Extensions to Automatic Certificate Management Environment for end user
                         S/MIME certificates
                    draft-ietf-acme-email-smime-01

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 May 2, 2018.

Copyright Notice

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 [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] 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.

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 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 MUST have a
single text/plain MIME body part [RFC2045]. 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 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].

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".

2. Do we need a proof that ACME client can submit email on behalf of
    the user, not just read the challenge using IMAP? Alexey:
    probably yes, because intercepting somebody's email is easier
    than generating email on the user's behalf.

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

[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-06 (work in progress), March 2017.

   [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>.

   [RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321,
              DOI 10.17487/RFC5321, October 2008,
              <https://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, <https://www.rfc-editor.org/info/rfc5751>.

   [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