Stream: Internet Engineering Task Force (IETF)
RFC: 9219
Category: Standards Track
Published: April 2022
ISSN: 2070-1721
Author: A. Melnikov
Isode Ltd

RFC 9219
S/MIME Signature Verification Extension to the JSON Meta Application Protocol (JMAP)

Abstract

This document specifies an extension to "The JSON Meta Application Protocol (JMAP) for Mail" (RFC 8621) for returning the S/MIME signature verification status.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9219.

Table of Contents

1. Introduction

JMAP for Mail [RFC8621] is a JSON-based application protocol for synchronizing email data between a client and a server.

This document describes an extension to JMAP for returning the S/MIME signature verification status [RFC8551], without requiring a JMAP client to download the signature body part and all signed body parts (when the multipart/signed media type [RFC1847] is used) or to download and decode the Cryptographic Message Syntax (CMS) (when the application/pkcs7-mime media type (Section 3.2 of [RFC8551]) is used). The use of the extension implies the client trusts the JMAP server's S/MIME signature verification code and configuration. This extension is suitable for cases where reduction in network bandwidth and client-side code complexity outweigh security concerns about trusting the JMAP server to perform S/MIME signature verifications. One possible use case is when the same organization controls both the JMAP server and the JMAP client.

2. Conventions Used in This Document

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Type signatures, examples, and property descriptions in this document follow the conventions established in Section 1.1 of [RFC8620]. Data types defined in the core specification are also used in this document.

3. Addition to the Capabilities Object

The **capabilities** object is returned as part of the standard JMAP Session object; see Section 2 of [RFC8620]. Servers supporting this specification **MUST** add a property called "urn:ietf:params:jmap:smimeverify" 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 for S/MIME Signature Verification

4.1. Extension to Email/get

[RFC8621] defines the Email/get method for retrieving message-specific information. This document defines the following pseudo values in the *properties* argument:

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

smimeStatusAtDelivery:
: If "smimeStatusAtDelivery" is included in the list of requested properties, it **MUST** be interpreted by the server as a request to return the "smimeStatusAtDelivery" response property. (It is effectively the same as the "smimeStatus" value calculated at the date/time of delivery, as specified by "receivedAt".)

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

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

The "smimeStatus" response property is defined as follows:

smimeStatus:
"String|null" (server-set). null signifies that the message doesn't contain any signature. Otherwise, this property contains the S/MIME signature and certificate verification status calculated according to [RFC8551], [RFC8550], and [RFC5280]. Possible string values of the property are listed below. Servers **MAY** return other values not defined below, as defined in extensions to this document. Clients **MUST** treat unrecognized values as "unknown" or "signed/failed". Note that the value of this property might change over time.

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

signed:
An S/MIME signed message, but the signature was not yet verified. Some servers might not attempt to verify a signature until a particular message is requested by the client. (This is a useful optimization for a JMAP server to avoid doing work until exact information is needed. A JMAP client that only needs to display an icon that signifies presence of an S/MIME signature can still use this value.) JMAP servers compliant with this document **SHOULD** attempt signature verification and return "signed/verified" or "signed/failed" instead of this signature status.

signed/verified:
An S/MIME signed message, and the sender's signature was successfully verified according to [RFC8551] and [RFC8550]. Additionally, the signer email address extracted from the S/MIME certificate matches the From header field value, and the signer certificate **SHOULD** be checked for revocation.

signed/failed:
S/MIME signed message, but the signature failed to verify according to [RFC8551] and [RFC8550]. This might be because of a policy-related decision (e.g., the message signer email address doesn't match the From header field value), the message was modified, the signer's certificate has expired or was revoked, etc.

encrypted+signed/verified:
This value is reserved for future use. It is typically handled in the same way as "signed/verified".

encrypted+signed/failed:
This value is reserved for future use. It is typically handled in the same way as "signed/failed".

The "smimeStatusAtDelivery" response property has the same syntax as "smimeStatus" but is calculated in relationship to the "receivedAt" date/time. Unlike "smimeStatus", the "smimeStatusAtDelivery" response property value doesn't change unless trust anchors are added. (For example, addition of a trust anchor can change the value of a message

"smimeStatusAtDelivery" property from "signed/failed" to "signed/verified". Note that trust anchor removal doesn't affect this response property.) The "smimeStatusAtDelivery" response property value allows clients to compare the S/MIME signature verification status at delivery with the current status as returned by "smimeStatus", for example, to help to answer questions like "was the signature valid at the time of delivery?".

Note that the "smimeStatusAtDelivery" response property value doesn't have to be calculated at delivery time. A JMAP server can defer its calculation until it is explicitly requested; however, once it is calculated, its value is remembered for later use.

The "smimeErrors" response property is defined as follows:

smimeErrors:
: "String[]|null" (server-set). null signifies that the message doesn't contain any signature or that there were no errors when verifying the S/MIME signature. (That is, this property is non-null only when the corresponding "smimeStatus" response property value is "signed/failed" or "encrypted+signed/failed". Note that future extensions to this document can specify other "smimeStatus" values that can be used with "smimeErrors".) Each string in the array is a human-readable description (in the language specified in the Content-Language header field, if any) of a problem with the signature, the signing certificate, or the signing certificate chain. (See Section 3.8 of [RFC8620] in regards to how this is affected by the language selection.) In one 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. In another example, the certificate might be expired and the JMAP server might be unable to retrieve a Certificate Revocation List (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. (Retrieval of the "smimeStatus" value can be used to distinguish these 2 cases). In all other cases, it is set to the date and time of when the S/MIME signature was most recently verified. Note that a request to fetch "smimeStatus", "smimeStatusAtDelivery", and/or "smimeErrors" would force this response property to be set to a non-null value if an S/MIME signature exists.

The "smimeStatus" and "smimeErrors" values are calculated at the time the corresponding JMAP request is processed (but see below about the effect of result caching), not at the time when the message is generated (according to its Date header field value). In all cases, "smimeVerifiedAt" is set to the time when "smimeStatus" and "smimeErrors" were last updated. As recalculating these values is expensive for the server, they **MAY** be cached for up to 24 hours from the moment when they were calculated.

Example 1: Retrieval of minimal information about a message, including its From, Subject, and Date header fields, as well as the S/MIME signature verification status at delivery and date/time when the message was received.

```
["Email/get", {
"ids": [ "fe123u457" ],
"properties": [ "mailboxIds", "from", "subject", "date",
 "smimeStatusAtDelivery", "receivedAt" ]
}, "#1"]
```

This might result in the following response:

```
[["Email/get", {
   "accountId": "abc",
   "state": "51234123231",
   "list": [
     {
       "id": "fe123u457",
       "mailboxIds": { "f123": true },
       "from": [{"name": "Joe Bloggs",
               "email": "joe@bloggs.example.net"}],
       "subject": "Dinner tonight?",
       "date": "2020-07-07T14:12:00Z",
       "smimeStatusAtDelivery": "signed/verified",
       "receivedAt": "2020-07-07T14:15:18Z"
     }
   ]
}, "#1"]]
```

Example 2: Retrieval of minimal information about a message, including its From, Subject, and Date header fields, as well as the latest S/MIME signature verification status, S/MIME verification errors (if any), and when the S/MIME signature status was last verified. The response contains 2 S/MIME errors related to S/MIME signature verification.

```
["Email/get", {
"ids": [ "ag123u123" ],
"properties": [ "mailboxIds", "from", "subject", "date",
 "smimeStatus", "smimeErrors", "smimeVerifiedAt" ]
}, "#1"]
```

This might result in the following response:

```
[["Email/get", {
   "accountId": "abc",
   "state": "47234123231",
   "list": [
     {
       "id": "ag123u123",
       "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"]]
```

4.1.1. "smimeStatus" Response Property Extensibility

Future extensions to this document can specify extra allowed values for the "smimeStatus" response property. All values (defined in this document or in extensions to this document) **MUST** be in ASCII. (Note that this response property contains tokens; thus, it is not subject to internationalization or localization).

New "smimeStatus" response property values defined in extensions may affect the behavior of properties, such as the "smimeErrors" response property of Email/get (see Section 4.1) or the "hasVerifiedSmime" property of Email/query (see Section 4.2). In particular, the new values can be treated similarly to values defined in this document.

For example, a putative JMAP extension for automatically decrypting S/MIME messages can specify two additional values, one specifying that a message is both encrypted and signed with a valid S/MIME signature (e.g. "encrypted+signed/verified") and another one specifying that a message is both encrypted and signed with an invalid S/MIME signature (e.g. "encrypted+signed/failed"). The former value can be treated as "signed/verified" (and would thus affect "hasVerifiedSmime") and the latter can be treated as "signed/failed" (and thus can be used with "smimeErrors").

4.2. Extension to Email/query

[RFC8621] defines the Email/query method for searching for messages with specific properties. This document defines the following properties of the **FilterCondition** object:

hasSmime:
: "Boolean". If "hasSmime" has the value true, only messages with "smimeStatus" other than null match the condition. If "hasSmime" has the value false, only messages with "smimeStatus" equal to null match the condition.

hasVerifiedSmime:
"Boolean". If "hasVerifiedSmime" has the value true, only messages with "smimeStatus" equal to "signed/verified" or "encrypted+signed/verified" (*) match the condition. If "hasVerifiedSmime" has the value false, only messages with "smimeStatus" not equal to "signed/verified" and not equal to "encrypted+signed/verified" (*) (including the value null) match the condition. Note that use of this attribute is potentially expensive for a JMAP server, as it forces calculation of the "smimeStatus" property value for each message. However, caching of the "smimeStatus" values should ameliorate this cost somewhat.

(*) as well as the "smimeStatus" values added by future extensions to this document that are explicitly specified as having similar effect to "signed/verified" as far as "hasVerifiedSmime" calculation is concerned.

hasVerifiedSmimeAtDelivery:
"Boolean". The "hasVerifiedSmimeAtDelivery" property is handled similarly to the "hasVerifiedSmime" property, but the value of "smimeStatusAtDelivery" is used instead of "smimeStatus" to assess whether a particular message matches the condition.

4.3. Interaction with Email/changes

Changes to the "smimeVerifiedAt" response property value **MUST NOT** cause the message to be included in the "updated" argument of the Email/changes response. However, changes to the "smimeStatus", "smimeStatusAtDelivery", and/or "smimeErrors" response properties **MUST** result in message inclusion in the "updated" argument of the Email/changes response.

5. IANA Considerations

5.1. JMAP Capability Registration for "smimeverify"

IANA has registered the "smimeverify" JMAP capability as follows:

Capability Name: urn:ietf:params:jmap:smimeverify
Specification document: RFC 9219
Intended use: common
Change Controller: IETF
Security and privacy considerations: RFC 9219, Section 6

6. Security Considerations

Use of the server-side S/MIME signature verification JMAP extension requires the client to trust the server signature verification code, the server configuration, and the server's operational practices to perform S/MIME signature verification, as well as to trust that the channel between the client and the server is integrity protected. (For example, if the server is not configured with some trust anchors, some messages will have the "signed/failed" status instead of "signed/verified".) A malicious or compromised server could return a false verification status to a client.

A successful verification could be conveyed to a client for a forged or altered message. A properly signed message could be signaled as having a failed signature verification or no signature at all. In the case of the latter attack, no new attack surface is presented with this extension above what a malicious or compromised server could already do by stripping or tampering with the S/MIME information in the message. In the case of the former attack, client software capable of performing S/MIME signature verification could detect this attack. Local configuration of the client should determine if this client-side verification should occur. For clients without local verification capabilities, such an attack would be difficult to detect.

Integrity protection of the channel between the client and the server is provided by use of TLS, as required by the JMAP specification (see Section 8.1 of [RFC8620]).

Constant recalculation of the S/MIME signature status can result in a denial-of-service condition. For that reason, it is **RECOMMENDED** that servers cache results of signature verification for up to 24 hours.

7. References

7.1. 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>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[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>.

7.2. Informative References

[RFC1847] Galvin, J., Murphy, S., Crocker, S., and N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", RFC 1847, DOI 10.17487/RFC1847, October 1995, <https://www.rfc-editor.org/info/rfc1847>.

Acknowledgements

This document is a product of the JMAP Working Group. Special thank you to Bron Gondwana, Neil Jenkins, Murray Kucherawy, Kirsty Paine, Benjamin Kaduk, Roman Danyliw, Peter Yee, Robert Wilton, Erik Kline, and Menachem Dodge for suggestions, comments, and corrections to this document.

Author's Address

Alexey Melnikov
Isode Ltd
14 Castle Mews
Hampton, Middlesex
TW12 2NP
United Kingdom
Email: Alexey.Melnikov@isode.com