

Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 9, 2017

A. Melnikov
Isode Ltd
June 7, 2017

Extensions to Automatic Certificate Management Environment for end user
S/MIME certificates
[draft-melnikov-acme-email-smime-00](#)

Abstract

This document specifies identifiers and challenges required to enable the Automated Certificate Management Environment (ACME) to issue certificates for use for email recipients 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 <http://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 December 9, 2017.

Copyright Notice

Copyright (c) 2017 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 (<http://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

- [1.](#) Introduction [2](#)
- [2.](#) Conventions Used in This Document [2](#)
- [3.](#) Use of ACME for issuing end user S/MIME certificates [2](#)
- [4.](#) Open Issues [3](#)
- [5.](#) IANA Considerations [3](#)
- [6.](#) Security Considerations [3](#)
- [7.](#) Normative References [3](#)
- Author's Address [4](#)

[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 email services. [Section 3](#) defines extensions for issuing end user S/MIME [[RFC5751](#)] 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](#)]. This can be used with S/MIME or other similar service that requires possession of a certificate tied to an email address.

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: [[Very rough outline follows]]

- 1. ACME server generates an email message with the subject containing "ACME <token-part1>", where <token-part1> is the base64url encoded first part of the token, which contains at

least 64 bit of entropy. The second part of the token (token-part2, which also contains at least 64 bit of entropy) is returned over HTTPS to the ACME client. 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 included the base64url encoded SHA-256 digest [FIPS180-4] of the key authorization in a response email message. The response email message has a single text/plain MIME body part. [[Do we need to handle text/html or multipart/alternative? Simplicity suggests "no".]]

[[Do we need a proof that ACME client can submit email on behalf of the user, not just read the challenge using IMAP?]]

4. Open Issues

[[This section should be empty before publication]]

5. IANA Considerations

IANA is requested to register a new Identifier Type "email" which corresponds to an (all ASCII) email address [[RFC5321](#)].

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

- [I-D.ietf-acme-acme]
Barnes, R., Hoffman-Andrews, J., and J. Kasten, "Automatic Certificate Management Environment (ACME)", [draft-ietf-acme-acme-06](#) (work in progress), March 2017.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC5321] Klensin, J., "Simple Mail Transfer Protocol", [RFC 5321](#), DOI 10.17487/RFC5321, October 2008, <<http://www.rfc-editor.org/info/rfc5321>>.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", [RFC 5751](#), DOI 10.17487/RFC5751, January 2010, <<http://www.rfc-editor.org/info/rfc5751>>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", [RFC 7515](#), DOI 10.17487/RFC7515, May 2015, <<http://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

