Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 4, 2017

A. Melnikov
Isode Ltd

June 2, 2017

Extensions to Automatic Certificate Management Environment for email TLS and S/MIME

draft-melnikov-acme-email-tls-smime-00

Abstract

This document specifies identifiers and challenges required to enable the Automated Certificate Management Environment (ACME) to issue certificates for use by TLS email services and 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 4, 2017.

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 extensions to ACME for use by email services. Section 3 defines extensions for how email services (such as SMTP, IMAP) can get certificates for use with TLS. Section 4 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 use by TLS-protected SMTP and IMAP services

SMTP [RFC5321] (including SMTP submission) and IMAP [RFC3501] servers use TLS to provide server identity authentication, data confidentiality and integrity services. Such TLS protected email services either use STARTTLS command or run on a separate TLS-protected port.

[I-D.ietf-acme-acme] defines several challenge types that can be extended for use by email services. This document also defines some new challenge types specific to SMTP and IMAP.

In order to use these challenges JWS [RFC7515] object used by [I-D.ietf-acme-acme] is extended. The following extra requirements are in addition to requirements on JWS objects sent in ACME defined in Section 6.2 of [I-D.ietf-acme-acme]:

1. "service" JWS header parameter MUST be included. See Section 3.1 for more details.

2. "port" JWS header parameter MUST (SHOULD?) be included. See Section 3.2 for more details.

For example, if the client were to respond to the "tls-sni-email-00" challenge, it would send the following request:

```
POST /acme/authz/asdf/0 HTTP/1.1
Host: example.com
Content-Type: application/jose+json

{
  "protected": base64url({
    "alg": "ES256",
    "kid": "https://example.com/acme/acct/1",
    "nonce": "Q_s3MWoqT05TrdkM2MTDcw",
    "url": "https://example.com/acme/authz/asdf/0",
    "service": "smtp",
    "port": 25
  }),
  "payload": base64url({
    "type": "tls-sni-email-00",
    "keyAuthorization": "IlirfxKKXA...vb29HhjjLPSggQiE"
  }),
  "signature": "7cbg5JO1Gf5YLjjF...SpkUfcdPai9uVYYU"
}
```

Figure 1

3.1. "service" JWS header parameter

The "service" JWS header parameter specifies the service for which TLS server certificate should be issued. Valid values come from "Service Names and Transport Protocol Port Numbers" IANA registry <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>. ACME server MAY include SRV-ID [RFC6125] subjectAltNames in issued certificates.

3.2. "port" JWS header parameter

The "port" JWS header parameter specifies the TCP port number where the corresponding service is running.

[[This parameter might have applicability beyond email services.]]

3.3. TLS with Server Name Indication (SNI) challenge for email services

"tls-sni-email-00" is very similar to "tls-sni-01" defined in Section 8.3 of [I-D.ietf-acme-acme].

The difference between processing of "tls-sni-email-00" and "tls-sni-01" are listed below:

1. SAN A MUST be constructed as follows: compute the SHA-256 digest [FIPS180-4] of the challenge token and encode it in lowercase hexadecimal form. The dNSName is "<x>.<y>.<token>.acme.invalid", where <x> is the first half of the hexadecimal representation and <y> is the second half, and <token> was generated by the ACME server. SAN B MUST be constructed as follows: compute the SHA-256 digest of the key authorization and encode it in lowercase hexadecimal form. The dNSName is "<x>.<y>.<ka>.acme.invalid" where <x> is the first half of the hexadecimal representation and <x> is the second half, and <ka> is the key authorization. [[OPEN ISSUE: Should service name and port number be incorporated into SAN A and B?]]

2. When verifying the client's control of the domain/service, ACME server connects to port as specified in "port" JWS header parameter (Section 3.2), instead of port 443. When connecting to ports 25, 143 and 587, ACME server needs to use STARTTLS command. When connecting to ports 465 or 993, ACME server initiate TLS negotiation immediately upon connection to the corresponding ports. In all cases ACME server presents SAN A in the SNI field, constructed as specified above.

3.4. DNS challenge for email services

"dns-email-00" is very similar to "dns-01" defined in Section 8.4 of [I-D.ietf-acme-acme].

The difference between processing of "dns-email-00" and "dns-01" are listed below:

1. The TXT record used to validate this challenge is _<port>._<service>_acme-challenge.<domain>. For example, for domain "example.com" and IMAP service running on port 993, the

TXT record name is _993._imaps._acme-challenge.example.com. For domain "example.net" and IMAP service running on port 143, the TXT record name is _143._imap._acme-challenge.example.next.

2. [[OPEN ISSUE: Should service name and port number be incorporated into the hash?]]

3.5. CAPABILITY challenge for email services

For "capability-smtp-00" challenge, ACME client (== SMTP server) constructs a key authorization from the "token" value provided in the challenge and the client's account key. The client then computes the SHA-256 digest [FIPS180-4] of the key authorization. SMTP server than returns the base64url encoding of this digest as a value of the "ACME" EHLO capability:

```
250-smtp.example.com
250-SIZE
250-8BITMIME
250-BINARYMIME
250-PIPELINING
250-HELP
250-DSN
250-CHUNKING
250-AUTH SCRAM-SHA-1
250-AUTH=SCRAM-SHA-1
250-STARTTLS
250-ACME gfj9Xq...Rg85nM
250-MT-PRIORITY
250 ENHANCEDSTATUSCODES
```

Figure 2

Similarly, "capability-imap-00" challenge, ACME client (== IMAP server) constructs a key authorization from the "token" value provided in the challenge and the client's account key. The client then computes the SHA-256 digest [FIPS180-4] of the key authorization. SMTP server than returns the base64url encoding of this digest as a value of the "ACME" capability:

```
* OK [CAPABILITY IMAP4rev1 LOGINDISABLED LITERAL+ ENABLE STARTTLS
ACME=gfj9Xq...Rg85nM] Example IMAP4rev1 server ready
```

or

```
* CAPABILITY IMAP4rev1 LOGINDISABLED LITERAL+ ENABLE STARTTLS
ACME=gfj9Xq...Rg85nM
```

Figure 3

4. 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 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 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?]]

5. Open Issues

[[This section should be empty before publication]]

1. One possible alternative for issuing TLS certificates for email services is to define a new Identifier Type that specifies service@domain. The current version of the document just reuses "dns".

6. IANA Considerations

IANA is requested to register the following ACME challenge types that are used with Identifier Type "dns": "tls-sni-email", "dns-email",

"capability-smtp" and "capability-imap". The reference for all of them is this document.

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.

7. Security Considerations

TBD.

8. Normative References

[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>.

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, DOI 10.17487/RFC3501, March 2003, <http://www.rfc-editor.org/info/rfc3501>.

[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>.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, DOI 10.17487/RFC6125, March 2011, <http://www.rfc-editor.org/info/rfc6125>.

[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.

Author's Address

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

EMail: Alexey.Melnikov@isode.com