Network Working Group
Internet-Draft
Updates: 7208 (if approved)
Intended status: Standards Track
Expires: January 22, 2015

M. Kucherawy
July 21, 2014

Email Authentication Status Codes
draft-ietf-appsawg-email-auth-codes-05

Abstract

There is at present no way to return a status code to an email client that indicates a message is being rejected or deferred specifically because of email authentication failures. This document registers codes for this purpose.

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 January 22, 2015.

Copyright Notice

Table of Contents

1. Introduction

[RFC3463] introduced Enhanced Mail System Status Codes, and [RFC5248] created an IANA registry for these.

[RFC6376] and [RFC7208] introduced, respectively, DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF), two protocols for conducting message authentication. Another common email acceptance test is the reverse Domain Name System (DNS) check on an email client's IP address, as described in Section 3 of [RFC7001].

The current set of enhanced status codes does not include any code for indicating that a message is being rejected or deferred due to local policy reasons related to any of these mechanisms. This is potentially useful information to agents that need more than rudimentary handling information about the reason a message was rejected on receipt. This document introduces enhanced status codes for reporting those cases to clients.

Section 3.2 updates [RFC7208], as new enhanced status codes relevant to that specification are being registered and recommended for use.

2. Key Words

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 [RFC2119].

3. New Enhanced Status Codes

The following new enhanced status codes are defined:

3.1. DKIM Failure Codes

Code:	X.7.20
Sample Text:	No valid DKIM signature found
Associated basic status code:	550
Description:	This status code is returned when a message did not contain a valid DKIM signature, contrary to local policy requirements. (Note that this violates the advice of Section 6.1 of RFC6376.)
Reference:	[this document]; RFC6376
Submitter:	M. Kucherawy
Change controller:	IESG

Code: X.7.21
Sample Text: No valid author-matched DKIM signature found
Associated basic status code: 550
Description: This status code is returned when a message did not contain a valid DKIM signature whose identifier(s) match the author address(es) found in the From header field, contrary to local policy requirements. (Note that this violates the advice of Section 6.1 of RFC6376.)
Reference: [this document]; RFC6376
Submitter: M. Kucherawy
Change controller: IESG

3.2. SPF Failure Codes

Code: X.7.22
Sample Text: SPF validation failed
Associated basic status code: 550
Description: This status code is returned when a message completed an SPF check that produced a "fail" result, contrary to local policy requirements. Used in place of 5.7.1 as described in Section 8.4 of RFC7208.
Reference: [this document]; RFC7208
Submitter: M. Kucherawy
Change controller: IESG

Code: X.7.23
Sample Text: SPF validation error
Associated basic status code: 451/550
Description: This status code is returned when evaluation of SPF relative to an arriving message resulted in an error. Used in place of 4.4.3 or 5.5.2 as described in Sections 8.6 and 8.7 of RFC7208.
Reference: [this document]; RFC7208
Submitter: M. Kucherawy
Change controller: IESG

3.3. Reverse DNS Failure Code

Code:	X.7.24
Sample Text:	Reverse DNS validation failed
Associated basic status code:	550
Description:	This status code is returned when an SMTP client's IP address failed a reverse DNS validation check, contrary to local policy requirements.
Reference:	[this document]; Section 3 of RFC7001
Submitter:	M. Kucherawy
Change controller:	IESG

3.4. Multiple Authentication Failures Code

Code:	X.7.25
Sample Text:	Multiple authentication checks failed
Associated basic status code:	550
Description:	This status code is returned when a message failed more than one message authentication check, contrary to local policy requirements. The specific mechanisms that failed are not specified.
Reference:	[this document]
Submitter:	M. Kucherawy
Change controller:	IESG

4. General Considerations

By the nature of the Simple Mail Transfer Protocol (SMTP), only one enhanced status code can be returned for a given exchange between client and server. However, an operator might decide to defer or reject a message for a plurality of reasons. Clients receiving these codes need to consider that the failure reflected by one of these status codes might not reflect the only reason, or the most important reason, for non-acceptance of the message or command.

It is important to note that Section 6.1 of [RFC6376] discourages special treatment of messages bearing no valid DKIM signature. There are some operators that disregard this advice, a few of which go so far as to require a valid Author Domain signature (that is, one matching the domain(s) in the From header field) in order to accept the message. Moreover, some nascent technologies built atop SPF and DKIM depend on such authentications. This work does not endorse configurations that violate DKIM's recommendations, but rather acknowledges that they do exist and merely seeks to provide for improved interoperability with such operators.

A specific use case for these codes is mailing list software, which

processes rejections in order to remove from the subscriber set those addresses that are no longer valid. There is a need in that case to distinguish authentication failures versus indications that the recipient address is no longer valid.

If a receiving server performs multiple authentication checks, and more than one of them fails thus warranting rejection of the message, the SMTP server SHOULD use the code that indicates multiple methods failed rather than only reporting the first one that failed. It may be the case that one method is always expected to fail, and thus returning that method's specific code is not information useful to the sending agent.

The reverse IP DNS check is defined in Section 2.6.3 of [RFC7001].

Any message authentication or policy enforcement technologies developed in the future should also include registration of their own enhanced status codes so that this kind of specific reporting is available to operators that wish to use them.

5. Security Considerations

Use of these codes reveals local policy with respect to email authentication, which can be useful information to actors attempting to deliver undesired mail. It should be noted that there is no specific obligation to use these codes; if an operator wishes not to reveal this aspect of local policy, it can continue using a generic result code such as 5.7.7, 5.7.1, or even 5.7.0.

6. IANA Considerations

Registration of new enhanced status codes, for addition to the SMTP Enhanced Status Codes Registry, can be found in Section 3.

7. Normative References

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

[RFC3463] Vaudreuil, G., "Enhanced Mail System Status Codes", RFC 3463, January 2003.

[RFC5248] Hansen, T. and J. Klensin, "A Registry for SMTP Enhanced Mail System Status Codes", BCP 138, RFC 5248, June 2008.

[RFC6376] Crocker, D., Hansen, T., and M. Kucherawy, "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, September 2011.

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

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, April 2014.

Appendix A. Acknowledgments

Claudio Allocchio, Dave Crocker, Ned Freed, Arnt Gulbrandsen, Scott Kitterman, Barry Leiba, Alexey Melnikov, S. Moonesamy, Hector Santos, and Stephen Turnbull contributed to this work.

Author's Address

Murray S. Kucherawy
270 Upland Drive
San Francisco, CA 94127
USA

EMail: superuser@gmail.com