Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 30, 2021

A. Melnikov
Isode Ltd

October 27, 2020

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

draft-ietf-acme-email-smime-10

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 April 30, 2021.

Table of Contents

1. Introduction

ACME [RFC8555] 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 [RFC8550] 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

ACME [RFC8555] defines a "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]. (When Internationalized Email addresses are used, both U-labels and A-labels [RFC5890] are allowed in the domain part.) This can be used with S/MIME or other similar service that requires possession of a certificate tied to an email address.

Any identifier of type "email" in a newOrder 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. An end-user initiates issuance of an S/MIME certificate for one of her email addresses. This might be done using email client UI (and might use some HTTP API underneath), by visiting a Certificate Authority web page or by sending an email to a well known Certificate Authority's email address. This document doesn't prescribe how exactly S/MIME certificate issuance is initiated.

2. The ACME server (run by the Certificate Authority or their authorized third party) generates a "challenge" email message with the subject "ACME: <token-part1>", where <token-part1> is the base64url encoded [RFC4648] first part of the token, which contains at least 64 bits of entropy. (ACME server MUST generate token afresh for each S/MIME issuance request.) 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 bits of entropy) is returned over HTTPS [RFC2818] to the ACME client.

3. The ACME client concatenates "token-part1" and "token-part2" to create "token", calculates keyAuthorization (as per Section 8.1 of [RFC8555]), 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", the PKCS#10 [RFC2986] Certificate Signing Request (CSR) MUST contain the requested email address in an extensionRequest attribute [RFC2985] requesting a subjectAltName extension.

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 folding white space (FWS, see [RFC5322]) and then by <token-part1>, which is the base64url encoded first part of the ACME token that MUST be at least 64 bits long after decoding. Due to the recommended

78-octet line length limit in [RFC5322], the subject line can be folded, so whitespaces (if any) within the <token-part1> MUST be ignored. [RFC2231] encoding of the message Subject header field MUST be supported, but when used, only "UTF-8" and "US-ASCII" charsets MUST be used (i.e. other charsets MUST NOT be used).

2. The To header field MUST be the email address of the entity that requested the S/MIME certificate to be generated.

3. The message MAY contain a Reply-To header field.

4. The message MUST include the "Auto-Submitted: auto-generated" header field [RFC3834]. The "Auto-Submitted" header field SHOULD include the "type=acme" parameter. It MAY include other optional parameters as allowed by the syntax of the Auto-Submitted header field.

5. In order to prove authenticity of a challenge message, it MUST be either DKIM [RFC6376] signed or S/MIME [RFC8551] signed. If DKIM signing is used, the resulting DKIM-Signature header field MUST contain the "h=" tag that includes at least "From", "Sender", "Reply-To", "To", "CC", "Subject", "Date", "In-Reply-To", "References", "Message-ID", "Content-Type", and "Content-Transfer-Encoding" header fields. The message MUST also pass DMARC validation [RFC7489], which implies DKIM and SPF validation [RFC7208].

6. The body of the challenge message is not used for automated processing, so it can be any media type. (However there are extra requirements on S/MIME signing, if used. See below.) Typically it is text/plain or text/html containing a human-readable explanation of the purpose of the message. If S/MIME signing is used to prove authenticity of the challenge message, then the multipart/signed or "application/pkcs7-mime; smime-type=signed-data;" media type should be used. Either way, it MUST use S/MIME header protection.

An example ACME "challenge" email (note that DKIM related header fields are not included for simplicity).

```
Auto-Submitted: auto-generated; type=acme
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-bits-of-entropy>
Content-Type: text/plain
MIME-Version: 1.0

This is an automatically generated ACME challenge for email address
"alexey@example.com". 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 valid "response" email message MUST have the following structure:

1. The message Subject header field has the following syntax: "<Reply-prefix> ACME: <token-part1>", where <Reply-prefix> is typically the reply prefix "Re:" and the string "ACME:" is preceded and followed by folding white space (FWS, see [RFC5322]) and then by <token-part1>. <token-part1> is the base64url encoded first part of the ACME token (as received in the ACME challenge) that MUST be at least 64 bits long after decoding. Due to recommended 78 octet line length limit in [RFC5322], the subject line can be folded, so whitespaces (if any) within the <token-part1> MUST be ignored. [RFC2231] encoding of the Subject header field MUST be supported, but when used, only "UTF-8" and "US-ASCII" charsets MUST be used (i.e. other charsets MUST NOT be used). When parsing subjects, ACME servers must decode [RFC2231] encoding (if any) and then they can ignore any prefix before the "ACME:" label.

2. The From: header field contains the email address of the user that is requesting S/MIME certificate issuance.

3. The To: header field of the response contains the value from the Reply-To: header field from the challenge message (if set) or from the From: header field of the challenge message otherwise.

4. The Cc: header field is ignored if present in the "response" email message.

5. The In-Reply-To: header field SHOULD be set to the Message-ID header field of the challenge message according to rules in Section 3.6.4 of [RFC5322].

6. List-* header fields [RFC4021][RFC8058] MUST be absent (i.e., the reply can't come from a mailing list)

7. The media type of the "response" email message is either text/plain or multipart/alternative containing text/plain as one of the alternatives. The text/plain body part (whether or not it is inside multipart/alternative) MUST contain a block of lines starting with the line "-----BEGIN ACME RESPONSE-----", followed by one or more line containing the base64url-encoded SHA-256 digest [FIPS180-4] of the key authorization, calculated from concatenated token-part1 (received over email) and token-part2 (received over HTTPS). See the 3rd bullet point in Section 3 for more details. (Note that due to historical line length limitations in email, line endings (CRLFs) can be freely inserted in the middle of the encoded digest, so they MUST be ignored when processing it.) The final line of the encoded digest is followed by a line containing "-----END ACME RESPONSE-----". Any text before and after this block is ignored. For example such text might explain what to do with it for ACME-unaware clients.

8. There is no need to use any Content-Transfer-Encoding other than 7bit for the text/plain body part, however use of Quoted-Printable or base64 is not prohibited in a "response" email message.

9. In order to prove authenticity of a response message, it MUST be DKIM [RFC6376] signed. The resulting DKIM-Signature header field MUST contain the "h=" tag that includes at least "From", "Sender", "Reply-To", "To", "CC", "Subject", "Date", "In-Reply-To", "References", "Message-ID", "Content-Type", and "Content-Transfer-Encoding" header fields. The message MUST also pass DMARC validation [RFC7489], which implies DKIM and SPF validation [RFC7208].

Example ACME "response" email (note that DKIM related header fields are not included for simplicity).

```
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-enough-entropy>
Content-Type: text/plain
MIME-Version: 1.0

-----BEGIN ACME RESPONSE-----
LoqXcYV8q5ONbJQxbmR7SCTNo3tiAXDfowy
jxAjEuX0.9jg46WB3rR_AHD-EBXdN7cBkH1WOu0tA3M9
fm21mqTI
-----END ACME RESPONSE-----
```

Figure 2

4. Internationalization Considerations

[RFC8616] updated/clarified use of DKIM/SPF/DMARC with Internationalized Email addresses [RFC6531]. Please consult RFC 8616 in regards to any changes that need to be implemented.

Use of non ASCII characters in left hand sides of Internationalized Email addresses requires putting Internationalized Email Addresses in X.509 Certificates [RFC8398].

5. IANA Considerations

5.1. ACME Identifier Type

IANA is requested to register a new Identifier type in the "ACME Identifier Types" registry defined in Section 9.7.7 of [RFC8555] with Label "email" and a Reference to [RFCXXXX], [RFC5321] and [RFC6531]. The new Identifier Type corresponds to an (all ASCII) email address [RFC5321] or Internationalized Email addresses [RFC6531].

5.2. ACME Challenge Type

IANA is also requested to register a new entry in the "ACME Validation Methods" registry defined in Section 9.7.8 of [RFC8555]. This entry is as follows:

Label	Identifier Type	ACME	Reference
email-reply-00	email	Y	[RFCXXXX]

6. Security Considerations

Please see Security Considerations of [RFC8555] for general security considerations related to use of ACME. This challenge/response protocol demonstrates that an entity that controls the private key (corresponding to the public key in the certificate) also controls the named email account. Any claims about the correctness or fitness-for-purpose of the email address must be otherwise assured. I.e. ACME server is only vouching that the requested email address seem to belong to the entity that requested the certificate.

The security of the "email-reply-00" challenge type depends on the security of the email system. A third party that can read and reply to user's email messages (by possessing a user's password or a secret derived from it that can give read and reply access, such as "password equivalent" information; or by being given permissions to act on a user's behalf using email delegation feature common in some email systems) can request S/MIME certificates using the protocol specified in this document and is indistinguishable from the email account owner. This has several possible implications:

1. an entity that compromised an email account would be able to request S/MIME certificates using the protocol specified in this document and such entity couldn't be distinguished from the legitimate email account owner (unless some external sources of information are consulted);

2. for email addresses with legitimate shared access/control by multiple users, any such user would be able to request S/MIME certificates using the protocol specified in this document and such requests can't be attributed to a specific user without consulting external systems (such as IMAP/SMTP access logs);

3. protocol specified in this document is not suitable for use with email addresses associated with mailing lists [RFC5321]. While it is not always possible to guarantee that a particular S/MIME certificate request is not from a mailing list address, prohibition on inclusion of List-* header fields helps Certificate Issuers to handle most common cases.

An email system in its turn depends on DNS. A third party that can manipulate DNS MX records for a domain might be able to redirect

email and can get (at least temporary) read and reply access to it. Similar considerations apply to SPF and DMARC TXT records in DNS. Use of DNSSEC by email system administrators is recommended to avoid making it easy to spoof DNS records affecting email system. However use of DNSSEC is not ubiquitous at the time of publishing of this document, so it is not required here. Also, many existing systems that rely on verification of ownership of an email address, for example 2 factor authentication systems used by banks or traditional certificate issuance systems send email messages to email addresses, expecting the owner to click on the link supplied in them (or to reply to a message), without requiring use of DNSSEC. So the risk of not requiring DNSSEC is presumed acceptable in this document.

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>.

[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>.

[RFC2231] Freed, N. and K. Moore, "MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations", RFC 2231, DOI 10.17487/RFC2231, November 1997, <https://www.rfc-editor.org/info/rfc2231>.

[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>.

[RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", RFC 2986, DOI 10.17487/RFC2986, November 2000, <https://www.rfc-editor.org/info/rfc2986>.

[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>.

[RFC4021] Klyne, G. and J. Palme, "Registration of Mail and MIME Header Fields", RFC 4021, DOI 10.17487/RFC4021, March 2005, <https://www.rfc-editor.org/info/rfc4021>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/info/rfc4648>.

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

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/info/rfc5322>.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <https://www.rfc-editor.org/info/rfc5890>.

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/info/rfc6376>.

[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>.

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014, <https://www.rfc-editor.org/info/rfc7208>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/info/rfc7489>.

[RFC8058] Levine, J. and T. Herkula, "Signaling One-Click Functionality for List Email Headers", RFC 8058, DOI 10.17487/RFC8058, January 2017, <https://www.rfc-editor.org/info/rfc8058>.

[RFC8398] Melnikov, A., Ed. and W. Chuang, Ed., "Internationalized Email Addresses in X.509 Certificates", RFC 8398, DOI 10.17487/RFC8398, May 2018, <https://www.rfc-editor.org/info/rfc8398>.

[RFC8550] Schaad, J., Ramsdell, B., and S. Turner, "Secure/ Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Certificate Handling", RFC 8550, DOI 10.17487/RFC8550, April 2019, <https://www.rfc-editor.org/info/rfc8550>.

[RFC8551] Schaad, J., Ramsdell, B., and S. Turner, "Secure/ Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification", RFC 8551, DOI 10.17487/RFC8551, April 2019, <https://www.rfc-editor.org/info/rfc8551>.

[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/info/rfc8555>.

[RFC8616] Levine, J., "Email Authentication for Internationalized Mail", RFC 8616, DOI 10.17487/RFC8616, June 2019, <https://www.rfc-editor.org/info/rfc8616>.

Appendix A. Acknowledgements

Thank you to Andreas Schulze, Gerd v. Egidy, James A. Baker, Ben Schwartz, Peter Yee and Michael Jenkins for suggestions, comments, and corrections on this document.

Author's Address

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

EMail: alexey.melnikov@isode.com