Network Working Group
Internet-Draft
Intended status: Informational
Expires: March 5, 2019

A. Melnikov
Isode Ltd

September 1, 2018

Extensions to Automatic Certificate Management Environment for end user S/MIME certificates

draft-ietf-acme-email-smime-03

Abstract

This document specifies identifiers and challenges required to enable the Automated Certificate Management Environment (ACME) to issue certificates for use by email users that want to use S/MIME.

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 March 5, 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 an extension to ACME for use by S/MIME. Section 3 defines extensions for issuing end user S/MIME [RFC5750] certificates.

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 issuing end user S/MIME certificates

[I-D.ietf-acme-acme] defines "dns" Identifier Type that is used to verify that a particular entity has control over a domain or specific service associated with the domain. In order to be able to issue end-user S/MIME certificates, ACME needs a new Identifier Type that proves ownership of an email address.

This document defines a new Identifier Type "email" which corresponds to an (all ASCII) email address [RFC5321] or Internationalized Email addresses [RFC6531]. This can be used with S/MIME or other similar service that requires posession of a certificate tied to an email address.

Any identifier of type "email" in a new-order request MUST NOT have a wildcard ("*") character in its value.

A new challenge type "email-reply-00" is used with "email" Identifier Type, which provides proof that an ACME client has control over an email address:

1. ACME server generates a "challenge" email message with the subject "ACME: <token-part1>", where <token-part1> is the base64url encoded first part of the token, which contains at least 64 bit of entropy. The challenge email message structure is described in more details in Section 3.1. The second part of the token (token-part2, which also contains at least 64 bit of entropy) is returned over HTTPS [RFC2818] to the ACME client.

2. ACME client concatenates "token-part1" and "token-part2" to create "token", calculates key-authz (as per Section 8.1 of [I-D.ietf-acme-acme]), then includes the base64url encoded SHA-256 digest [FIPS180-4] of the key authorization in the body of a response email message containing a single text/plain MIME body part [RFC2045]. The response email message structure is described in more details in Section 3.2

For an identifier of type "email", CSR MUST contain the request email address in an extensionRequest attribute [RFC2985] requesting a subjectAltName extension. (These identifiers may appear in any sort order.)

3.1. ACME challenge email

A "challenge" email message MUST have the following structure:

1. The message Subject header field has the following syntax: "ACME: <token-part1>", where the prefix "ACME:" is followed by at least one SP or TAB character. <token-part1> is the base64url encoded first part of the ACME token.

2. The message MUST include the "Auto-Submitted: auto-generated" header field [RFC3834]. It MAY include optional parameters as allowed by syntax of Auto-Submitted header field.

3. The message MUST have a single text/plain MIME body part [RFC2045], that contains human readable explanation of the purpose of the message.

Example ACME "challenge" email

```
Auto-Submitted: auto-generated
Date: Sat, 1 Sep 2018 10:08:55 +0100
Message-ID: <A2299BB.FF7788@example.org>
From: acme-generator@example.org
To: alexey@example.com
Subject: ACME: <base64url-encoded-token-with-64-octets-of-entropy>
Content-Type: text/plain

This is an automatically generated ACME challenge for email address
&lt;alexey@example.com&gt;. If you haven't requested an S/MIME
certificate generation for this email address, be very afraid.
If you did request it, your email client might be able to process
this request automatically, or you might have to paste the first
token part into an external program.
```

Figure 1

3.2. ACME response email

A "response" email message MUST have the following structure:

1. The message Subject header field has the following syntax: "Re: ACME: <token-part1>", where the prefix "ACME:" is followed by at least one SP or TAB character. <token-part1> is the base64url encoded first part of the ACME token.

2. The To: header field of the response contains the value from the From: header field of the challenge email.

3. The message MUST have a single text/plain MIME body part [RFC2045], containing base64url encoded SHA-256 digest [FIPS180-4] of the key authorization. Note that due to historic line length limitations in email, line endings (CRLFs) can be freely inserted in the middle of the encoded digest, so they need to be ignored when processing it.

Example ACME "response" email

```
Date: Sat, 1 Sep 2018 11:12:00 +0100
Message-ID: <111-22222-3333333@example.com>
From: alexey@example.com
To: acme-generator@example.org
Subject: Re: ACME: <base64url-encoded-token-with-64-octets-of-entropy>
Content-Type: text/plain

LoqXcYV8q5ONbJQxbmR7SCTNo3tiAXDfowy
jxAjEuX0.9jg46WB3rR_AHD-EBXdN7cBkH1WOu0tA3M9
fm21mqTI
```

Figure 2

4. Open Issues

[[This section should be empty before publication]]

1. Do we need to handle text/html or multipart/alternative in email challenge? Simplicity suggests "no". However, for automated processing it might be better to use at least multipart/mixed with a special MIME type.

2. Define a new parameter to "Auto-Submitted: auto-generated", so that it is easier to figure out that a particilar message is an ACME challenge message?

5. IANA Considerations

IANA is requested to register a new Identifier Type "email" which corresponds to an (all ASCII) email address [RFC5321] or Internationalized Email addresses [RFC6531].

And finally, IANA is requested to register the following ACME challenge types that are used with Identifier Type "email": "email-reply". The reference for it is this document.

6. Security Considerations

TBD.

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., and J. Kasten, "Automatic Certificate Management Environment (ACME)", draft-ietf-acme-acme-14 (work in progress), August 2018.

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, DOI 10.17487/RFC2045, November 1996, <https://www.rfc-editor.org/info/rfc2045>.

[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>.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, DOI 10.17487/RFC2818, May 2000, <https://www.rfc-editor.org/info/rfc2818>.

[RFC2985] Nystrom, M. and B. Kaliski, "PKCS #9: Selected Object Classes and Attribute Types Version 2.0", RFC 2985, DOI 10.17487/RFC2985, November 2000, <https://www.rfc-editor.org/info/rfc2985>.

[RFC3834] Moore, K., "Recommendations for Automatic Responses to Electronic Mail", RFC 3834, DOI 10.17487/RFC3834, August 2004, <https://www.rfc-editor.org/info/rfc3834>.

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

[RFC5750] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling", RFC 5750, DOI 10.17487/RFC5750, January 2010, <https://www.rfc-editor.org/info/rfc5750>.

[RFC6531] Yao, J. and W. Mao, "SMTP Extension for Internationalized Email", RFC 6531, DOI 10.17487/RFC6531, February 2012, <https://www.rfc-editor.org/info/rfc6531>.

[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>.

Author's Address

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

EMail: alexey.melnikov@isode.com