

DMARC  
Internet-Draft  
Obsoletes: 7489 (if approved)  
Updates: 6591 (if approved)  
Intended status: Standards Track  
Expires: 13 October 2025

S. Jones (ed)  
DMARC.org  
A. Vesely (ed)  
Tana  
11 April 2025

Domain-based Message Authentication, Reporting, and Conformance (DMARC)  
Failure Reporting  
draft-ietf-dmarc-failure-reporting-13

## Abstract

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a scalable 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.

## 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 13 October 2025.

## Copyright Notice

Copyright (c) 2025 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. Code Components

extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	2
1.1. Terminology . . . . .	3
2. DMARC Failure Reports . . . . .	3
3. Other Failure Reports . . . . .	4
4. Reporting Format Update . . . . .	4
5. Verifying External Destinations . . . . .	5
5.1. Transport . . . . .	6
6. IANA Considerations . . . . .	6
6.1. Feedback Report Header Fields Registry Update . . . . .	6
7. Privacy Considerations . . . . .	6
7.1. Data Exposure Considerations . . . . .	6
7.2. Report Recipients . . . . .	7
8. Security Considerations . . . . .	7
9. Normative References . . . . .	7
10. Informative References . . . . .	8
Appendix A. Example Failure Report . . . . .	9
Appendix B. Change Log {change-log} . . . . .	12
B.1. 00 to 01 . . . . .	12
B.2. 01 to 02 . . . . .	13
B.3. 02 to 03 . . . . .	13
B.4. 03 to 04 . . . . .	13
B.5. 04 to 05 . . . . .	13
B.6. 05 to 06 . . . . .	14
B.7. 06 to 07 . . . . .	14
B.8. 07 to 08 . . . . .	14
B.9. 08 to 09 . . . . .	14
B.10. 09 to 10 . . . . .	14
B.11. 10 to 11 . . . . .	14
B.12. 11 to 12 . . . . .	14
B.13. 12 to 13 . . . . .	14
Authors' Addresses . . . . .	15

## 1. Introduction

RFC EDITOR: PLEASE REMOVE THE FOLLOWING PARAGRAPH BEFORE PUBLISHING:  
 The source for this draft is maintained in GitHub at:  
<https://github.com/ietf-wg-dmarc/draft-ietf-dmarc-failure-reporting>  
<https://github.com/ietf-wg-dmarc/draft-ietf-dmarc-failure-reporting>

Domain-based Message Authentication, Reporting, and Conformance (DMARC) [I-D.ietf-dmarc-dmarcbis] is a scalable mechanism by which a mail-originating organization can express domain-level policies and

preferences for message validation, disposition, and reporting, that a mail-receiving organization can use 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. They are meant to aid in cases where a Domain Owner is unable to detect why failures that were reported in aggregate form occurred. 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.

### 1.1. Terminology

There are a number of terms defined in [!I-D.ietf-dmarc-dmarcbis, section 3.2] that are used within this document. Understanding those definitions will aid in reading this document.

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.

## 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 the 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. Whether the failure is due to an infrastructure problem or the message is inauthentic, failure reports also provide more information about the failed message than is available in an aggregate report.

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) that failure reports are sent to, and options for when they will be sent, are defined by the "ruf" and "fo" tags as defined in Section 4.7 of [I-D.ietf-dmarc-dmarcbis].

When multiple 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 having a "psd=y" tag, unless there are specific agreements between the interested parties.

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 Abuse Reporting Format [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)

### 3. Other Failure Reports

This document only describes DMARC failure reports. DKIM failure reports [RFC6651] and SPF failure reports [RFC6652] are described in separate documents. A Mail Receiver generating a DMARC failure report may or may not also issue a failure report specific to the failed authentication mechanism, according to its policy.

### 4. Reporting Format Update

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

1. A DMARC failure report includes the following 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 none did. ABNF ([RFC5234]):

```
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, 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.

Without this check, a bad actor could publish a DMARC Policy Record that requests that failure reports be sent to an external destination, then deliberately send messages that will generate failure reports as a form of abuse. Or, a Domain Owner could

incorrectly publish a DMARC Policy Record with an external destination for failure reports, forcing the external destination to deal with unwanted messages and potential privacy issues.

Therefore, in case of external destinations, a Mail Receiver who generates failure reports MUST use the Verifying External Destinations procedure described in Section 4 of [I-D.ietf-dmarc-aggregate-reporting], substituting the "ruf" tag where the "rua" tag appears in that procedure.'

#### 5.1. Transport

Email streams carrying DMARC failure reports SHOULD be DMARC aligned.

Reporters MAY rate limit 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 is requested to change the "Identity-Alignment" entry in the "Feedback Report Header Fields" registry to refer to this document.

### 7. Privacy Considerations

This section discusses issues specific to private data that may be included in the DMARC reporting functions.

#### 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 [RFC6591] format used for failed-message reporting supports redaction, failed-message reporting is capable of exposing the entire message to the Report Consumer.

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 messages mistakenly or accidentally using the wrong sending domain.

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 contracts with 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, et cetera. 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.

## 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 [I-D.ietf-dmarc-dmarcbis]; and in sections 7 and 8 of [I-D.ietf-dmarc-aggregate-reporting].

In addition, note that Organizational Domains are only an approximation to actual domain ownership. Therefore, reports may be sent to someone unrelated to the actual sender or Domain Owner. That makes considerations in Section 7.1 all the more relevant.

## 9. Normative References

[I-D.ietf-dmarc-aggregate-reporting]

Brotman, A., "Domain-based Message Authentication, Reporting, and Conformance (DMARC) Aggregate Reporting", Work in Progress, Internet-Draft, draft-ietf-dmarc-aggregate-reporting-32, 17 March 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-dmarc-aggregate-reporting-32>>.

[I-D.ietf-dmarc-dmarcbis]

Herr, T. and J. R. Levine, "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", Work in Progress, Internet-Draft, draft-ietf-dmarc-dmarcbis-41, 4 April 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-dmarc-dmarcbis-41>>.

[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>>.

[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>>.

[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>>.

## 10. 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>>.

#### Appendix A. Example Failure Report

This is the full content of a 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 0000000005DC0DD.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=rCrhlaFDE8d/Fltt8wbcu48bLOu4OM23QXqphUZPAIM=;
  h=From:To:Date:Subject:From;
  b=IND9JkuwF9/5841kzxMbPeej0VYimVzNkozR2R89M8eYO2zOlCBblx507Gz0YK7mE
  /h6pslWm0ODBFVzLlwY9CXv4Vu62QsN0RBIXHPjEXOkom2VCD5zCd+5i5dtCFX7Mxh
  LThb2ZJ3efklbSB9RQRwxcmRvCPV7z6lt/Ds9sucVE1RDODYHjx+iWnAUQrlos6ZQb
  u/YOUGjf60LPpyljfPu3EpFwo80mSHyQlP/4S5KEykgPQMgCqLPPKvJwulaAIDj+jG
  q2yl03fmc/ERDeDWACtR67YNabEKBWtjqCRLNxKttazViJTZ5drcLfpX0853KooougX
  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/zwTbYxBdp0k8kpmWSXh5hlM7T8J4vtRo+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/Rwi8Zd2WZTXWWneQGRCOJLRcbBJpjqrwtqd
76IqawH86tihz4Z/12JlGBCdNxlgfazsoI3yaqfooRDYg0mSyZhrYhQBmodnPcqZj4
/25L5278sc/UNrY09az2n7R/skbVZ0bvSo2eEiGU8fcp08+a5SKNYskhaviAI4eGIB
iRMdEP7gP8dESdnZguNbY5HI32UMDPppNqajzd/BgcqbveYpRrWCD0hcY47POV7GHM
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=hETrymCbz6TlDyo5dCG9dk8rPykKLdhJCPFeJ9TiiP/kaon2afpUYtj+SrI+I83lp
p1F/FfYSGy7zz3Q30dxBA==
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-alf889f8bdb4@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]

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

## Appendix B. Change Log {change-log}

[RFC Editor: Please remove this section prior to publication.]

### B.1. 00 to 01

- \* Replace references to RFC7489 with references to I-D.ietf-dmarc-dmarcbis.
- \* Replace the 2nd paragraph in the Introduction with the text proposed by Ned for Ticket #55, which enjoys some consensus:  
[https://mailarchive.ietf.org/arch/msg/dmarc/  
HptVyJ9SgrfxWRbeGwORagPrhCw](https://mailarchive.ietf.org/arch/msg/dmarc/HptVyJ9SgrfxWRbeGwORagPrhCw)  
([https://mailarchive.ietf.org/arch/msg/dmarc/  
HptVyJ9SgrfxWRbeGwORagPrhCw](https://mailarchive.ietf.org/arch/msg/dmarc/HptVyJ9SgrfxWRbeGwORagPrhCw))

- \* Strike a spurious sentence about criticality of feedback, which was meant for feedback in general, not failure reports. In fact, failure reports are not critical to establishing and maintaining accurate authentication deployments. Still attributable to Ticket #55.
- \* Remove the content of section "Verifying External Destinations" and refer to I-D.ietf-dmarc-aggregate-reporting.
- \* Remove the content of section "Security Considerations" and refer to I-D.ietf-dmarc-dmarcbis.
- \* Slightly tweak the wording of the example in Appendix A.1 so that it makes sense standing alone.
- \* Remove the sentence containing "must include any URI(s)", as the issue arose <eref target="https://mailarchive.ietf.org/arch/msg/dmarc/mFk0qiTCy8tzghRvcxus0lW\_Blw"/>.
- \* Add paragraph in Security Considerations, noting that note that Organizational Domains are only an approximation...
- \* Add a Transport section, mentioning DMARC conformance and failure report mail loops (Ticket #28).

#### B.2. 01 to 02

- \* Add a sentence to make clear that counting failures is not the aim.

#### B.3. 02 to 03

- \* Updated references.

#### B.4. 03 to 04

- \* Add an example report.
- \* Remove the old Acknowledgements section.
- \* Add a IANA Consideration section

#### B.5. 04 to 05

- \* Convert to markdown
- \* Remove irrelevant material.

## B.6. 05 to 06

- \* A Vesely was incorrectly removed from list of document editors. Corrected.
- \* Added Terminology section with recommended boilerplate re: RFC2119.

## B.7. 06 to 07

- \* Reduce Terminology section
- \* minor nits

## B.8. 07 to 08

- \* Specify what detailed information a report contains, in the 1st paragraph of Section 2
- \* A couple of typos

## B.9. 08 to 09

- \* Replace &lt; with < and &gt; with > in Appendix B

## B.10. 09 to 10

- \* Add an informative section about other failure reports (DKIM, SPF)

## B.11. 10 to 11

- \* Remove appendix with redundant examples - pull request by Daniel K.

## B.12. 11 to 12

- \* Reference Terminology in [I-D.ietf-dmarc-dmarcbis]
- \* Expand the Verifying External Destinations section and reference [I-D.ietf-dmarc-aggregate-reporting]

## B.13. 12 to 13

- \* Update references to numbered sections of [I-D.ietf-dmarc-dmarcbis] and [I-D.ietf-dmarc-aggregate-reporting]
- \* Clarify potential information disclosures when failure reports are sent
- \* Minor edits for readability and clarity

Authors' Addresses

Steven M Jones  
DMARC.org  
Email: [smj@dmarc.org](mailto:smj@dmarc.org)

Alessandro Vesely  
Tana  
Email: [vesely@tana.it](mailto:vesely@tana.it)