Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 17, 2014

A. Melnikov
Isode Ltd
March 16, 2014

Authentication-Results Registration for S/MIME signature verification
draft-melnikov-authentication-results-smime-08

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 Internet-Draft will expire on September 17, 2014.

Copyright Notice

Table of Contents

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 (MUA) 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 RFC 5234 [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:

Result code	Meaning
none	The message was not signed.
pass	The message was signed, the signature or signatures were acceptable to the verifier, and the signature(s) passed verification tests.
fail	The message was signed and the signature or signatures were acceptable to the verifier, but they failed the verification test(s).
policy	The message was signed, signature(s) passed verification tests, but the signature or signatures were not acceptable to the verifier.
neutral	The message was signed but the signature or signatures contained syntax errors or were not otherwise able to be processed. This result is also be used for other failures not covered elsewhere in this list.
temperror	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 CRL. A later attempt may produce a final result.
permerror	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.

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, 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 the message will be treated as if it had not been signed.

3.2. Examples

```
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="----=_NextBoundry____Fri,_06_Sep_2002_00:25:21";
    protocol="application/pkcs7-signature"

This is a multi-part message in MIME format.

------=_NextBoundry____Fri,_06_Sep_2002_00:25:21

This is some sample content.
------=_NextBoundry____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

MIIDdwYJKoZIhvcNAQcCoIIDaDCCA2QCAQExCTAHBgUrDgMCGjALBgkqhkiG9w0BBwGgggL
gMIIC3DCCApugAwIBAgICAMgwCQYHKoZIzjgEAzASMRAwDgYDVQQDEwdDYXJsRFNTMB4XDT
k5MDgxNzAxMTA0OVoXDTM5MTIzMTIzNTk1OVowEzERMA8GA1UEAxMIQWxpY2VEU1MwggG2M
IIBKwYHKoZIzjgEATCCAR4CgYEAgY3N7YPqCp45PsJIKKPkR5PdDteoDuxTxauECE//lOFz
SH4M1vNESNH+n6+koYkv4dkwyDbeP5u/t0zcX2mK5HXQNwyRCJWb3qde+fz0ny/dQ6iLVPE
/sAcIR01diMPDtbPjVQh11Tl2EMR4vf+dsISXN/LkURu15AmWXPN+W9sCFQDiR6YaRWa4E8
baj7g3IStii/eTzQKBgCY40BSJMqo5+z5t2UtZakx2IzkEAjVc8ssaMMMeUF3dm1nizaoFP
VjAe6I2uG4Hr32KQiWn9HXPSgheSz6Q+G3qnMkhijt2FOnOLl2jB80jhbgvMAF8bUmJEYk2
RL34yJVKU1a14vlz7BphNh8Rf8K97dFQ/5h0wtGBSmA5ujY5A4GEAAKBgFzjuVp1FJYLqXr
d4z+p7Kxe3L23ExE0phaJKBEj2TSGZ3V1ExI9Q1tv5VG/+onyohs+JH09B41bY8i7RaWgSu
OF1s4GgD/oI34a8iSrUxq4Jw0e7wi/ZhSAXGKsZfoVi/G7NNTSljf2YUeyxDKE8H5BQP1Gp
2NOM/Kl4vTyg+W4o4GBMH8wDAYDVR0TAQH/BAIwADAOBgNVHQ8BAf8EBAMCBsAwHwYDVR0j
BBgwFoAUcEQ+gi5vh95K03XjPSC8QyuT8R8wHQYDVR0OBBYEFL5sobPjwfftQ3CkzhMB4v3
jl/7NMB8GA1UdEQQYMBaBFEFsaWNlRFNTQGV4YW1wbGUuY29tMAkGByqGSM44BAMDMAAwLQ
IUVQykGR9CK4lxIjONg2q1PWdrv0UCFQCfYVNSVAtcst3a53Yd4hBSW0NevTFjMGECAQEwG
DASMRAwDgYDVQQDEwdDYXJsRFNTAgIAyDAHBgUrDgMCGjAJBgcqhkjOOAQDBC4wLAIUM/mG
f6gkgp9Z0XtRdGimJeB/BxUCFGFFJqwYRt1WYcIOQoGiaowqGzVI

------=_NextBoundry____Fri,_06_Sep_2002_00:25:21--
```

4. IANA Considerations

IANA is requested to add the the following entries to the "Email Authentication Methods" subregistry of the "Email Authentication Parameters" registry:

Method	Defined	ptype	property	value
smime	[RFC5751]	body	smime-part	The MIME body part reference which contains the signature. 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 references using the <section> syntax (see Section 6.4.5 of [RFC3501]). If the signature being verified is encapsulated by another CMS content type (e.g. application/pkcs7-mime containing EnvelopedData, which contains SignedData), such inner signature body part can be references using "section[/section..." syntax.
smime	[RFC5751]	body	smime-identifier	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.
smime	[RFC5751]	body	smime-serial	serialNumber of the certificate associated with the S/MIME signature (see section 4.1.2.2 of [RFC5280].
smime	[RFC5751]	body	smime-issuer	Issuer name DN (e.g. "CN=CA1,ST=BC,c=CA") of the certificate associated with the S/MIME signature (see section 4.1.2.4 of [RFC5280].

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

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.

IANA is requested to add the the following entries to the "Email Authentication Result Names" subregistry of the "Email Authentication Parameters" registry:

Code	Defined	Auth Method	Meaning	Status
none	this document	smime	[this memo] Section 3.1	active
pass	this document	smime	[this memo] Section 3.1	active
fail	this document	smime	[this memo] Section 3.1	active
policy	this document	smime	[this memo] Section 3.1	active
neutral	this document	smime	[this memo] Section 3.1	active
temperror	this document	smime	[this memo] Section 3.1	active
permerror	this document	smime	[this memo] Section 3.1	active

5. Security Considerations

This document doesn't add new security considerations not already covered by [RFC7001] and [RFC5751]. In particular security considerations related to use of weak cryptography over plaintext, weakening and breaking of cryptographic algorithms over time, as well as 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 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 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

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, March 2003.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.

[RFC7001] Kucherawy, M., "Message Header Field for Indicating Message Authentication Status", RFC 7001, September 2013.

[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, May 2008.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, January 2010.

6.2. Informative References

[RFC3183] Dean, T. and W. Ottaway, "Domain Security Services using S /MIME", RFC 3183, October 2001.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, September 2009.

[RFC5083] Housley, R., "Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type", RFC 5083, November 2007.

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
5 Castle Business Village
36 Station Road
Hampton, Middlesex TW12 2BX
UK

EMail: Alexey.Melnikov@isode.com