A Property Types Registry for the Authentication-Results Header Field

Abstract

This document updates RFC 7001 by creating a registry for property
types in the Authentication-Results header field, used in email
authentication work, rather than limiting participants to using the
original, small set of fixed values.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force
(IETF). It represents the consensus of the IETF community. It has
received public review and has been approved for publication by the
Internet Engineering Steering Group (IESG). Further information on
Internet Standards is available in 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/rfc7410.

Copyright Notice

Table of Contents

1. Introduction

   [RFC7001] defines the email Authentication-Results header field that
   presents the results of an authentication effort in a machine-
   readable format. The header field creates a place to collect the
   output from authentication processes that are disjoint from later
   processes that might use the output, such as analysis, filtering, or
   sorting mechanisms.

   The specification in that document enumerated a small set of types of
   properties that can be reported using this mechanism. There has
   emerged a desire to report types of properties about a message
   through this mechanism. Accordingly, this document updates the
   specification to allow for additional property types ("ptypes")
   beyond the original set and creates a registry where new ones can be
   listed and their defining documents referenced.

2. Updated "ptype" Definition

   Advanced Backus Naur Form (ABNF) is defined in [RFC5234].

   The ABNF in Section 2.2 of [RFC7001] is updated as follows:

       ptype = Keyword
               ; indicates whether the property being evaluated was
               ; a parameter to an [SMTP] command, was a value taken
               ; from a message header field, was some property of
               ; the message body, or was some other property evaluated by
               ; the receiving Message Transfer Agent (MTA)

   The ABNF token "Keyword" is defined in Section 4.1.2 of [RFC5321].

Legal values of "ptype" are as defined in the IANA "Email
Authentication Property Types" registry (see Section 3). The initial
values are as follows, matching those defined in [RFC7001]:

body: Indicates information that was extracted from the body of the
   message. This might be an arbitrary string of bytes, a hash of a
   string of bytes, a Uniform Resource Identifier, or some other
   content of interest.

header: Indicates information that was extracted from the header of
   the message. This might be the value of a header field or some
   portion of a header field.

policy: A local policy mechanism was applied that augments or
   overrides the result returned by the authentication mechanism.
   See Section 2.3 of [RFC7001].

smtp: Indicates information that was extracted from an SMTP command
   that was used to relay the message.

When a consumer of this header field encounters a "ptype" that it
does not understand, it ignores the result reported with that
"ptype".

3. IANA Considerations

IANA has created the "Email Authentication Property Types" sub-
registry within the existing "Email Authentication Parameters"
registry. Entries in this registry are subject to the Expert Review
rules as described in [RFC5226]. Each entry in the registry requires
the following values:

o The "ptype" token to be registered, which must fit within the ABNF
   described in Section 2.

o A brief description of what sort of information this "ptype" is
   meant to cover.

o An optional reference to the defining document. This is
   recommended, but not required.

The initial entries in this table are as follows, taken from
[RFC7001]:

+--------+-------------+--+
| ptype | Definition | Description |
+--------+-------------+--+
| body | RFC 7001 | The property being reported was found |
| | Section 2.2 | in the body of the message. |
+--------+-------------+--+
| header | RFC 7001 | The property being reported was found |
| | Section 2.2 | in a header field of the message. |
+--------+-------------+--+
| policy | RFC 7001 | The property being reported relates to |
| | Section 2.3 | a locally defined policy. |
+--------+-------------+--+
smtp	RFC 7001	The property being reported is a
	Section 2.2	parameter to an SMTP command used to
		relay the message.
+--------+-------------+--+

For new entries, the Designated Expert needs to assure that the
description provided for the new entry adequately describes the
intended use. An example would be helpful to include in the entry's
defining document, if any, although entries in the "Email
Authentication Methods" registry or the "Email Authentication Result
Names" registry might also serve as examples of intended use.

4. Security Considerations

It is unknown how legacy code, which expects one of a fixed set of
"ptype" tokens, will handle new tokens as they begin to appear.
There are typically two options: prevent delivery of the message, or
ignore those portions of the field that use unknown "ptype" tokens
and allow processing of the message to continue.

The choice comes down to whether the consumer considers it a threat
when there are unknown "ptypes" present. The semantics of the report
are unknown; the report might be indicating the message is authentic,
fraudulent, or that a test failed to complete. The report itself is
not actionable because it cannot be understood, and only its presence
is certain.

Generally, the advice in this situation is to ignore unknown
"ptypes". It is anticipated that a new property type evaluated by
earlier handling agents would also result in the filtering of
messages by those agents until consumers can be updated to interpret
them.

5. Normative References

[RFC5226]   Narten, T. and H. Alvestrand, "Guidelines for Writing an
            IANA Considerations Section in RFCs", BCP 26, RFC 5226,
            May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[RFC5234]   Crocker, D. and P. Overell, "Augmented BNF for Syntax
            Specifications: ABNF", STD 68, RFC 5234, January 2008,
            <http://www.rfc-editor.org/info/rfc5234>.

[RFC5321]   Klensin, J., "Simple Mail Transfer Protocol", RFC 5321,
            October 2008, <http://www.rfc-editor.org/info/rfc5321>.

[RFC7001]   Kucherawy, M., "Message Header Field for Indicating
            Message Authentication Status", RFC 7001, September 2013,
            <http://www.rfc-editor.org/info/rfc7001>.

Acknowledgements

Author's Address

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

EMail: superuser@gmail.com