Internet Engineering Task Force (IETF)
Request for Comments: 9991
Obsoletes: 7489
Updates: 6591
Category: Standards Track
ISSN: 2070-1721

S. Jones, Ed.
DMARC.org
A. Vesely, Ed.
Tana

May 2026

Domain-Based Message Authentication, Reporting, and Conformance (DMARC) Failure Reporting

Abstract

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a mechanism by which a Domain Owner can request feedback about email messages using their domain in the From: address field. This document describes "failure reports", or "failed message reports", which provide details about individual messages that failed to authenticate according to the DMARC mechanism.

This document updates RFC 6591 and obsoletes RFC 7489.

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 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9991.

Table of Contents

1. Introduction

Domain-based Message Authentication, Reporting, and Conformance (DMARC) [RFC9989] is a mechanism by which a mail-originating organization can express domain-level policies and preferences for message validation, disposition, and reporting that can be used by a mail-receiving organization to improve mail handling. This document focuses on one type of reporting that can be requested under DMARC.

Failure reports provide detailed information about the failure of a single message or a group of similar messages failing for the same reason. Their purpose is twofold. On the one hand, they are meant to aid in cases where a Domain Owner wishes to determine the cause of failures that were part of aggregate reports (see [RFC9990]). On the other hand, they can allow the Domain Owner to quickly identify and address harmful messages involving direct domain abuse. It is important to note that these reports can contain the header fields or sometimes the entire content of a failed message, which may contain Personally Identifiable Information (PII). The potential disclosure of PII should be considered when deciding whether to request failure reports as a Domain Owner, or what information to include or redact in failure reports when creating them as a Mail Receiver, or whether to create failure reports at all. Refer to Section 7 for more discussion on privacy considerations.

1.1. Terminology

There are a number of terms defined in Section 3.2 of [RFC9989] that are used within this document. Understanding those definitions will aid in reading this document.

The format of DMARC failure reports is derived from "Authentication Failure Reporting Using the Abuse Reporting Format" [RFC6591], and the terms defined there are used here.

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Document Status

This document, in part, along with [RFC9989] and [RFC9990], obsoletes and replaces [RFC7489].

2. DMARC Failure Reports

Besides the header fields or the entire contents of a failed message, failure reports supply details about transmission and DMARC authentication, which may aid a Domain Owner in determining the cause of an authentication failure.

Failure reports are normally generated and sent almost immediately after the Mail Receiver detects a DMARC failure. Rather than waiting for an aggregate report, these reports are useful for quickly notifying the Domain Owners when there is an authentication failure. Failure reports also provide more information about the failed message than is available in an aggregate report. This allows the failure report consumer to better determine whether the failure is of a message that the Domain Owner intended to authenticate or one for which use of its domain was not authorized.

These reports should include as much of the message header fields and body as possible, consistent with the reporting party's privacy policies, to enable the Domain Owner to diagnose the authentication failure.

When a Domain Owner requests failure reports for the purpose of forensic analysis, and the Mail Receiver is willing to provide such reports, the Mail Receiver generates and sends a message using the format described in [RFC6591]; this document updates that reporting format, as described in Section 4.

The destination(s) to which failure reports are sent, and options for when they will be sent, are defined by the "ruf" and "fo" tags as provided in Section 4.7 of [RFC9989].

When multiple Uniform Resource Identifiers (URIs) are provided to receive failure reports, the report generator MUST make an attempt to deliver to each of them. External destinations MUST be verified (see Section 5). Report generators MUST NOT consider "ruf" tags in DMARC Policy Records that have a "psd=y" tag, unless there are specific agreements between the interested parties.

Report generators MUST implement a rate-limit on outgoing reports so as not to flood Report Consumers with excessive reports, which would allow denial of service (see Section 8.1).

3. Other Failure Reports

This document only describes DMARC failure reports. DomainKeys Identified Mail (DKIM) failure reports and Sender Policy Framework (SPF) failure reports are described in [RFC6591]. A Mail Receiver that generates DMARC failure reports MAY choose to issue failure reports of the type specific to the authentication mechanism that failed instead of, or in addition to, the DMARC failure report type described here. The Receiver SHALL determine which failure report types, if any, to transmit based on its own policy, the failure in question, and the content of the "fo" tag in the retrieved DMARC Policy Record.

Note that DKIM failure reports and SPF failure reports can also be requested using the methods described in [RFC6651] and [RFC6652], respectively. Report generators are free to follow any of the specifications.

4. Reporting Format Update

Operators implementing this specification also implement an augmented version of failure reporting described in [RFC6591] as follows:

1. A DMARC failure report includes the following Abuse Reporting Format (ARF) header fields, with the indicated normative requirement levels:

    * Identity-Alignment (REQUIRED; defined below)

    * Delivery-Result (OPTIONAL)

* DKIM-Domain, DKIM-Identity, DKIM-Selector (REQUIRED for DKIM failures of an aligned identifier)

* DKIM-Canonicalized-Header, DKIM-Canonicalized-Body (OPTIONAL if reporting a DKIM failure)

* SPF-DNS (REQUIRED for SPF failure of an aligned identifier)

2. The Identity-Alignment field is defined to contain a comma-separated list of authentication mechanism names that failed to authenticate an aligned identity or the keyword "none" if all of the attempted methods were successful at authenticating an aligned identity. Here is the ABNF [RFC5234] (importing comments and/or folding white space (CFWS) from [RFC5322]):

```
id-align     = "Identity-Alignment:" [CFWS]
                 ( "none" /
                   dmarc-method
                     *( [CFWS] "," [CFWS] dmarc-method ) )
                 [CFWS]

dmarc-method = ( "dkim" / "spf" )
                 ; each may appear at most once in an id-align
```

3. Authentication Failure Type "dmarc" is defined for the Auth-Failure field, which is to be used when a failure report is generated because some or all of the authentication mechanisms failed to produce aligned identifiers. Note that a failure report generator MAY also independently produce an ARF message for any or all of the underlying authentication methods.

5. Verifying External Destinations

It is possible to specify destinations for failure reports that are outside of the Organizational Domain of the DMARC Policy Record that was requesting the reports. These destinations are commonly referred to as "external destinations" and may represent a different domain controlled by the same organization, a contracted report processing service, or some other arrangement.

In case of external destinations, a Mail Receiver who generates failure reports MUST use the Verifying External Destinations procedure described in Section 4 of [RFC9990], substituting the "ruf" tag where the "rua" tag appears in that procedure.

This prevents a bad actor from publishing a DMARC Policy Record requesting failure reports to an external destination and then deliberately sending messages that will generate failure reports as a form of abuse. It also prevents a Domain Owner from unilaterally publishing a DMARC Policy Record with an external destination for failure reports, forcing the external destination to deal with unwanted messages and potential privacy issues.

5.1. Transport

Email streams carrying DMARC failure reports SHOULD be DMARC-aligned.

We recommend that reporters set a reasonable rate-limit for the number of failure reports sent to any recipient to avoid overloading recipient systems. Unaligned reports may in turn produce subsequent failure reports that could cause mail loops.

6. IANA Considerations

6.1. Feedback Report Header Fields Registry Update

IANA has updated the reference and description for the "Identity-Alignment" entry in the "Feedback Report Header Fields" registry within the "Messaging Abuse Reporting Format (MARF) Parameters" registry group, as follows:

Field Name: Identity-Alignment
Description: a list of authentication mechanism names that failed to authenticate an aligned identity, or "none" if all were successful
Multiple Appearances: No
Related "Feedback-Type": auth-failure
Reference: RFC 9991
Status: current

7. Privacy Considerations

The generation and transmission of DMARC failure reports raise significant privacy concerns that must be carefully considered before deployment.

Given these factors, many large-scale providers limit or entirely disable the generation of failure reports, preferring to rely on aggregate reports, which provide statistical visibility without exposing sensitive content. Operators that choose to enable failure reporting are strongly encouraged to:

* Limit the scope and duration of use to targeted diagnostic activities;

* Ensure that reporting URIs are carefully controlled and validated;

* Apply minimization techniques, such as redaction of message bodies and header fields, to reduce sensitive data exposure;

* Always transmit reports over secure channels.

In summary, while DMARC failure reports can offer diagnostic value, the associated privacy concerns have led many operators to restrict their use. Aggregate reports remain the recommended mechanism for gaining visibility into authentication results while preserving the confidentiality of end-user communications.

Particular privacy-specific issues are explored below.

7.1. Data Exposure Considerations

Failure reports may include PII and non-public information (NPI) from messages that fail to authenticate, since these reports may contain message content as well as trace header fields. These reports may expose sender and recipient identifiers (e.g., RFC5322.From addresses), and although the [RFC5965] format used for failed-message reporting supports redaction [RFC6590], failed-message reporting is capable of exposing the entire message to the Report Consumer. They may also expose PII, sensitive business data, or other confidential communications to unintended recipients. Such exposure can create regulatory, legal, and operational risks for both senders and receivers. Examples include product launches, termination notices for employees, or calendar data. Even innocuous-seeming failures (such as malformed or "broken" calendar invitations) can result in the leakage of private communications.

Domain Owners requesting reports will receive information about mail using their domain, but which they did not actually cause to be sent. This might provide valuable insight into content used in abusive messages, but it might also expose PII or NPI from legitimate messages mistakenly or accidentally failing authentication.

Information about the final destination of mail, where it might otherwise be obscured by intermediate systems, may be exposed through a failure report. A commonly cited example is exposure of members of mailing lists when one list member sends messages to the list, and failure reports are generated when that message is delivered to other list members. Those failure reports would be sent to the Domain Owner of the list member posting the message or their delegated Report Consumer(s).

Similarly, when message forwarding arrangements exist, Domain Owners requesting reports may receive information about mail forwarded to domains that were not originally part of their messages' recipient list. This means that destinations previously unknown to the Domain Owner may now become visible.

7.2. Report Recipients

A DMARC Policy Record can specify that reports should be sent to a Report Consumer operating on behalf of the Domain Owner. This might be done when the Domain Owner sends reports to an entity to monitor mail streams for deliverability, performance issues, or abuse. Receipt of such data by third parties may or may not be permitted by the Mail Receiver's privacy policy, terms of use, etc. Domain Owners and Mail Receivers should both review and understand whether their own internal policies constrain the use and transmission of DMARC reporting.

Some potential exists for Report Consumers to perform traffic analysis, making it possible to obtain metadata about the Mail Receiver's traffic. In addition to verifying compliance with policies, Mail Receivers need to consider that before sending reports to a third party. On the other hand, a Domain Owner may publish a destination address that appears to be an Internal Report Consumer but is actually a forwarding address; in this case, the final destination of a report is not guaranteed.

7.3. Additional Damage

The risks associated with failure reports are compounded by volume and content distribution concerns. Partially or unredacted reports may propagate large amounts of spam, phishing, or malware content, all of which may require special handling by Report Consumers or other recipients to avoid incidents. This underscores the need to avoid misconfiguration of the destinations in the "ruf" reporting URIs and the suggestions for redaction in this document, for example, using the method described in [RFC6590]. All of these concerns are heightened for high-volume domains. To mitigate such concerns, the following steps should be considered:

By report generators:

* Help prevent accidental access to potentially malicious URIs by substituting hxxp for http;

* Remove attachments that could embed malicious payload.

By report consumers:

* Isolate report streams from other mail streams;

* Use sandboxes in evaluating failure reports;

* Use network segmentation;

* Limit access to failure reports to authorized individuals with

appropriate security training.

8. Security Considerations

While reviewing this document and its security considerations, the reader should also review the privacy considerations above, as well as the privacy considerations and security considerations in Sections 10 and 11 of [RFC9989] and in Sections 7 and 8 of [RFC9990].

8.1. Denial of Service

Failure reports represent a possible denial-of-service attack that could be perpetrated by an attacker who sends numerous messages purporting to be from the intended victim Domain Owner but which fail both SPF and DKIM; this would cause participating Mail Receivers to send failure reports to the Domain Owner or its delegate(s), potentially in large numbers. Accordingly, participating Mail Receivers are encouraged to aggregate these reports as much as is practical, using the Incidents field of the ARF [RFC5965]. Indeed, the aim is not to count each and every failure but rather to report different failure conditions. Various pruning techniques are possible, including the following:

* Store reports for a period of time before sending them, allowing detection, collection, and consolidation of like incidents;

* Apply rate-limiting, such as a maximum number of reports per minute that will be generated (and the remainder discarded).

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/info/rfc5322>.

[RFC5965] Shafranovich, Y., Levine, J., and M. Kucherawy, "An Extensible Format for Email Feedback Reports", RFC 5965, DOI 10.17487/RFC5965, August 2010, <https://www.rfc-editor.org/info/rfc5965>.

[RFC6590] Falk, J., Ed. and M. Kucherawy, Ed., "Redaction of Potentially Sensitive Data from Mail Abuse Reports", RFC 6590, DOI 10.17487/RFC6590, April 2012, <https://www.rfc-editor.org/info/rfc6590>.

[RFC6591] Fontana, H., "Authentication Failure Reporting Using the Abuse Reporting Format", RFC 6591, DOI 10.17487/RFC6591, April 2012, <https://www.rfc-editor.org/info/rfc6591>.

[RFC6692] Clayton, R. and M. Kucherawy, "Source Ports in Abuse Reporting Format (ARF) Reports", RFC 6692, DOI 10.17487/RFC6692, July 2012, <https://www.rfc-editor.org/info/rfc6692>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9989] Herr, T., Ed. and J. Levine, Ed., "Domain-Based Message Authentication, Reporting, and Conformance (DMARC)", RFC 9989, DOI 10.17487/RFC9989, May 2026, <https://www.rfc-editor.org/info/rfc9989>.

[RFC9990] Brotman, A., Ed., "Domain-Based Message Authentication, Reporting, and Conformance (DMARC) Aggregate Reporting", RFC 9990, DOI 10.17487/RFC9990, May 2026, <https://www.rfc-editor.org/info/rfc9990>.

9.2. Informative References

[RFC6651] Kucherawy, M., "Extensions to DomainKeys Identified Mail (DKIM) for Failure Reporting", RFC 6651, DOI 10.17487/RFC6651, June 2012, <https://www.rfc-editor.org/info/rfc6651>.

[RFC6652] Kitterman, S., "Sender Policy Framework (SPF) Authentication Failure Reporting Using the Abuse Reporting Format", RFC 6652, DOI 10.17487/RFC6652, June 2012, <https://www.rfc-editor.org/info/rfc6652>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/info/rfc7489>.

Appendix A. Example Failure Report

This is the full content of a sample failure message, including the message header.

```
Received: from gen.example (gen.example [192.0.2.1])
  (TLS: TLS1.3,256bits,ECDHE_RSA_AES_256_GCM_SHA384)
  by mail.consumer.example with ESMTPS
  id 00000000005DC0DD.0000442E; Tue, 19 Jul 2022 07:57:50 +0200
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
  d=gen.example; s=mail; t=1658210268;
  bh=rCrh1aFDE8d/Fltt8wbcu48bLOu4OM23QXqphUZPAIM=;
  h=From:To:Date:Subject:From;
  b=IND9JkuwF9/5841kzxMbPeej0VYimVzNKozR2R89M8eYO2zOlCBblx507Gz0YK7mE
   /h6pslWm0ODBVFzLlwY9CXv4Vu62QsN0RBIXHPjEXOkoM2VCD5zCd+5i5dtCFX7Mxh
   LThb2ZJ3efklbSB9RQRwxcmRvCPV7z6lt/Ds9sucVE1RDODYHjx+iWnAUQrlos6ZQb
   u/YOUGjf60LPpyljfPu3EpFwo80mSHyQlP/4S5KEykgPQMgCqLPPKvJwu1aAIDj+jG
   q2ylO3fmc/ERDeDWACtR67YNabEKBWtjqCRLNxKttazViJTZ5drcLfpX0853KoougX
   Rltp7zdoLdy4A==
From: DMARC Filter <DMARC@gen.example>;
To: dmarcfail@consumer.example
Date: Tue, 19 Jul 2022 00:57:48 -0500 (CDT)
Subject: FW: This is the original subject
Mime-Version: 1.0
Content-Type: multipart/report; report-type=feedback-report;
  boundary="=_mime_boundary_"
Message-Id: <20220719055748.4AE9D403CC@gen.example>;

This is a MIME-formatted message.  If you see this text it means that
your E-mail software does not support MIME-formatted messages.

--=_mime_boundary_
Content-Type: text/plain; charset=utf-8
Content-Disposition: inline
Content-Transfer-Encoding: 7bit
```

```
This is an authentication failure report for an email message
received from IP 192.0.2.2 on Tue, 19 Jul 2022 00:57:48 -0500.

--=_mime_boundary_
Content-Type: message/feedback-report
Content-Transfer-Encoding: 7bit

Feedback-Type: auth-failure
Version: 1
User-Agent: DMARC-Filter/1.2.3
Auth-Failure: dmarc
Authentication-Results: gen.example;
  dmarc=fail header.from=consumer.example
Identity-Alignment: dkim
DKIM-Domain: consumer.example
DKIM-Identity: @consumer.example
DKIM-Selector: epsilon
Original-Envelope-Id: 65E1A3F0A0
Original-Mail-From: author=gen.example@forwarder.example
Source-IP: 192.0.2.2
Source-Port: 12345
Reported-Domain: consumer.example

--=_mime_boundary_
Content-Type: message/rfc822; charset=utf-8
Content-Transfer-Encoding: 7bit

Authentication-Results: gen.example;
  dkim=permerror header.d=forwarder.example header.b="EjCbN/c3";
  dkim=temperror header.d=forwarder.example header.b="mQ8GEWPc";
  dkim=permerror header.d=consumer.example header.b="hETrymCb";
  dkim=neutral header.d=consumer.example header.b="C2nsAp3A";
Received: from mail.forwarder.example
  (mail.forwarder.example [IPv6:2001:db8::23ac])
  by mail.gen.example (Postfix) with ESMTP id 5E8B0C159826
  for <x@gen.example>; Sun, 14 Aug 2022 07:58:29 -0700 (PDT)
Received: from mail.forwarder.example (localhost [127.0.0.1])
  by mail.forwarder.example (Postfix) with ESMTP id 4Ln7Qw4fnvz6Bq
  for <x@gen.example>; Tue, 19 Jul 2022 07:57:44 +0200
DKIM-Signature: v=1; a=ed25519-sha256; c=relaxed/relaxed;
  d=forwarder.example; s=ed25519-59hs; t=1658210264;
  x=1663210264; bh=KYH/g7ForvDbnyyDLYSjauMYMW6sEIqu75/9w3OIONg=;
  h=Message-ID:Date:List-Id:List-Archive:List-Post:List-Help:
   List-Subscribe:List-Unsubscribe:List-Owner:MIME-Version:Subject:
   To:References:From:In-Reply-To:Content-Type:
   Content-Transfer-Encoding:autocrypt:cc:content-transfer-encoding:
   content-type:date:from:in-reply-to:message-id:mime-version:
   openpgp:references:subject:to;
  b=EjCbN/c3bTU4QkZH/zwTbYxBDp0k8kpmWSXh5h1M7T8J4vtRo+hvafJazT3ZRgq+7
   +4dzEQwUhl+NOJYXXNUAA==
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=forwarder.example; s=rsa-wgJg; t=1658210264; x=1663210264;
  bh=KYH/g7ForvDbnyyDLYSjauMYMW6sEIqu75/9w3OIONg=;
  h=Message-ID:Date:List-Id:List-Archive:List-Post:List-Help:
   List-Subscribe:List-Unsubscribe:List-Owner:MIME-Version:Subject:
   To:References:From:In-Reply-To:Content-Type:
   Content-Transfer-Encoding:autocrypt:cc:content-transfer-encoding:
   content-type:date:from:in-reply-to:message-id:mime-version:
   openpgp:references:subject:to;
  b=mQ8GEWPcVpBpeqQ88pcbXpGHBT0J/Rwi8Zd2WZTXWWneQGRCOJLRcbBJpjqnrwtqd
   76IqawH86tihz4Z/12J1GBCdNx1gfazsoI3yaqfooRDYg0mSyZHrYhQBmodnPcqZj4
   /25L5278sc/UNrYO9az2n7R/skbVZ0bvSo2eEiGU8fcpO8+a5SKNYskhaviAI4eGIB
   iRMdEP7gP8dESdnZguNbY5HI32UMDpPPNqajzd/BgcqbveYpRrWCDOhcY47POV7GHM
   i/KLHiZXtJsL3/Pr/4TL+HTjdX8EDSsy1K5/JCvJCFsJHnSvkEaJQGLn/2m03eW9r8
   9w1bQ90aY+VCQ==
```

```
X-Original-To: users@forwarder.example
Received: from mail.consumer.example
  (mail.consumer.example [192.0.2.4])
  (using TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits)
   key-exchange ECDHE (P-256) server-signature ECDSA (P-384)
   server-digest SHA384)
  (Client did not present a certificate)
  by mail.forwarder.example (Postfix) with ESMTPS id 4Ln7Qs55xmz4nP
  for <users@forwarder.example>;
  Tue, 19 Jul 2022 07:57:41 +0200 (CEST)
Authentication-Results: mail.forwarder.example;
  arc=none smtp.remote-ip=192.0.2.4
Authentication-Results: mail.forwarder.example;
  dkim=pass (512-bit key; secure) header.d=consumer.example
   header.i=@consumer.example header.a=ed25519-sha256
   header.s=epsilon header.b=hETrymCb;
  dkim=pass (1152-bit key; secure) header.d=consumer.example
   header.i=@consumer.example header.a=rsa-sha256
   header.s=delta header.b=C2nsAp3A
DKIM-Signature: v=1; a=ed25519-sha256; c=relaxed/relaxed;
  d=consumer.example; s=epsilon; t=1658210255;
  bh=KYH/g7ForvDbnyyDLYSjauMYMW6sEIqu75/9w3OIONg=;
  h=Date:Subject:To:References:From:In-Reply-To;
  b=hETrymCbz6T1Dyo5dCG9dk8rPykKLdhJCPFeJ9TiiP/kaoN2afpUYtj+SrI+I83lp
   p1F/FfYSGy7zz3Q3OdxBA==
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=consumer.example; s=delta; t=1658210255;
  bh=KYH/g7ForvDbnyyDLYSjauMYMW6sEIqu75/9w3OIONg=;
  h=Date:To:References:From:In-Reply-To;
  b=C2nsAp3AMNX33Nq7nN/StPo921xE3XGF8Ju3iAKdYB3EKhsril0N5IjWGlglJECst
   jLNKSo7KWZZ2lkH/dVZ9Rs1GHT2uaKy1sc/xmNIC5rHdhrxammiwpTSo4PsT8disfc
   3DVF6Q62n0EsdLFqcw1KY8A9inFqYKY2tqoo+y4zMtItqCYx3xjsj3I0IFLuX
Author: Message Author <author@consumer.example>
Received: from [192.0.2.8] (host-8-2-0-192.isp.example [192.0.2.8])
  (AUTH: CRAM-MD5 uXDGrn@SYT0/k, TLS: TLS1.3,128bits,
  ECDHE_RSA_AES_128_GCM_SHA256)
  by mail.consumer.example with ESMTPSA
  id 00000000005DC076.00004417; Tue, 19 Jul 2022 07:57:35 +0200
Message-ID: <2431dc66-b010-c9cc-4f2b-a1f889f8bdb4@consumer.example>
Date: Tue, 19 Jul 2022 07:57:33 +0200
List-Id: <users.forwarder.example>
List-Post: <mailto:users@forwarder.example>
List-Help: <mailto:users+help@forwarder.example>
List-Subscribe: <mailto:users+subscribe@forwarder.example>
List-Unsubscribe: <mailto:users+unsubscribe@forwarder.example>
List-Owner: <mailto:users+owner@forwarder.example>
Precedence: list
MIME-Version: 1.0
Subject: This is the original subject
Content-Language: en-US
To: users@forwarder.example
Authentication-Results: consumer.example; auth=pass (details omitted)
From: Message Author <author@consumer.example>
In-Reply-To: <20220718102753.0f6d9dde.cel@example.com>
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 8bit

[ Message body was here ]
--=_mime_boundary_--
```

The Source-Port field definition is given by [RFC6692].

In the final MIME entity, the local-parts of To and From addresses are reported unredacted. Since we know that the local parts are PII, we can reduce the privacy risk by redacting them. In the example, the report generator could have replaced "users" with "lRLxexey" and

"author" with "RT47aVey" throughout the entity.

If the body of the message is not included, the last MIME entity would have "Content-Type: text/rfc822-headers" instead of "message/rfc822".

Authors' Addresses

Steven M. Jones (editor)
DMARC.org
Email: smj@dmarc.org

Alessandro Vesely (editor)
Tana
Email: vesely@tana.it