Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 3, 2021

A. Melnikov
Isode Ltd

July 2, 2020

S/MIME signature verification extension to JMAP
draft-ietf-jmap-smime-02

Abstract

This document specifies an 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 3, 2021.

Copyright Notice

Table of Contents

1. Introduction

[RFC8621] 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 body part and all signed body parts (when multipart/signed media type is used) or to download and decode CMS (when application/pkcs7-mime media type is used).

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

[RFC8621] 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" response property.
o *smimeErrors*: If "smimeErrors" is included in the list of requested properties, it MUST be interpreted by the server as a request to return "smimeErrors" response property.
o *smimeVerifiedAt*: If "smimeVerifiedAt" is included in the list of requested properties, it MUST be interpreted by the server as a request to return "smimeVerifiedAt" response property.

The "smimeStatus" response property is defined as follows:

smimeStatus: "String|null". null signifies that the message doesn't contain any signature. This property contains the S/MIME signature and certificate verification status calculated according to [RFC8551] and [RFC8550]. Possible string values of the property are listed below. Servers MAY return other values not defined below. Client MUST treat unrecognized values as "unknown" or "signed/failed". Note that the value of this property might change over time.

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. JMAP servers compliant with this document SHOULD return "signed/verified" or "signed/failed" instead of this signature status.

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.

The "smimeErrors" response property is defined as follows:

smimeErrors: "String[]|null". null signifies that the message doesn't contain any signature or that there were no errors when verifying S/MIME signature. (I.e. this property is non null only when the corresponding "smimeStatus" response property value is "signed/failed".) Each string in the array is a human readable description (in the language specified in Content-Language header field, if any)

of a problem with the signature or the signing certificate. (See Section 3.8 of [RFC8620] in regards to how this is affected by the language selection.) For example, the signing certificate might be expired and the message From email address might not correspond to any of the email addresses in the signing certificate. Or the certificate might be expired and the JMAP server might be unable to retrieve CRL for the certificate. In both of these cases there would be 2 elements in the array.

The "smimeVerifiedAt" response property is defined as follows:

smimeVerifiedAt: "UTCDate|null" (server-set). null signifies that the message doesn't contain any S/MIME signature or that there is a signature, but there was no attempt to verify it. In all other cases it is set to the date and time of when S/MIME signature was verified the last time.

"smimeStatus" and "smimeErrors" values are calculated at the time the corresponding JMAP request was processed, not at the time when the message was generated (according to it's Date header field value). It MAY be calculated at the time the message was delivered to the mailbox. In all cases "smimeVerifiedAt" is set to time when "smimeStatus" and "smimeErrors" were last updated. As recalculating these values is expensive for the server they MAY be cached for up to 10 minutes from the moment when they were calculated.

```
["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.example.net"}],
       subject: "Dinner tonight?",
       date: "2020-07-07T14:12:00Z",
       smimeStatus: "signed/verified"
     }
   ]
}, "#1"]]
```

Example 1:

```
        ["Email/get", {
        "ids": [ "af123u123" ],
        "properties": [ "mailboxIds", "from", "subject", "date",
         "smimeStatus", "smimeErrors", "smimeVerifiedAt" ]
        }, "#1"]
```

This will result in the following response:

```
        [["Email/get", {
           "accountId": "abc",
           "state": "41234123231",
           "list": [
             {
               id: "af123u123",
               mailboxIds: { "f123": true },
               from: [{name: "Jane Doe",
                       email: "jdoe@example.com"}],
               subject: "Company takeover",
               date: "2020-01-31T23:00:00Z",
               smimeStatus: "signed/failed",
               smimeErrors: [
                 "From email address doesn't match the certificate",
                 "Can't retrieve CRL from the CRL URL"],
               "smimeVerifiedAt": "2020-03-01T12:11:19Z"
             }
           ]
        }, "#1"]]
```

Example 2:

5. Open Issues

[[This section should be empty before publication]]

1. Should a new property be added on requests to allow signature verification "at specified time"?

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".

Constant recalculation of S/MIME signature status can result in Denial-of-Service condition. For that reason it is RECOMMENDED to cache results of signature verification for 10 minutes.

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, <https://www.rfc-editor.org/info/rfc2119>.

[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>.

[RFC8620] Jenkins, N. and C. Newman, "The JSON Meta Application Protocol (JMAP)", RFC 8620, DOI 10.17487/RFC8620, July 2019, <https://www.rfc-editor.org/info/rfc8620>.

[RFC8621] Jenkins, N. and C. Newman, "The JSON Meta Application Protocol (JMAP) for Mail", RFC 8621, DOI 10.17487/RFC8621, August 2019, <https://www.rfc-editor.org/info/rfc8621>.

Author's Address

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

EMail: Alexey.Melnikov@isode.com