provisioned some certificate for each profile in the new profile set definition.

ACME Clients MAY implement the above with the following example procedure, run periodically:

1. Fetch the Directory object from the ACME Server.

2. For each profile in the selected profile set:

    a. Check if the client has an unfinished order for the profile. If so, check if it has entered the "valid" state and download the certificate.

    b. Otherwise, check if the client already has a certificate for the profile, and if it should be renewed, e.g. because it is soon to expire.

    c. If the certificate does not exist, or is soon to expire, start a new order with the profile, as described in [I-D.ietf-acme-profiles], and complete its authorizations.

3. Cancel any unfinished orders for profiles that are no longer in the profile set.

4. If the client has a certificate for each profile in the profile set, remove certificates for profiles that are no longer in the profile set.

Determining which certificate to use with which relying party is out of scope for this document. TLS [RFC8446] implementations MAY use the procedures defined in Sections 4.4.2.2 and 4.4.2.3 of [RFC8446], as well as other TLS extensions, to select certificates.

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], along with the mechanism defined in [I-D.ietf-acme-profiles]. It does not change the account management or identifier validation flows, so the security considerations are largely unchanged. It also does not change the lifecycle of any individual order, or issuance from the perspective of the server.

Profile sets allow an ACME Server to help ACME Clients configure themselves appropriately during PKI security transitions, such as a change in algorithm, a change in trusted CAs, or CA key rotation. Most PKIs have far fewer ACME Servers than ACME Clients, with ACME Server operators well-connected to relying party requirements. This can help transitions complete more quickly, and thus allow the PKI to realize the security benefits sooner.

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
profileSets	object	This document

Table 1

7. References

7.1. Normative References

[I-D.ietf-acme-profiles]
Gable, A., "Automated Certificate Management Environment (ACME) Profiles Extension", Work in Progress, Internet-Draft, draft-ietf-acme-profiles-00, 8 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-acme-profiles-00>.

[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>.

7.2. Informative References

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

Acknowledgements

Thanks to Aaron Gable for feedback on this document, as well as many valuable design discussions.

Author’s Address

David Benjamin
Google LLC
Email: davidben@google.com