

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: November 3, 2020

A. Melnikov  
Isode Ltd  
May 2, 2020

Extensions to Automatic Certificate Management Environment for end user  
S/MIME certificates  
[draft-ietf-acme-email-smime-07](#)

## 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 November 3, 2020.

## Copyright Notice

Copyright (c) 2020 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.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Conventions Used in This Document . . . . .	<a href="#">2</a>
<a href="#">3.</a>	Use of ACME for issuing end user S/MIME certificates . . . . .	<a href="#">2</a>
<a href="#">3.1.</a>	ACME challenge email . . . . .	<a href="#">3</a>
<a href="#">3.2.</a>	ACME response email . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Open Issues . . . . .	<a href="#">6</a>
<a href="#">5.</a>	Internationalization Considerations . . . . .	<a href="#">6</a>
<a href="#">6.</a>	IANA Considerations . . . . .	<a href="#">7</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">7</a>
<a href="#">8.</a>	Normative References . . . . .	<a href="#">7</a>
<a href="#">Appendix A.</a>	Acknowledgements . . . . .	<a href="#">10</a>
	Author's Address . . . . .	<a href="#">10</a>

## [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 [[RFC8555](#)] 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 "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. ACME server 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 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 \[RFC8555\]](#)), 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", CSR MUST contain the request 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> is the base64url encoded first part of the ACME token that MUST be at least 64 bit 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 subject 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 message MUST include the "Auto-Submitted: auto-generated" header field [\[RFC3834\]](#). The "Auto-Submitted" header field SHOULD include "type=acme" parameter. It MAY include other optional parameters as allowed by syntax of Auto-Submitted header field.



3. The message MAY contain Reply-To header field.
4. 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](#)].
5. 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 human readable explanation of the purpose of the message. If S/MIME signing is used to prove authenticity of the challenge message, then multipart/signed or "application/pkcs7-mime; smime-type=signed-data;" media type should be used. Either way, it MUST use S/MIME header protection.

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 "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 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 bit 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 subject 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 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. 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 base64url encoded SHA-256 digest [\[FIPS180-4\]](#) of the key authorization, calculated based on token-part1 (received over email) and token-part2 (received over HTTPS). (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 MUST be ignored when processing it.). The final line of the encoded digest is followed by the 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.





7. 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.
8. 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.

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-EBXdN7cBkH1W0u0tA3M9
fm21mqTI
-----END ACME RESPONSE-----
```

Figure 2

#### **4. Open Issues**

[[This section should be empty before publication]]

#### **5. 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](#)].



## 6. 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.

## 7. 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.

Security of "email-reply-00" challenge type depends on security of email system. A third party that can read and reply to user's email messages (by possessing user's password or a secret derived from it that can give read and reply access ("password equivalent" information), or by being given permissions to act on user's behalf using email delegation feature) can request S/MIME certificates and is indistinguishable from the email account owner.

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 easy spoofing of DNS records affecting email system.

## 8. 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>>.
- [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>>.
- [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>>.
- [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 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

