Network Working Group
Internet-Draft
Intended status: Informational
Expires: November 24, 2014

M. Kucherawy

May 23, 2014

# Email Authentication Status Codes
# draft-ietf-appsawg-email-auth-codes-00

## 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 November 24, 2014.

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 and Sender Policy Framework, two protocols for conducting email authentication. Another common email acceptance test is the reverse Domain Name System 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 either of these two mechanisms. This document introduces enhanced status codes for reporting those cases to clients.

## 2. New Status Codes

The following new status codes are defined:

### 2.1. DKIM Failures Code

```
Code:                X.7.19
Sample Text:         No valid DKIM signature found
Associated basic status code:  5
Description:         This status code is returned when a message
                     did not contain a valid DKIM signature,
                     contrary to local policy requirements.
Reference:           [this document]
Submitter:           M. Kucherawy
Change controller:   IESG
```

```
Code:                X.7.20
Sample Text:         No valid author DKIM signature found
Associated basic status code:  5
Description:         This status code is returned when a message
                     did not contain a valid DKIM signature
                     matching the domain(s) found in the From
                     header field, contrary to local policy
                     requirements.
Reference:           [this document]
Submitter:           M. Kucherawy
Change controller:   IESG
```

## 2.2. SPF Failures Code

```
Code:                X.7.21
Sample Text:         SPF validation failed
Associated basic status code:  5
Description:         This status code is returned when a message
                     failed an SPF check, contrary to local
                     policy requirements.
Reference:           [this document]
Submitter:           M. Kucherawy
Change controller:   IESG
```

## 2.3. Reverse DNS Failure Code

```
Code:                X.7.22
Sample Text:         reverse DNS validation failed
Associated basic status code:  5
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]
Submitter:           M. Kucherawy
Change controller:   IESG
```

## 3. 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.

## 4. Security Considerations

Use of these codes reveals local policy with respect to email authentication, which can be useful information to actors attempting to deliver undesirable 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 or even 5.7.0.

## 5. IANA Considerations

Registration of two new enhanced status codes, for addition to the SMTP Enhanced Status Codes Registry, can be found in Section 2.

## 6. Normative References

[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

Ned Freed, Arnt Gulbrandsen, and Barry Leiba contributed to this work.

Author's Address

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

EMail: superuser@gmail.com