Authentication-Results Registration for S/MIME Signature Verification

Abstract

RFC 7001 specifies the Authentication-Results header field for conveying results of message authentication checks. This document defines a new authentication method to be used in the Authentication-Results header field for S/MIME-related signature checks.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7281.

Copyright Notice

Copyright (c) 2014 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 (http://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.
1. Introduction

[RFC7001] specifies the Authentication-Results header field for conveying results of message authentication checks. As S/MIME signature verification (and alteration) is sometimes implemented in border message transfer agents, guards, and gateways (for example, see [RFC3183]), there is a need to convey signature verification status to Mail User Agents (MUAs) and downstream filters. This document defines a new authentication method to be used in the Authentication-Results header field for S/MIME-related signature checks.

2. Conventions Used in This Document

The formal syntax uses the Augmented Backus-Naur Form (ABNF) [RFC5234] notation, including the core rules defined in Appendix B of [RFC5234].

3. "smime" Authentication Method

S/MIME signature and countersignature verification is represented by the "smime" method and is defined in [RFC5751].
3.1. S/MIME Results

The result values used by S/MIME [RFC5751] are as follows:

<table>
<thead>
<tr>
<th>Result code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>The message was not signed.</td>
</tr>
<tr>
<td>pass</td>
<td>The message was signed, the signature or signatures were acceptable to the verifier, and the signature(s) passed verification tests.</td>
</tr>
<tr>
<td>fail</td>
<td>The message was signed and the signature or signatures were acceptable to the verifier, but they failed the verification test(s).</td>
</tr>
<tr>
<td>policy</td>
<td>The message was signed and signature(s) passed verification tests, but the signature or signatures were not acceptable to the verifier.</td>
</tr>
<tr>
<td>neutral</td>
<td>The message was signed but the signature or signatures contained syntax errors or were not otherwise able to be processed. This result is also used for other failures not covered elsewhere in this list.</td>
</tr>
<tr>
<td>temperror</td>
<td>The message could not be verified due to some error that is likely transient in nature, such as a temporary inability to retrieve a certificate or Certificate Revocation List (CRL). A later attempt may produce a final result.</td>
</tr>
<tr>
<td>permerror</td>
<td>The message could not be verified due to some error that is unrecoverable, such as a required header field being absent or the signer’s certificate not being available. A later attempt is unlikely to produce a final result.</td>
</tr>
</tbody>
</table>

A signature is "acceptable to the verifier" if it passes local policy checks (or there are no specific local policy checks). For example, a verifier might require that the domain in the rfc822Name subjectAltName in the signing certificate matches the domain in the address of the sender of the message (value of the Sender header field, if present; value of the From header field otherwise), thus making third-party signatures unacceptable. [RFC5751] advises that
if a message fails verification, it should be treated as an unsigned message. A report of "fail" here permits the receiver of the report to decide how to handle the failure. A report of "neutral" or "none" preempts that choice, ensuring that the message will be treated as if it had not been signed.

3.2. Email Authentication Parameters for S/MIME

This document defines several new authentication parameters for conveying S/MIME-related information, such as the location of an S/MIME signature and the identity associated with the entity that signed the message or one of its body parts.

3.2.1. body.smime-part

body.smime-part contains the MIME body part reference that contains the S/MIME signature. The syntax of this property is described by the smime-part ABNF production below. application/pkcs7-signature or application/pkcs7-mime (containing SignedData) media type body parts are referenced using the <section> syntax (see Section 6.4.5 of [RFC3501]). If the signature being verified is encapsulated by another Cryptographic Message Syntax (CMS) content type (e.g., application/pkcs7-mime containing EnvelopedData, which contains SignedData), such an inner signature body part can be referenced using "section[/section..." syntax.

body.smime-part = section ["/" smime-subpart]
smime-subpart = smime-part
section = <Defined in Section 6.4.5 of [RFC3501]>

3.2.2. body.smime-identifier

body.smime-identifier contains the email address [RFC5322] associated with the S/MIME signature referenced in the corresponding body.smime-part. The email address can be specified explicitly in the signer’s X.509 certificate or derived from the identity of the signer. Note that this email address can correspond to a countersignature.
3.2.3. **body.smime-serial** and **body.smime-issuer**

`body.smime-serial` contains the `serialNumber` of the X.509 certificate associated with the S/MIME signature (see Section 4.1.2.2 of [RFC5280]) referenced in the corresponding `body.smime-part`.

`body.smime-issuer` contains the issuer name DN (distinguished name) (e.g., "CN=CA1,ST=BC,c=CA") of the X.509 certificate associated with the S/MIME signature (see Section 4.1.2.4 of [RFC5280]) referenced in the corresponding `body.smime-part`.

Either both or neither of `body.smime-serial` and `body.smime-issuer` should be present in an Authentication-Results header field.

`body.smime-serial` and `body.smime-issuer` are used for cases when `body.smime-identifier` (email address) can’t be derived by the entity adding the corresponding Authentication-Results header field. For example, this can be used when gatewaying from X.400.

3.3. **Examples**

```plaintext
Return-Path: <aliceDss@example.com>
Authentication-Results: example.net;
    smime=fail (certificate is revoked by CRL)
    body.smime-identifier=aliceDss@example.com
    body.smime-part=2
Received: from ietfa.example.com (localhost [IPv6:::1])
    by ietfa.example.com (Postfix) with ESMTP id 2875111E81A0;
    Fri, 06 Sep 2002 00:35:14 -0700 (PDT)
MIME-Version: 1.0
To: User2@example.com
From: aliceDss@example.com
Subject: Example 4.8
Message-Id: <020906002550300.249@example.com>
Date: Fri, 06 Sep 2002 00:25:21 -0700
Content-Type: multipart/signed;
    micalg=SHA1;
    boundary="-----_NextBoundary____Fri,_06_Sep_2002_00:25:21";
    protocol="application/pkcs7-signature"
```
This is a multi-part message in MIME format.

------=_NextBoundary____Fri,_06_Sep_2002_00:25:21

This is some sample content.

------=_NextBoundary____Fri,_06_Sep_2002_00:25:21

Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s

MIIDdwYJKoZIhvcNAQcCoIIDaDCCCA2DCAQExCTAHBgUrDgMCGjALBkgkqhkIg9w0BBwGgggL
gMIIC3DCCApugAwIBAgICASICwCQQH3TiwOIQgEzASMRARwDgVyg9DEWdDXYJsaQFNTM2dXDT
k5MDgXZAxMTA0T0oXDTM5MTIzMTIzNTk1OwoWxA ERA8GA1UEAxMiQWxpY2VEU1MwggG2MIIBKwY
HkoZIgjgEATCCAR4gYEAgY3N7YQpCp45PSJIKKrkR5PdDteoDuxTxaUECE1/0Fz
SH4MvWESNH+n6+koykwk4dwyDbeP5u/t0zcX2mK5HXQXnywvRCJW3b3qe+fx0ny/dQ6iLVPE
/sAcCIR01iMPdtbRjQVh1112EMR4v+dsISXN/4kURu15AmWXPN+W9sCFQDiR6YrWA4e8E
baj7g3IStii/eTzQKBgCY40B5MjMg0+5zt2Ut2axx2IzkEAjVc8sاناMMEy4f3dm1nizaroF
VjaE612uG4r32QkiWh9HXP7scheSz6O+G3gnMkhijt2F0nOL12j8B80jibyvMAF8BuUmJEYk2
RL34yJKVU1a14v1z7BphNh8Rf8K9f7QFQ/5h0wTB3SaM5ujY5A4GEAAkB9zju'VpFJYLqXr
d4z+pT7xe3L2exX0phaJKBEj2TSGZ2V1ExI9Q1tv5VG/+onyohs/JH09B41bY8i7RaWgSu
OF1s4Gg/idI34a8iSrUxq4iw0e7wi/ZhSAXGksZfoVi/G7NNTs1jF2UYeMyDKEH85BQP1Gp
2NOM/K14Tyg+W4o4GBM8h8wDAYDVR0TAQ/8BAIwADAOBgNVHdMQ8BAf8EBAMCBsAwHwYDVVR0j
BBg/woAUCESQ+g5ivh95K03JxPS8QyuvT8R8wHQvYDVR0BBYEFL5obp9jwfttQ3CkzhMB4v3j
1/7NMB8GAI1EdQQYMBaBEFsaW/k1RFNtT9QV4YWlwbGUyY29tMAKBByqGSM49BAMDAwLQ
1UVQyktJG5C4Lx1j0Ng2qI1FwvUQFCyYVNSVA1cst3a53ld4h6VW0NeTfJjM5GECAGEW
DASMRAwDgYDVQQDEwdYXJnsFNTAgIAYAHB9UrDgMCGjAlBgcqhkj0QAQDBCAwLAIUM/mG
f6gkq920XtRdGimJeB/BxUCGFFJqwYr1WYc1OQoGiaawGzV

------=_NextBoundary____Fri,_06_Sep_2002_00:25:21--
4. IANA Considerations

IANA has added the following entries to the "Email Authentication Methods" sub-registry of the "Email Authentication Parameters" registry:

<table>
<thead>
<tr>
<th>Method</th>
<th>Defined in</th>
<th>ptype</th>
<th>Property</th>
<th>Value</th>
<th>Status</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>smime</td>
<td>[RFC5751]</td>
<td>body</td>
<td>smime-part</td>
<td>A reference to the MIME body part that contains the signature, as defined in Section 3.2.1 of [RFC7281].</td>
<td>active</td>
<td>1</td>
</tr>
<tr>
<td>smime</td>
<td>[RFC5751]</td>
<td>body</td>
<td>smime-identifier</td>
<td>The email address [RFC5322] associated with the S/MIME signature. The email address can be specified explicitly or derived from the identity of the signer. Note that this email address can correspond to a counter-signature.</td>
<td>active</td>
<td>1</td>
</tr>
<tr>
<td>Code</td>
<td>Defined</td>
<td>Auth Method</td>
<td>Meaning</td>
<td>Status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
<td>-------------</td>
<td>----------------------------------------------</td>
<td>--------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>none</td>
<td>[RFC7281]</td>
<td>smime</td>
<td>[RFC7281] Section 3.1</td>
<td>active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pass</td>
<td>[RFC7281]</td>
<td>smime</td>
<td>[RFC7281] Section 3.1</td>
<td>active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fail</td>
<td>[RFC7281]</td>
<td>smime</td>
<td>[RFC7281] Section 3.1</td>
<td>active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>policy</td>
<td>[RFC7281]</td>
<td>smime</td>
<td>[RFC7281] Section 3.1</td>
<td>active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>neutral</td>
<td>[RFC7281]</td>
<td>smime</td>
<td>[RFC7281] Section 3.1</td>
<td>active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>temperror</td>
<td>[RFC7281]</td>
<td>smime</td>
<td>[RFC7281] Section 3.1</td>
<td>active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>permerror</td>
<td>[RFC7281]</td>
<td>smime</td>
<td>[RFC7281] Section 3.1</td>
<td>active</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IANA has added the following entries to the "Email Authentication Result Names" sub-registry of the "Email Authentication Parameters" registry:
5. Security Considerations

This document doesn’t add new security considerations not already covered by [RFC7001] and [RFC5751]. In particular, security considerations related to the use of weak cryptography over plaintext, weakening and breaking of cryptographic algorithms over time, and changing the behavior of message processing based on presence of a signature specified in [RFC5751] are relevant to this document. Similarly, the following security considerations specified in [RFC7001] are particularly relevant to this document: Forged Header Fields, Misleading Results, Internal Mail Transfer Agent (MTA) Lists, and Compromised Internal Hosts.

To repeat something already mentioned in RFC 7001, Section 7.1:

An MUA or filter that accesses a mailbox whose messages are handled by a non-conformant MTA, and understands Authentication-Results header fields, could potentially make false conclusions based on forged header fields. A malicious user or agent could forge a header field using the DNS domain of a receiving ADMD as the authserv-id token in the value of the header field and, with the rest of the value, claim that the message was properly authenticated. The non-conformant MTA would fail to strip the forged header field, and the MUA could inappropriately trust it.

For this reason, it is best not to have processing of the Authentication-Results header field enabled by default; instead, it should be ignored, at least for the purposes of enacting filtering decisions, unless specifically enabled by the user or administrator after verifying that the border MTA is compliant. It is acceptable to have an MUA aware of this specification but have an explicit list of hostnames whose Authentication-Results header fields are trustworthy; however, this list should initially be empty.

So, to emphasize this point: whenever possible, MUAs should implement their own S/MIME signature verification instead of implementing this specification.

Note that agents adding Authentication-Results header fields containing S/MIME authentication method might be unable to verify S/MIME signatures inside encrypted CMS content types such as EnvelopedData [RFC5652]. So, agents processing Authentication-Results header fields can’t treat the lack of an Authentication-Results header field with S/MIME authentication method as an indication that the corresponding S/MIME signature is missing, invalid, or valid.
6. References

6.1. Normative References


6.2. Informative References


Appendix A. Acknowledgements

Thank you to Murray S. Kucherawy, David Wilson, Jim Schaad, SM, and Steve Kille for comments and corrections on this document.

Author’s Address

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

EMail: Alexey.Melnikov@isode.com