DMARC Working Group
Internet-Draft
Obsoletes: 7489 (if approved)
Intended status: Standards Track
Expires: 21 August 2022

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

20 February 2022

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

draft-ietf-dmarc-failure-reporting-03

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 21 August 2022.

Copyright Notice

Table of Contents

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.

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 aggregation techniques are possible, including the following:

* only send a report to the first recipient of multi-recipient messages;

* 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).

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 if the message was signed by DKIM)

   * DKIM-Canonicalized-Header, DKIM-Canonicalized-Body (OPTIONAL if the message was signed by DKIM)

   * SPF-DNS (REQUIRED)

2. The "Identity-Alignment" field is defined to contain a comma-separated list of authentication mechanism names that produced 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

The procedure described for aggragate reports Section 2.1 of [I-D.ietf-dmarc-aggregate-reporting] applies to failure reports as well.

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. Privacy Considerations

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

4.1. 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.

4.2. 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.

5. 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 4.1 all the more relevant.

6. 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-05, 22 January 2022, <https://tools.ietf.org/html/draft-ietf-dmarc-dmarcbis-05>.

[I-D.ietf-dmarc-aggregate-reporting] Brotman, A., "DMARC Aggregate Reporting", Work in Progress, Internet-Draft, draft-ietf-dmarc-aggregate-reporting-04, 13 December 2021, <https://tools.ietf.org/html/draft-ietf-dmarc-aggregate-reporting-04>.

7. Informative References

[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>.

[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.

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.

Acknowledgements

DMARC and the draft version of this document submitted to the Independent Submission Editor were the result of lengthy efforts by an informal industry consortium: DMARC.org (see http://dmarc.org (http://dmarc.org)). Participating companies included Agari, American Greetings, AOL, Bank of America, Cloudmark, Comcast, Facebook, Fidelity Investments, Google, JPMorgan Chase & Company, LinkedIn, Microsoft, Netease, PayPal, ReturnPath, The Trusted Domain Project, and Yahoo!. Although the contributors and supporters are too numerous to mention, notable individual contributions were made by J. Trent Adams, Michael Adkins, Monica Chew, Dave Crocker, Tim Draegen, Steve Jones, Franck Martin, Brett McDowell, and Paul Midgen. The contributors would also like to recognize the invaluable input and guidance that was provided early on by J.D. Falk.

Additional contributions within the IETF context were made by Kurt Anderson, Michael Jack Assels, Les Barstow, Anne Bennett, Jim Fenton, J. Gomez, Mike Jones, Scott Kitterman, Eliot Lear, John Levine, S. Moonesamy, Rolf Sonneveld, Henry Timmes, and Stephen J. Turnbull.

Authors' Addresses

Steven M Jones (editor)
DMARC.org

Email: smj@dmarc.org

Alessandro Vesely (editor)
Tana

Email: vesely@tana.it