Workgroup: Network Working Group
Internet-Draft: draft-adams-bimi-reporting-03
Published: 9 October 2022
Intended Status: Informational
Expires: 12 April 2023
Authors: T. Adams
Proofpoint
A. Brotman
Comcast, Inc.

# BIMI Reporting

## Abstract

To support the utility of Brand Indicators for Message Identification (BIMI), domains publishing BIMI records may find it useful to know when their logos are failing to be displayed as expected. When an entity, for example a mailbox operator, determines whether or not to display the logo identified in the BIMI record, they may encounter errors trying to retrieve the image file. Similarly, the associated evidence document used to validate the logo may fail evaluation. In other cases, the evaluator may decide that despite everything validating, they may rely on local policies that determine validated logos should still not be displayed. This specification defines how BIMI evaluators should report their evaluation outcome back to the publisher within the context of existing Domain-based Message Authentication, Reporting, and Conformance (DMARC) reports.

## 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 12 April 2023.

**Table of Contents**



## 1. Introduction

Organizations sending email associated with specific brands and domains may use Brand Indicators for Message Identification (BIMI) [I-D.blank-ietf-bimi] to signal which brand identifier (e.g. a company logo) should be displayed when receiving authenticated email for the specified domain. This document is intended as a companion to the BIMI specification as it defines the associated error reporting method and schema. It includes information necessary for Domain Owners to identify and troubleshoot potential issues related to the evaluation of the elements identified within their BIMI records.

The document supports the ability for a domain sending email to identify and diagnose problems with their BIMI deployment. It is designed to be as easy to deploy as possible for BIMI reporters and report consumers. It integrates with existing Domain-based Message

Authentication, Reporting, and Conformance (DMARC) [RFC7489] aggregate reporting (RUA) rather than adding a new reporting mechanism. The data being reported is aggregated in a way that respects the privacy of senders, receivers, and users by not leaking potentially sensitive information.

This document is intended as a companion to the BIMI specification draft [I-D.blank-ietf-bimi] by adding reporting abilities.

### 1.1. Terminology and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] and [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document is designed to operate within the context of Internet Mail service, as defined in [RFC5598], as well as the reporting structure defined by [RFC7489]. In addition to the terms defined below, some terminology throughout the document has been inherited from those specifications.

**Aligned Domain:** The FQDN that passes the DMARC evaluation to determine where to initially look the associated DMARC policy record.

**Assertion Domain:** The FQDN where the BIMI record associated with an email is found.

**Evaluator:** The entity or organization that evaluates the BIMI assertions when an email is received and has passed DMARC evaluation. This may be the email receiver (e.g. the MX server identified as the inbound MTA gateway), or another entity that processes the email later in the email evaluation pipeline. For example, an MTA may perform DMARC and BIMI evaluation within a single authentication process, while in some contexts DMARC evaluation may occur at a perimeter MTA while BIMI evaluation is performed by another MTA later in the process (which may or may not be operated by the same organization).

**Report:** The data compiled by the Evaluator about how it evaluated BIMI in relation to email sent from, or on behalf of, a specified domain.

**Reporter:** The operator that sends Reports to the Report Consumer identified within the applicable DMARC record.

**Report Consumer:** An operator that receives Reports from a Reporter implementing the reporting mechanism described in this document.

Such an operator might be receiving reports about its own messages, or Reports about messages related to another operator. This term applies collectively to the system components that receive and process these reports and the organizations that operate them.

**Selector Name:** The name of the BIMI selector, if one exists, within the designated header field in an email. If no specific BIMI selector is identified, the Selector Name is assumed to be "default".

## 2. Identifying the Report Consumer

Given that BIMI relies on DMARC evaluation, this document does not define a separate Report Consumer outside the context of DMARC. The BIMI Report MUST be included as part of a DMARC report sent to the RUA address identified within the applicable DMARC record for the email being evaluated. The applicable Report address is determined by the DMARC policy discovered for the Aligned Domain of the sending email. This may be the Fully-Qualified Domain Name (FQDN) [RFC1983], or Organizational Domain as determined by DMARC evaluation. Note that the domain of the applicable DMARC policy may not be the same domain where the applicable BIMI record is discovered.

### 2.1. Example 1: Sub-domain Reporting

For example, consider the following situation in which an Organizational Domain (i.e. "example.com") has slightly different DMARC and BIMI reporting configurations for the two FQDNs:

**Domain: example.com** Publishes a DMARC record
*Requests RUA reports be sent to "rua@example.com"
*Publishes a BIMI record

**Domain: sub.example.com** Publishes a DMARC record
*Requests RUA reports sent to "rua@sub.example.com"
*Does not publish a BIMI record

When the organization sends email with the [RFC5322].From domain set to "sub.example.com", the Evaluator does not find a BIMI record at the FQDN, but does find one at the Organizational Domain level: "example.com".

The Evaluator sends BIMI reports to the applicable report consumer identified within the Aligned Domain's DMARC record: "rua@sub.example.com", not to the RUA address associated with the Organizational Domain where the BIMI record was discovered.

### 2.2. Example 2: Inherited Reporting

In another example, consider another situation in which an Organizational Domain (i.e. "example.com") has slightly different DMARC and BIMI reporting configurations for the two FQDNs:

**Domain: ěxample.com** Publishes a DMARC record covering all sub-domains
*Requests RUA reports be sent to "rua@example.com"
*Publishes a BIMI record

**Domain: šub.example.com** Does not publish a DMARC record
*Does not publish a BIMI record

When the organization sends email with the [RFC5322].From domain set to "sub.example.com", the Evaluator does not find a BIMI record at the FQDN, but does find one at the Organizational Domain level: "example.com".

The Evaluator sends BIMI reports to the applicable report consumer identified for the Aligned Domain which is discovered within the applicable DMARC record published at the organizational domain: "rua@example.com".

## 3. Reporting Schema

The following data defined in this section MUST be reported within the context of an XML-formatted DMARC [RFC7489] Aggregate Report (RUA). Given the reliance on DMARC evaluation, the BIMI Reports are sent as additional elements within RUA reports, inheriting its terminology and metadata (e.g. "date_range", "report_id", etc.).

The complete set of BIMI Report elements and attributes are collected within a single top-level <bimi> element within the RUA <xml> root element (i.e. at the same level as the <record> elements). The <bimi> element SHOULD be the last top-level element within the <xml> root element, but MAY be placed in any order in relation to other top-level elements.

The nested structure of the elements is illustrated below. The attributes and contents for each element are described in more detail in the following sections.

```
<bimi>
  <domain>
    <assertion>
      <evidence />
      <errors>
        <assertion>[count]</assertion>
        <evidence>[count]</evidence>
        <indicator>[count]</indicator>
        <undefined>[count]</undefined>
      </errors>
    </assertion>
  </domain>
</bimi>
```

### 3.1. <domain> Element

Within the <bimi> element is one or more <domain> elements, each element of which MUST include the following attributes:

**"aligned" (REQUIRED):** The Aligned Domain.

**"assertion" (REQUIRED):** The Assertion Domain.

Each <domain> element MUST represent a unique "aligned":"assertion" tuple within the enclosing <bimi> element. All BIMI assertion records related to this domain tuple MUST be reported within this element.

### 3.2. <assertion> Element

The content of each <domain> element MUST include one or more <assertion> elements, each element of which MUST include the following attributes:

**"selector" (REQUIRED):** The Selector Name defined by the relevant email header, or set to "default" if no Selector Name was specifically defined.

**"l" (REQUIRED):** The field extracted from the "l=" field within the BIMI assertion record. If blank, the attribute label MUST be present, and the attribute MUST be set to "unpublished".

**"a" (REQUIRED):** The field extracted from the "a=" field within the BIMI assertion record. If blank, the attribute label MUST be present, and the attribute MUST be left blank (i.e. a="")

Each <assertion> element MUST represent a unique "selector":"l":"a" tuple within the enclosing <domain> element. All errors related to this assertion tuple MUST be reported within this element.

In the case in which a non-default Selector Name is provided, but the evaluation of the referenced selector results in an error, and evaluation of the default selector also results in an error, both the initial error and the default selector errors are reported within separate <assertion> elements. One <assertion> element will include the "selector" attribute set to "default"', and the other will include the "selector" attribute set to the Selector Name identified in the email.

### 3.3. <evidence> Element

The <evidence> element is OPTIONAL and is only REQUIRED if the attributes as described below are included in the Report. The <evidence> element is a null element that contains the following attributes:

**"evidence-date" (OPTIONAL):** A [RFC5322]-formatted date expression indicating when the evidence document was evaluated. Evaluators MAY periodically evaluate Evidence Documents and locally cache the results for some period of time before re-evaluating them.

**"evidence-issuer" (OPTIONAL):** The issuer of the Evidence Document retrieved and evaluated.

**"evidence-type" (OPTIONAL):** The type of Evidence Document retrieved and evaluated.

**"evidence-url" (OPTIONAL; REQUIRED if the "a=" field is populated):** The URL defined by the "a=" field within the BIMI record pointing to the authority Evidence Document. If the field exists and is populated, but evaluation of the field results in errors during parsing or retrieval, the attribute is set to the value of the "a=" field, and the appropriate set of "evidence-error-" elements (defined below) are populated).

### 3.4. <errors> Element

All errors to be reported MUST be included within the <errors> element which is within the <assertion> element. Within the <errors> element are one or more elements containing the error data aggregated as described below. If there are no errors within a reporting period, the <errors> element MUST NOT exist in the Report.

The count of non-zero errors being reported MUST be grouped by the logical tuple:

ERROR-NAME:class:type

Where ERROR-NAME is an element named one of:

*"assertion"
*"evidence"
*"indicator"
*"undefined"

The "class" for each error tuple is set to one of:

**"temp"** If the Evaluator determines that the error is temporary (e.g. a recoverable error such as a DNS query timeout when trying to retrieve the resource), the Evaluator MAY rely on a previously cached result and SHOULD set the class of the error to "temp". Doing so indicates the Evaluator will try again in the future for updated results. For example, a temporary error may cause an Evaluator to stop processing BIMI for a single message, but try again for the next message it receives from the domain.

**"perm"** If the Evaluator determines that the error is permanent (e.g. the resource is successfully retrieved, but is non-conformant), the Evaluator SHOULD set the class to "perm". Doing so indicates the Evaluator MAY stop evaluating BIMI for all messages from the specified domain until additional information becomes available.

The "type" component of the tuple is defined for the specific error elements in their descriptions below.

There MUST only be one instance of a specific error tuple per Report, each of which aggregates the count of errors associated with that tuple during the report period. There MAY be multiple error elements with the same name, but the tuples MUST be differentiated by distinct element attributes.

For example, the <errors> element may contain two <indicator> error elements. One <indicator> error element may contain a "class=temp" attribute, while the other may contain a "class=perm" attribute. Each of which aggregates the count of the specified class of errors.

### 3.4.1. <assertion> Errors Element

The <assertion> errors element is OPTIONAL and is only REQUIRED if there are assertion errors to report. The <assertion> error element encloses a positive natural number indicating the count of assertion errors encountered during the reporting period for the set of element attributes indicating the class, type, and (optionally) description:

**"class" Attribute:**
Set to either "temp" or "perm" depending upon whether the Evaluator is treating the errors as temporary or permanent.

**"type" Attribute:** Set to one of:

* "retrieval" if the Evaluator was unable to successfully retrieve the assertion record (e.g. receiving a DNS RCODE:3 when trying to retrieve the selector)

* "parsing" if one or more fields in the BIMI assertion record fails to parse (e.g. the value in the "l=" or "a=" fields contain unexpected characters)

**"description" Attribute (OPTIONAL):** Free-form text provided by the Evaluator indicating any specific details they believe useful to understanding the error(s). The element SHOULD contain no more than 256 characters.

### 3.4.2. <evidence> Errors Element

The <evidence> errors element is OPTIONAL and is only REQUIRED if there are evidence errors to report. The <evidence> error element encloses a positive natural number indicating the count of evidence errors encountered during the reporting period for the set of element attributes indicating the class, type, and (optionally) description:

**"class" Attribute:** Set to either "temp" or "perm" depending upon whether the Evaluator is treating the errors as temporary or permanent.

**"type" Attribute:** Set to one of:

* "retrieval" if the Evaluator was unable to successfully retrieve the authority evidence document (e.g. receiving a DNS RCODE:3 when trying to retrieve the document)

* "parsing" if the authority evidence document in the BIMI record fails to parse (e.g. the URI identified in the BIMI record contains invalid characters)

* "validation" if the retrieved authority evidence document fails to validate (e.g. the retrieved X.509 [RFC5280] certificate fails to validate)

* "expired" if the authority evidence document has expired (e.g. the retrieved X.509 certificate expiration date has passed at the time of validation)

*"revoked" if the authority evidence document has been reported as being revoked (e.g. the X.509 certificate being evaluated, or any in its progenitor chain, have been reported to the issuer's Certificate Revocation List)

*"policy" if the Evaluator determines that, even if the authority evidence document is technically validated, they have additional information that may impact the evaluation (e.g. the Evaluator has a local policy that doesn't recognize the issuing authority, the evidence type is deemed insufficient, etc.)

**"description" Attribute:** Free-form text provided by the Evaluator indicating any specific details they believe useful to understanding the error(s). The element SHOULD contain no more than 256 characters.

#### 3.4.3. <indicator> Errors Element

The <indicator> errors element is OPTIONAL and is only REQUIRED if there are indicator errors to report. The <indicator> errors element encloses a positive natural number indicating the count of indicator errors encountered during the reporting period for the set of element attributes indicating the class, type, and (optionally) description:

**"class" Attribute:** Set to either "temp" or "perm" depending upon whether the Evaluator is treating the errors as temporary or permanent.

**"type" Attribute:** Set to one of:

*"retrieval" if the Evaluator was unable to successfully retrieve the indicator (e.g. receiving a DNS RCODE:3 when trying to retrieve the indicator)

*"parsing" if the indicator in the BIMI record fails to parse (e.g. the indicator cannot be extracted from the presented evidence document)

*"validation" if the Evaluator cannot validate that the indicator can be used in the context of BIMI (e.g. the SVG document referenced by the "l=" URI isn't a valid SVG Tiny Portable Secure (SVG P/S) [I-D.svg-tiny-ps-abrotman] profile)

**"description" (OPTIONAL):** Free-form text provided by the Evaluator indicating any specific details they believe useful to understanding the error(s). The element SHOULD contain no more than 256 characters

#### 3.4.4. <undefined> Errors Element

The <undefined> errors element is OPTIONAL and SHOULD be used to report errors that are not covered by other error elements. The <undefined> errors element encloses a positive natural number indicating the count of undefined errors encountered during the reporting period for the set of element attributes indicating the class and (optionally) description:

**"class" Attribute:** Set to either "temp" or "perm" depending upon whether the Evaluator is treating the error as temporary or permanent.

**"description" Attribute:** Free-form text provided by the Evaluator indicating any specific details they believe useful to understanding the error(s). The element SHOULD contain no more than 256 characters.

## 4. Acknowledgements

This document was informed by discussions with and/or contributions from Arne Allisat, Kurt Andersen, Tom Bartel, Marcel Becker, Seth Blank, Marc Bradshaw, Alex Brotman, Wei Chuang, Todd Herr, Neil Kumaran, Hansen Lee, Thede Loder, Maddie McCaffrey, Alex Rubin, Len Shneyder, and Matthew Vernhout.

## 5. IANA Considerations

This section will be filled out in more detail when the draft moves toward completion.

## 6. Security Considerations

Security considerations related to this document are inherited from those mentioned in [RFC7489] and [I-D.blank-ietf-bimi]. This section will be filled out in more detail when the draft moves toward completion.

## 7. On-going Discussions

*Can/Should the BIMI report data include information about MUA use of BIMI images?

-Concerns about web bugs?
-What information would be provided?
-How is data aggregated?

## 8. References

### 8.1. 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>.

**[RFC5280]** Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

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

**[RFC5598]** Crocker, D., "Internet Mail Architecture", RFC 5598, DOI 10.17487/RFC5598, July 2009, <https://www.rfc-editor.org/info/rfc5598>.

**[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>.

**[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>.

### 8.2. Informative References

**[I-D.blank-ietf-bimi]** Blank, S., Goldstein, P., Loder, T., Zink, T., and M. Bradshaw, "Brand Indicators for Message Identification (BIMI)", Work in Progress, Internet-Draft, draft-blank-ietf-bimi-02, 9 March 2021, <https://datatracker.ietf.org/doc/html/draft-blank-ietf-bimi-02>.

**[I-D.svg-tiny-ps-abrotman]** Brotman, A. and J. T. Adams, "SVG Tiny Portable/Secure", Work in Progress, Internet-Draft, draft-svg-tiny-ps-abrotman-01, 9 March 2021, <https://datatracker.ietf.org/doc/html/draft-svg-tiny-ps-abrotman-01>.

**[RFC1983]** Malkin, G., Ed., "Internet Users' Glossary", FYI 18, RFC 1983, DOI 10.17487/RFC1983, August 1996, <https://www.rfc-editor.org/info/rfc1983>.

## Appendix A. Example RUA Report with BIMI

The following is an example DMARC RUA report with BIMI error elements.

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <report_metadata>
    <org_name>reporter.tld</org_name>
    <email>info@reporter.tld</email>
    <report_id>uniqueidentifier</report_id>
    <date_range>
      <begin>1609459200M</begin>
      <end>1609545599</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>sender.tld</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>reject</p>
    <sp>reject</sp>?
    <pct>100</pct>
  </policy_published>
  <record>
    <row>
      <source_ip>192.0.2.1</source_ip>
      <count>10</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>pass</dkim>
        <spf>pass</spf>
      </policy_evaluated>
    </row>
    <identifiers>
      <header_from>sender.tld</header_from>
    </identifiers>
    <auth_results>
      <dkim>
        <domain>sender.tld</domain>
        <result>pass</result>
        <selector>selector01</selector>
      </dkim>
      <spf>
        <domain>sender.tld</domain>
        <result>pass</result>
      </spf>
    </auth_results>
  </record>
  <bimi>
    <domain aligned="sender.tld" assertion="sender.tld">
      <assertion selector="default" a=""
        l="https://www.sender.tld/images/logos/bimi.svg">
        <evidence />
```

```
            <errors>
              <indicator class="temp" type="retrieval"
                description="DNS RCODE:3">1</indicator>
            </errors>
          </assertion>
        </domain>
      </bimi>
    </feedback>
```

## Authors' Addresses


J. Trent Adams
Proofpoint
105 Edgeview Drive, Suite 440
Broomfield, CO 80021
United States of America

Email: tadams@proofpoint.com

Alex Brotman (ed)
Comcast, Inc.

Email: alex_brotman@comcast.com