

Workgroup: DMARC Working Group
Internet-Draft:
draft-ietf-dmarc-failure-reporting-02

Obsoletes: [7489](#) (if approved)

Published: 17 August 2022

Intended Status: Standards Track

Expires: 18 February 2023

Authors: S. M. Jones, Ed. A. Vesely, Ed.

DMARC.org Tana

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

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 18 February 2023.

Copyright Notice

Copyright (c) 2022 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. Terminology and Definitions](#)
- [3. Failure Reports](#)
 - [3.1. Reporting Format Update](#)
 - [3.2. Verifying External Destinations](#)
 - [3.3. Transport](#)
- [4. IANA Considerations](#)
 - [4.1. Feedback Report Header Fields Registry Update](#)
 - [4.2. Authentication Failure Types](#)
- [5. Privacy Considerations](#)
 - [5.1. Data Exposure Considerations](#)
 - [5.2. Report Recipients](#)
- [6. Security Considerations](#)
- [7. Normative References](#)
- [8. Informative References](#)
- [Appendix A. Examples](#)
 - [A.1. Entire Domain, Monitoring Only, Per-Message Reports](#)
 - [A.2. Per-Message Failure Reports Directed to Third Party](#)
 - [A.3. Report Format Example](#)
- [Appendix B. Change Log](#)
- [Authors' Addresses](#)

1. Introduction

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 reported in aggregate form did occur. It is important to note these reports can contain either the header or the entire content of a failed message, which in turn may contain personally identifiable information, which should be considered when deciding whether to generate such reports.

2. Terminology and Definitions

This section defines terms used in the rest of the 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.

Readers are expected to be familiar with the contents of [[I-D.ietf-dmarc-dmarcbis](#)], specifically the terminology and definitions section.

3. Failure Reports

Failure reports can supply more detailed information about messages that failed to authenticate, enabling the Domain Owner to determine exactly what might be causing those specific failures.

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 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 3.1](#).

The destination(s) and nature of the reports are defined by the "ruf" and "fo" tags as defined in [Section 6.3](#) of [[I-D.ietf-dmarc-dmarcbis](#)].

Where multiple URIs are selected to receive failure reports, the report generator MUST make an attempt to deliver to each of them. External destinations MUST be verified, see [Section 3.2](#). Report generators SHOULD NOT consider ruf= tags in records having a psd=y tag, unless there are specific agreements between the interested parties.

An obvious consideration is the denial-of-service attack that can be perpetrated by an attacker who sends numerous messages purporting to be from the intended victim Domain Owner but that fail both SPF and DKIM; this would cause participating Mail Receivers to send failure reports to the Domain Owner or its delegate in potentially huge volumes. 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 paths. Various pruning techniques are possible, including the following:

- *store reports for a period of time before sending them, allowing detection, collection, and reporting of like incidents;
- *apply rate limiting, such as a maximum number of reports per minute that will be generated (and the remainder discarded);
- *only consider messages explicitly marked for debugging, where such a marking convention is established.

3.1. 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)

The syntax of this field is changed, dropping the DNS RRTYPE used:

```
spf-dns = "SPF-DNS:" [CFWS] domain [CFWS] ":"  
          [CFWS] quoted-string [CFWS] CRLF
```

Figure 1

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:

```
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 AFRF message for any or all of the underlying authentication methods.

3.2. Verifying External Destinations

If the target domain of a mailto address of a ruf= tag is not the same as the DMARC record domain where the tag was found, the report generator MUST verify that the target domain acknowledges sending those reports; the procedure is described in [Section 3](#) of [[I-D.ietf-dmarc-aggregate-reporting](#)].

3.3. Transport

Email streams carrying DMARC failure reports SHOULD provide DMARC-based authentication, so as to produce "dmarc=pass". This requirement is a MUST in case the report is sent through a host having a DMARC record with a ruf= tag. Indeed, special care must be taken of authentication in that case, as failure to authenticate failure reports may result in mail loops.

Reporters SHOULD rate limit the number of failure reports sent to any recipient to avoid overloading recipient systems. Again, in case the reports being sent are in turn at risk of being reported for DMARC authentication failure, reporters MUST make sure that possible mail loop are stopped.

4. IANA Considerations

4.1. Feedback Report Header Fields Registry Update

The following entry of the "Feedback Report Header Fields" registry has been modified to refer to this RFC:

Field Name:

Identity-Alignment

Description: indicates whether the message about which a report is being generated had any identifiers in alignment as defined in [\[I-D.ietf-dmarc-dmarcbis\]](#)

Multiple Appearances: No

Related "Feedback-Type": auth-failure

Reference: [[this rfc]]

Status: current

4.2. Authentication Failure Types

IANA has created the "Authentication Failure Types" registry. This registry contains defined email authentication failure types used in the "Auth-Failure:" field of message/feedback-report.

New registrations and updates MUST contain the following information:

1. Name
2. Description
3. Reference
4. Status

The initial entries of this registry are set as follows:

Name	Description	Reference	Status
adsp	The message did not conform to the author domain's published [RFC5617] signing practices. The DKIM-ADSP-DNS field MUST be included in the report.	[RFC6591]	historic
bodyhash	The body hash in the signature and the body hash computed by the verifier did not match. The DKIM-Canonicalized-Body field SHOULD be included in the report (see Section 3.2.4 of [RFC6591]).	[RFC6591]	current
revoked	The DKIM key referenced by the signature on the message has been revoked. The DKIM-Domain and DKIM-Selector fields MUST be included in the report.	[RFC6591]	current

Name	Description	Reference	Status
signature	The DKIM signature on the message did not successfully verify against the header hash and public key. The DKIM-Domain and DKIM-Selector fields MUST be included in the report, and the DKIM-Canonicalized-Header field SHOULD be included in the report (see Section 3.2.4 of [RFC6591]).	[RFC6591]	current
spf	The evaluation of the author domain's SPF record produced a "none", "fail", "softfail", "temperror", or "permerror" result. ("none" is not strictly a failure per [RFC7208] , but a service that demands successful SPF evaluations of clients could treat it like a failure.)	[RFC6591]	current
dmark	Some or all of the authentication mechanisms failed to produce aligned identifiers.	[[this rfc]]	current

Table 1

5. Privacy Considerations

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

5.1. Data Exposure Considerations

Failed-message reporting provides message-specific details pertaining to authentication failures. Individual reports can contain message content as well as trace header fields. Domain Owners are able to analyze individual reports and attempt to determine root causes of authentication mechanism failures, gain insight into misconfigurations or other problems with email and network infrastructure, or inspect messages for insight into abusive practices.

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 recipient.

Domain Owners requesting reports will receive information about mail claiming to be from them, which includes mail that was not, in fact, from them. Information about the final destination of mail where it might otherwise be obscured by intermediate systems will therefore be exposed.

When message-forwarding arrangements exist, Domain Owners requesting reports will also receive information about mail forwarded to domains that were not originally part of their messages' recipient lists. This means that destination domains previously unknown to the Domain Owner may now become visible.

Disclosure of information about the messages is being requested by the entity generating the email in the first place, i.e., the Domain Owner and not the Mail Receiver, so this may not fit squarely within existing privacy policy provisions. For some providers, failed-message reporting is viewed as a function similar to complaint reporting about spamming or phishing and is treated similarly under the privacy policy. Report generators (i.e., Mail Receivers) are encouraged to review their reporting limitations under such policies before enabling DMARC reporting.

5.2. Report Recipients

A DMARC record can specify that reports should be sent to an intermediary operating on behalf of the Domain Owner. This is done when the Domain Owner contracts with an entity to monitor mail streams for abuse and performance issues. Receipt by third parties of such data may or may not be permitted by the Mail Receiver's privacy policy, terms of use, or other similar governing document. Domain Owners and Mail Receivers should both review and understand if their own internal policies constrain the use and transmission of DMARC reporting.

Some potential exists for report recipients to perform traffic analysis, making it possible to obtain metadata about the Receiver's traffic. In addition to verifying compliance with policies, Receivers need to consider that before sending reports to a third party.

6. Security Considerations

Considerations discussed in [Section 11](#) of [\[I-D.ietf-dmarc-dmarcbis\]](#) apply.

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 5.1](#) all the more relevant.

7. 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>>.

[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>>.

[I-D.ietf-dmarc-dmarcbis] Herr, T. M. and J. Levine, "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", Work in Progress, Internet-Draft, draft-ietf-dmarc-dmarcbis-15, 28 July 2022, <<https://www.ietf.org/archive/id/draft-ietf-dmarc-dmarcbis-15.txt>>.

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

Brotman, A., "DMARC Aggregate Reporting", Work in Progress, Internet-Draft, draft-ietf-dmarc-aggregate-reporting-05, 20 April 2022, <<https://www.ietf.org/archive/id/draft-ietf-dmarc-aggregate-reporting-05.txt>>.

8. Informative References

[RFC5617] Allman, E., Fenton, J., Delany, M., and J. Levine, "DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)", RFC 5617, DOI 10.17487/RFC5617, August 2009, <<https://www.rfc-editor.org/info/rfc5617>>.

[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>>.

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014, <<https://www.rfc-editor.org/info/rfc7208>>.

[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>>.

Appendix A. Examples

This section presents some examples related to the use of DMARC reporting functions.

A.1. Entire Domain, Monitoring Only, Per-Message Reports

The owners of the domain "example.com" have deployed SPF and DKIM on their messaging infrastructure. As described in, [Appendix B.2.1](#) of [\[I-D.ietf-dmarc-aggregate-reporting\]](#) they have used the aggregate reporting to discover some messaging systems that had not yet implemented DKIM correctly. However, they are still seeing periodic

authentication failures. In order to diagnose these intermittent problems, they wish to request per-message failure reports when authentication failures occur.

Not all Receivers will honor such a request, but the Domain Owner feels that any reports it does receive will be helpful enough to justify publishing this record. The default per-message report format ([RFC6591](#)) meets the Domain Owner's needs in this scenario.

The Domain Owner accomplishes this by adding the following to its policy record:

```
*Per-message failure reports should be sent via email to the
  address "auth-reports@example.com" ("ruf=mailto:auth-
  reports@example.com")
```

The updated DMARC policy record might look like this when retrieved using a common command-line tool (the output shown would appear on a single line but is wrapped here for publication):

```
% dig +short TXT _dmarc.example.com.
"v=DMARC1; p=none; rua=mailto:dmarc-feedback@example.com;
ruf=mailto:auth-reports@example.com"
```

To publish such a record, the DNS administrator for the Domain Owner might create an entry like the following in the appropriate zone file (following the conventional zone file format):

```
; DMARC record for the domain example.com

_dmarc  IN TXT ( "v=DMARC1; p=none; "
                "rua=mailto:dmarc-feedback@example.com; "
                "ruf=mailto:auth-reports@example.com" )
```

A.2. Per-Message Failure Reports Directed to Third Party

The Domain Owner from the previous example is maintaining the same policy but now wishes to have a third party receive and process the per-message failure reports. Again, not all Receivers will honor this request, but those that do may implement additional checks to validate that the third party wishes to receive the failure reports for this domain.

The Domain Owner needs to alter its policy record from [Appendix A.1](#) as follows:

```
*Per-message failure reports should be sent via email to the
  address "auth-reports@thirdparty.example.net" ("ruf=mailto:auth-
  reports@thirdparty.example.net")
```

The DMARC policy record might look like this when retrieved using a common command-line tool (the output shown would appear on a single line but is wrapped here for publication):

```
% dig +short TXT _dmarc.example.com.  
"v=DMARC1; p=none; rua=mailto:dmarc-feedback@example.com;  
ruf=mailto:auth-reports@thirdparty.example.net"
```

To publish such a record, the DNS administrator for the Domain Owner might create an entry like the following in the appropriate zone file (following the conventional zone file format):

```
; DMARC record for the domain example.com  
  
_dmarc IN TXT ( "v=DMARC1; p=none; "  
                "rua=mailto:dmarc-feedback@example.com; "  
                "ruf=mailto:auth-reports@thirdparty.example.net" )
```

Because the address used in the "ruf" tag is outside the Organizational Domain in which this record is published, conforming Receivers will implement additional checks as described in [Section 3.2](#) of this document. In order to pass these additional checks, the third party will need to publish an additional DNS record as follows:

```
*Given the DMARC record published by the Domain Owner at  
  "_dmarc.example.com", the DNS administrator for the third party  
  will need to publish a TXT resource record at  
  "example.com._report._dmarc.thirdparty.example.net" with the  
  value "v=DMARC1;".
```

The resulting DNS record might look like this when retrieved using a common command-line tool (the output shown would appear on a single line but is wrapped here for publication):

```
% dig +short TXT example.com._report._dmarc.thirdparty.example.net  
"v=DMARC1;"
```

To publish such a record, the DNS administrator for example.net might create an entry like the following in the appropriate zone file (following the conventional zone file format):

```
; zone file for thirdparty.example.net  
; Accept DMARC failure reports on behalf of example.com  
  
example.com._report._dmarc  IN  TXT  "v=DMARC1;"
```

Intermediaries and other third parties should refer to [Section 3.2](#) for the full details of this mechanism.

A.3. Report Format Example

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

Received: from generator.example (generator.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=generator.example; s=mail; t=1658210268;
bh=rCrh1aFDE8d/Fltt8wbcu48bLOu40M23QXqphUZPAIM=;
h=From:To:Date:Subject:From;
b=IND9JkuwF9/5841kzxMbPeej0VYimVzNKozR2R89M8eY02z0lCBb1x507Gz0YK7mE
/h6pslWm0ODBVFzLlwY9CXv4Vu62QsN0RBIXHPjEX0koM2VCD5zCd+5i5dtCFX7Mxh
LThb2ZJ3efklbSB9RQRwxcmRvCPV7z6lt/Ds9sucVE1RD0DYHjx+iWnAUQrlos6ZQb
u/YOUGjf60LPpyljfPu3EpFwo80mSHyQlP/4S5KEykgPQMgCqLPPKvJwu1aAIDj+jG
q2yl03fmc/ERDeDWACTR67YNabEKBWtjqCRLNxKttazViJTZ5drcLfpX0853KoougX
Rltp7zdoLdy4A==
From: DMARC Filter <DMARC@generator.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@generator.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: generator.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=generator.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: generator.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.generator.example (Postfix) with ESMTP id 5E8B0C159826
for <x@generator.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@generator.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/g7ForvDbnyyDLYSjauMYMW6sEIQu75/9w30IONg=;
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/g7ForvDbnyyDLYSjauMYMW6sEIQu75/9w30IONg=;
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/Rwi8Zd2WZTXWneQGRC0JLRcbBJpjqrwtqd
76IqawH86tihz4Z/12J1GBCdNx1gfazsoI3yaqfooRDYg0mSyZHRyYhQBmodnPcqZj4
/25L5278sc/UNrY09az2n7R/skbVZ0bvSo2eEiGU8fcp08+a5SKNYskhaviAI4eGIB
iRMdEP7gP8dESdnZguNbY5HI32UMDPpNqajzd/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/g7ForvDbnyyDLYSjauMYMW6sEIQu75/9w30IONg=;
h=Date:Subject:To:References:From:In-Reply-To;
b=hETrymCbz6T1Dyo5dCG9dk8rPykKLdhJCPFeJ9TiiP/kaon2afpUYtj+SrI+I83lp
p1F/FfYSGy7zz3Q30dxBA==
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=consumer.example; s=delta; t=1658210255;
bh=KYH/g7ForvDbnyyDLYSjauMYMW6sEIQu75/9w30IONg=;
h=Date:To:References:From:In-Reply-To;
b=C2nsAp3AMNX33Nq7nN/StPo921xE3XGF8Ju3iAKdYB3EKhsril0N5IjWGlg1JECst
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_--

Figure 2

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

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

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>

*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 https://mailarchive.ietf.org/arch/msg/dmarc/mFk0qiTCy8tzghRvcxus01W_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).

01 to 02

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

02 to 03* Updated references.

03 to 04* Add an example report.

*Remove the old Acknowledgements section.

*Add a IANA Consideration section

Authors' Addresses

Steven M Jones (editor)
DMARC.org

Email: smj@dmarc.org

Alessandro Vesely (editor)
Tana

Email: vesely@tana.it