Extensions to Automatic Certificate Management Environment for email TLS

draft-ietf-acme-email-tls-05

Abstract

This document specifies identifiers and challenges required to enable the Automated Certificate Management Environment (ACME) to issue certificates for use by TLS email services.

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 January 26, 2019.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
1. Introduction

[I-D.ietf-acme-acme] is a mechanism for automating certificate management on the Internet. It enables administrative entities to prove effective control over resources like domain names, and automates the process of generating and issuing certificates.

This document describes extensions to ACME for use by email services. Section 3 defines extensions for how email services (such as SMTP, IMAP and POP3) can get certificates for use with TLS.

2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Use of ACME for use by TLS-protected SMTP, IMAP and POP3 services

SMTP [RFC5321] (including SMTP Submission [RFC6409]), IMAP [RFC3501] and POP3 [RFC2449] servers use TLS [RFC5246] to provide server identity authentication, data confidentiality and integrity services. Such TLS protected email services either use STARTTLS command or run on a separate TLS-protected port [RFC8314].

[I-D.ietf-acme-acme] defines several challenge types that can be extended for use by email services. This document also defines some new challenge types specific to SMTP, IMAP and POP3.

In order to use these challenges JWS [RFC7515] object used by [I-D.ietf-acme-acme] is extended. The following extra requirements
are in addition to requirements on JWS objects sent in ACME defined in Section 6.2 of [I-D.ietf-acme-acme]:

1. "service" JWS header parameter MUST be included. See Section 3.1 for more details.

2. "port" JWS header parameter SHOULD be included. See Section 3.2 for more details. If this JWS header parameter is not included, the default assigned IANA port for the corresponding "service" is assumed.

For example, if the ACME client were to respond to the "dns-email-00" challenge, it would send the following request:

```
POST /acme/authz/asdf/0 HTTP/1.1
Host: example.com
Content-Type: application/jose+json

{
  "protected": base64url({
    "alg": "ES256",
    "kid": "https://example.com/acme/acct/1",
    "nonce": "Q_s3MWoqT05TrdkM2MTDcw",
    "url": "https://example.com/acme/authz/asdf/0"
  }),
  "payload": base64url({
    "type": "dns-email-00",
    "service": "smtp",
    "port": 25,
    "keyAuthorization": "IlirfxKKXA...vb29HhjjLPSggQiE"
  }),
  "signature": "7cbg5J01gf5YLjjF...SpkUfcdPai9uVYYU"
}
```

3.1. "service" field in JSON payload

The "service" field in JSON payload specifies the service for which TLS server certificate should be issued. Valid values come from "Service Names and Transport Protocol Port Numbers" IANA registry <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>.

ACME servers compliant with this specification MUST support [RFC7817] (in particular see Section 4 of that document).

[[This parameter might have applicability beyond email services.]]
3.2. "port" field in JSON payload

The "port" field in JSON payload specifies the TCP port number where the corresponding service is running. ACME server MAY check that the TCP port corresponds to the requested "service", for example that the port is the assigned default IANA port for the service.

[[This parameter might have applicability beyond email services.]]

3.3. DNS challenge for email services

"dns-email-00" is very similar to "dns-01" defined in Section 8.4 of [I-D.ietf-acme-acme].

The difference between processing of "dns-email-00" and "dns-01" are listed below:

1. The TXT record used to validate this challenge is 
   _<port>._<service>._acme-challenge.<domain>_. For example, for domain "example.com" and IMAPS service running on port 993, the TXT record name is _993._imaps._acme-challenge.example.com. For domain "example.net" and IMAP service running on port 143, the TXT record name is _143._imap._acme-challenge.example.next.

3.4. CAPABILITY challenge for email services

For "capability-smtp-00" challenge, ACME client (== SMTP server) constructs a key authorization from the "token" value provided in the challenge and the client's account key. The client then computes the SHA-256 digest [FIPS180-4] of the key authorization. SMTP server than returns the base64url encoding of this digest as a value of the "ACME" EHLO capability. For example:
Note that in the above example only presence of the ACME is relevant as far as this document is concerned.

Figure 2

The ACME SMTP extension is formerly defined in Section 3.4.1.

Similarly, "capability-imap-00" challenge, ACME client (== IMAP server) constructs a key authorization from the "token" value provided in the challenge and the client's account key. The client then computes the SHA-256 digest \([\text{FIPS180-4}]\) of the key authorization. IMAP server than returns the base64url encoding of this digest as a value of the "ACME" capability:

* OK [CAPABILITY IMAP4rev1 LOGINDISABLED LITERAL+ ENABLE STARTTLS ACME=gfj9Xq...Rg85nM]

or

* CAPABILITY IMAP4rev1 LOGINDISABLED LITERAL+ ENABLE STARTTLS ACME=gfj9Xq...Rg85nM

Note that in the above example only presence of the ACME capability token is relevant as far as this document is concerned.

Figure 3

Similarly, "capability-pop-00" challenge, ACME client (== POP3 server) constructs a key authorization from the "token" value provided in the challenge and the client's account key. The client then computes the SHA-256 digest \([\text{FIPS180-4}]\) of the key authorization. POP3 server than returns the base64url encoding of this digest as a value of the "ACME" capability in response to CAPA command \([\text{RFC2449}]\):
Note that in the above example only presence of the ACME capability
token is relevant as far as this document is concerned.

Figure 3

3.4.1. Registration of the ACME SMTP extension

The ACME SMTP service extension is defined as follows:

1. The textual name of this extension is "ACME for SMTP".
2. The EHLO keyword value associated with this extension is "ACME".
3. The EHLO keyword has a single required parameter which is a
   base64url encoded SHA-256 hash, which is 44 octets in length.
4. This extension doesn't define any new SMTP verbs.
5. This extension doesn't add any new parameters to MAIL FROM or
   RCPT TO commands.
6. The ACME extension is valid for the submission service [RFC6409]
   (default port number 587) or its version running directly over

4. Open Issues

[[This section should be empty before publication]]

1. Should the same certificate be allowed to be used on both IMAP
   (143) and IMAPS (993) ports? (These ports have different service
   names associated with them. Is 1 service/port per ACME
   certificate a restriction imposed by this document?) Maybe if
   the ACME server sees a request for port 143 (or 993), it can
   include SRV-ID for the other port, if it can verify that both are
   running? (How can this be done reliably?) Many email servers
   don't allow different certificates to be configured for different
   ports they are listening on. The cleanest way is to change
"service" to "services", change "port" to "ports" and make both of them arrays.

2. Add support for LMTP (RFC 2033)?

5. IANA Considerations

IANA is requested to register the following ACME challenge types that are used with Identifier Type "dns": "dns-email", "capability-smtp", "capability-imap" and "capability-pop". The reference for all of them is this document.

6. Security Considerations

Security Considerations from [I-D.ietaf-acme-acme] relevant to the DNS challenge type are also relevant to "dns-email".

7. Normative References


Author's Address

Alexey Melnikov
Isode Ltd
14 Castle Mews
Hampton, Middlesex TW12 2NP
UK

EMail: Alexey.Melnikov@isode.com