

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: May 15, 2014

A. Melnikov  
Isode Ltd  
November 11, 2013

**Authentication-Results Registration for S/MIME signature verification  
draft-melnikov-authentication-results-smime-05**

**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 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 <http://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 May 15, 2014.

**Copyright Notice**

Copyright (c) 2013 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. 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.





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 SHOULD 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;



Internet-DraftAuthentication-Results Registration for S/MIMNovember 2013

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

MIIDdwYJKoZIhvcNAQcCoIIDaDCCA2QCAQExCTAHBgUrDgMCGjALBgkqhkiG9w0BBwGgggLGMIIC3DCCApugAwIBAgICAMgwCQYHkoZiZjgEAzASMRAdgYDVQQDEwdYXJsRFNTMB4XDTk5MDgxNzAxMTA0VoXDTM5MTIzMTIzNTk1OVowEzERMA8GA1UEAxMIQWxpY2VEU1MwggG2MIIBKwYHkoZiZjgEATCCAR4CgYEAgy3N7YPqCp45PsJIKKPkR5PdDteoDuxTxauECE//l0FzSH4M1vNESNH+n6+koYkv4dkwyDbeP5u/t0zcX2mK5HXQNwyRCJWb3qde+fz0ny/dQ6iLVPE/sAcIR01diMPDtbPjVQh11TL2EMR4vf+dsISXN/LkURu15AmWXPn+W9sCFQDiR6YaRwa4E8baj7g3IStii/eTzQKBgCY40BSJMqo5+z5t2UtZakx2IzKEAjVc8ssaMMMeUF3dm1nizaoFPVjAe6I2uG4Hr32KQiWn9HXPSgheSz6Q+G3qnMkhijt2F0n0LL2jB80jhbgvMAF8bUmJEYk2RL34yJVKU1a14vlz7BphNh8Rf8K97dFQ/5h0wtGBSmA5ujY5A4GEAAKBgFzjuVp1FJYLqXrd4z+p7Kxe3L23ExE0phaJKBj2TSGZ3V1ExI9Q1tv5VG/+onyohs+JH09B41bY8i7RaWgSu0F1s4GgD/oI34a8iSrUxq4Jw0e7wi/ZhSAXGKSzfoVi/G7NNTSljf2YUeyxDKE8H5BQP1Gp2NOM/Kl4vTyg+W4o4GBMH8wDAYDVR0TAQH/BAIwADA0BgNVHQ8BAf8EBAMCBsAwHwYDVR0jBBgwFoAUCEQ+gi5vh95K03XjPSC8QyuT8R8wHQYDVR00BBYEFL5s0bPjwfftQ3CkzhMB4v3jl/7NMB8GA1UdEQQYMBaBFEEsaWNLRFNTQGV4YW1wbGUuY29tMAkGBYqGSM44BAMDMAAwLQIUVQykGR9CK4lxIj0Ng2q1Pwdrv0UCFQCfYVNSVAtcst3a53Yd4hBSW0NevTFjMGECAQEWGDASMRAdgYDVQQDEwdYXJsRFNTAgIAyDAHBgUrDgMCGjAJBgqhkiG00AQDBC4wLAUUM/mGf6gk9Z0XtRdGimJeB/BxUCFGFFJqwYRt1WYcIOQoGiaoqwGzVI

-----\_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 <a href="#">Section 6.4.5</a> of <a href="#">[RFC3501]</a> ). 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 <a href="#">[RFC5322]</a> 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-part = section ["/" smime-subpart]  
smime-subpart = smime-part  
section = <Defined in [Section 6.4.5 of \[RFC3501\]](#)>

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] <a href="#">Section 3.1</a>	active
pass	this document	smime	[this memo] <a href="#">Section 3.1</a>	active
fail	this document	smime	[this memo] <a href="#">Section 3.1</a>	active
policy	this document	smime	[this memo] <a href="#">Section 3.1</a>	active
neutral	this document	smime	[this memo] <a href="#">Section 3.1</a>	active
temperror	this document	smime	[this memo] <a href="#">Section 3.1</a>	active
permerror	this document	smime	[this memo] <a href="#">Section 3.1</a>	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.

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 EncryptedData [\[RFC5652\]](#) and AuthEnvelopedData [\[RFC5083\]](#). So agents processing Authentication-Results header fields shouldn'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 or invalid.

## **6. References**

### **6.1. Normative References**

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [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.
- [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