Authentication-Results Registration for OpenPGP Signature Verification
draft-ser-authentication-results-openpgp-00

Abstract

RFC 7601 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 PGP-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 https://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 September 12, 2019.

Copyright Notice

Copyright (c) 2019 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 (https://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.
# 1. Introduction

[RFC7601] specifies the Authentication-Results header field for conveying results of message authentication checks. OpenPGP signature verification is sometimes implemented in border message transfer agents (for instance some MTAs have their own OpenPGP PKI), there is a need to convey signature verification status to Mail User Agents (MUAs) and downstream filters. This document defines a new authentication method to be used in the Authentication-Results header field for OpenPGP-related signature checks.

# 2. "pgp" Authentication Method

OpenPGP signature verification is represented by the "pgp" method and is defined in [RFC4880].

## 2.1. OpenPGP Results

The result values used by OpenPGP [RFC4880] are as follows:
<table>
<thead>
<tr>
<th>Result Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>The message was not signed.</td>
</tr>
<tr>
<td>pass</td>
<td>The message was signed, the signature or signatures were acceptable to the verifier, and the signature(s) passed verification tests.</td>
</tr>
<tr>
<td>fail</td>
<td>The message was signed and the signature or signatures were acceptable to the verifier, but they failed the verification test(s).</td>
</tr>
<tr>
<td>policy</td>
<td>The message was signed and signature(s) passed verification tests, but the signature or signatures were not acceptable to the verifier.</td>
</tr>
<tr>
<td>neutral</td>
<td>The message was signed but the signature or signatures contained syntax errors or were not otherwise able to be processed. This result is also used for other failures not covered elsewhere in this list.</td>
</tr>
<tr>
<td>temperror</td>
<td>The message could not be verified due to some error that is likely transient in nature, such as a temporary inability to retrieve a key. A later attempt may produce a final result.</td>
</tr>
<tr>
<td>permerror</td>
<td>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 key not being available. A later attempt is unlikely to produce a final result.</td>
</tr>
</tbody>
</table>

OpenPGP Results

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 user ID in the signing OpenPGP key matches the domain in the address of the author of the message (value of the From header field), 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 that the message will be treated as if it had not been signed.
This document defines several new authentication parameters for conveying OpenPGP-related information, such as the identity associated with the entity that signed the message or one of its body parts.

2.2.1. body.pgp-fingerprint

body.pgp-fingerprint contains the fingerprint [RFC4880] of the key used to generate the OpenPGP signature referenced in the corresponding body.pgp-part.

2.2.2. body.pgp-user-id

body.pgp-user-id contains the signer’s user ID [RFC4880] associated with the OpenPGP signature referenced in the corresponding body.pgp-part.

2.3. Examples
Did you know that talking to yourself is a sign of senility?

It’s generally a good idea to encode lines that begin with From=20because some mail transport agents will insert a greater-than (>)
sign, thus invalidating the signature.

Also, in some cases it might be desirable to encode any trailing whitespace that occurs on lines in order to ensure that the message signature is not invalidated when passing a gateway that modifies such whitespace (like BITNET).

me

Did you know that talking to yourself is a sign of senility?

It’s generally a good idea to encode lines that begin with From=20because some mail transport agents will insert a greater-than (>)
sign, thus invalidating the signature.

Also, in some cases it might be desirable to encode any trailing whitespace that occurs on lines in order to ensure that the message signature is not invalidated when passing a gateway that modifies such whitespace (like BITNET).

me
3. IANA Considerations

IANA has added the following entries to the "Email Authentication Methods" sub-registry of the "Email Authentication Parameters" registry:

TBD

IANA has added the following entries to the "Email Authentication Result Names" sub-registry of the "Email Authentication Parameters" registry:

TBD

4. Security Considerations

TODO

5. Normative References


Author’s Address

Simon Ser
14, rue Girardot
Villebon-sur-Yvette 91140
France

Email: contact@emersion.fr