

Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 9, 2020

A. Melnikov
Isode Ltd
July 8, 2019

Extensions to JMAP for S/MIME signature verification
draft-ietf-jmap-smime-00

Abstract

This document specifies extension to JMAP for returning S/MIME signature verification status.

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 January 9, 2020.

Copyright Notice

Copyright (c) 2019 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

1. Introduction	2
2. Conventions Used in This Document	2
3. Addition to the capabilities object	2
4. Extension to Email/get for S/MIME signature verification . .	2
5. Open Issues	4
6. IANA Considerations	4
6.1. JMAP capability registration for "smime"	4
7. Security Considerations	5
8. Normative References	5
Author's Address	5

1. Introduction

[I-D.ietf-jmap-mail] is a JSON based application protocol for synchronising email data between a client and a server.

This document describes an extension to JMAP for returning S/MIME [RFC8551] signature verification status, without requiring a JMAP client to download the signature and all signed body parts or to download and decode CMS.

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. Addition to the capabilities object

The capabilities object is returned as part of the standard JMAP Session object; see the JMAP spec. Servers supporting `_this_` specification MUST add a property called "urn:ietf:params:jmap:smime" to the capabilities object.

The value of this property is an empty object in both the JMAP session `_capabilities_` property and an account's `_accountCapabilities_` property.

4. Extension to Email/get for S/MIME signature verification

[I-D.ietf-jmap-mail] defines Email/get method for retrieving message specific information. This document defines the following pseudo values in the `_properties_` argument:

- o `*smimeStatus*`: If "smimeStatus" is included in the list of requested properties, it MUST be interpreted by the server as a request to return "smimeStatus" property.

The "smimeStatus" response property is defined as follows:

smimeStatus: "String|null". null signifies that the message doesn't contain any signature. Possible string values of the property are listed below. Servers MAY return other values not defined below. Client MUST treat unrecognized values as "unknown":

unknown S/MIME message, but it is neither signed, nor encrypted. This can also be returned for a multipart/signed message which contains unrecognized signing protocol (for example OpenPGP).

signed S/MIME signed message, but the signature was not yet verified. Some servers might not attempt to verify signature until a particular message is requested by the client.

signed/verified S/MIME signed message and the sender's signature was successfully verified, sender matches the From header field and the sender's certificate (and the certificate chain) is trusted for signing.

signed/failed S/MIME signed message, but the signature failed to verify. This might be a policy related decision (message signer doesn't match the From header field), message was modified, the signer's certificate has expired or was revoked, etc.

```
[ "Email/get", {  
  "ids": [ "f123u987" ],  
  "properties": [ "mailboxIds", "from", "subject", "date", "smimeStatus" ]  
}, "#1"]
```

This will result in the following response:

```
[[ "Email/get", {  
  "accountId": "abc",  
  "state": "41234123231",  
  "list": [  
    {  
      id: "f123u457",  
      mailboxIds: { "f123": true },  
      from: [{name: "Joe Bloggs", email: "joe@bloggs.com"}],  
      subject: "Dinner on Thursday?",  
      date: "2013-10-13T14:12:00Z",  
      smimeStatus: "signed/verified"  
    }  
  ]  
}, "#1"]]
```

Example

5. Open Issues

[[This section should be empty before publication]]

6. IANA Considerations

6.1. JMAP capability registration for "smime"

IANA is requested to register the "smime" JMAP Capability as follows:

Capability Name: "urn:ietf:params:jmap:smime"

Specification document: this document

Intended use: common

Change Controller: IETF

Security and privacy considerations: this document, Section 7

7. Security Considerations

Server side S/MIME signature verification requires the client to trust server verification code and configuration to perform S/MIME signature verification. For example, if the server is not configured with some Trust Anchors, some messages will have "signed/failed" status instead of "signed/verified".

TBD.

8. Normative References

[I-D.ietf-jmap-core]

Jenkins, N. and C. Newman, "JSON Meta Application Protocol", draft-ietf-jmap-core-17 (work in progress), March 2019.

[I-D.ietf-jmap-mail]

Jenkins, N. and C. Newman, "JMAP (JSON Meta Application Protocol) for Mail", draft-ietf-jmap-mail-16 (work in progress), March 2019.

[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>>.

[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>>.

Author's Address

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

EMail: Alexey.Melnikov@isode.com