Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 26, 2019

A. Melnikov
Isode Ltd

July 25, 2018

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.

Table of Contents

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": "7cbg5JO1Gf5YLjjF...SpkUfcdPai9uVYYU"
}
```

Figure 1

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:

```
250-smtp.example.com
250-SIZE
250-8BITMIME
250-BINARYMIME
250-PIPELINING
250-HELP
250-DSN
250-CHUNKING
250-AUTH SCRAM-SHA-1
250-AUTH=SCRAM-SHA-1
250-STARTTLS
250-ACME gfj9Xq...Rg85nM
250-MT-PRIORITY
250 ENHANCEDSTATUSCODES
```

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 [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] Example IMAP4rev1 server ready
```

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 [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 [RFC2449]:

```
C: CAPA
S: +OK Capability list follows
S: TOP
S: SASL CRAM-MD5 KERBEROS_V4
S: UIDL
S: ACME gfj9Xq...Rg85nM
S: IMPLEMENTATION Shlemazle-Plotz-v915
S: .
```

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 TLS [RFC8314] ("submissions" service, default port number 465) .

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.ietf-acme-acme] relevant to the DNS challenge type are also relevant to "dns-email".

7. Normative References

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

[I-D.ietf-acme-acme] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", draft-ietf-acme-acme-12 (work in progress), April 2018.

[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>.

[RFC2449] Gellens, R., Newman, C., and L. Lundblade, "POP3 Extension Mechanism", RFC 2449, DOI 10.17487/RFC2449, November 1998, <https://www.rfc-editor.org/info/rfc2449>.

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, DOI 10.17487/RFC3501, March 2003, <https://www.rfc-editor.org/info/rfc3501>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <https://www.rfc-editor.org/info/rfc5321>.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, DOI 10.17487/RFC6125, March 2011, <https://www.rfc-editor.org/info/rfc6125>.

[RFC6409] Gellens, R. and J. Klensin, "Message Submission for Mail", STD 72, RFC 6409, DOI 10.17487/RFC6409, November 2011, <https://www.rfc-editor.org/info/rfc6409>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/info/rfc7515>.

[RFC7817] Melnikov, A., "Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols", RFC 7817, DOI 10.17487/RFC7817, March 2016, <https://www.rfc-editor.org/info/rfc7817>.

[RFC8314] Moore, K. and C. Newman, "Cleartext Considered Obsolete: Use of Transport Layer Security (TLS) for Email Submission and Access", RFC 8314, DOI 10.17487/RFC8314, January 2018, <https://www.rfc-editor.org/info/rfc8314>.

Author's Address

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

EMail: Alexey.Melnikov@isode.com