Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 22 December 2025

A. Brotman
Comcast, Inc

20 June 2025

BIMI on an Independent MUA
draft-brotman-bimi-mua-00

Abstract

This document describes a method by which a receiving MTA may insert Brand Indicators for Message Identification (BIMI) headers into a message in such a way that a third party MUA can not only use the information in those headers but also validate that the headers were inserted by the MTA.

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 22 December 2025.

Table of Contents

1. Introduction

Brand Indicators for Message Identification (BIMI) describes a method to enable Domain Owners to coordinate with Mailbox Providers (MBPs), Mail Transfer Agents (MTAs), and Mail User Agents (MUAs) in the display of brand-specific Indicators (e.g., logos) next to properly authenticated messages.

BIMI relies on DMARC, which in turn relies on one of SPF or DKIM validation for the message in question, and it is generally accepted that an MTA is best positioned to do the SPF and DKIM validation that underpin DMARC since it has the access to the data necessary for such

validation. An MUA almost certainly cannot perform SPF validation on a message, as it will not know the sending IP of the message (short of attempting to interpret Received headers), and an MUA could only perform DKIM validation on a message if the MTA has not altered the DKIM-protected parts of the message. This makes the simplest path to the display of a BIMI Indicator one where the MTA performs the required checks for DMARC and BIMI and records the results of those checks in a way that can be accessed by the MUA.

BIMI makes no requirement that the MTA handling a message and the MUA reading and displaying it are operated by the same entity. In cases where a mailbox holder uses their MBP's MUA to read the contents of their mailbox, it is a relatively simple matter for the MTA and MUA to interoperate in a way in which the display of the BIMI Indicator can be controlled by the MBP.

What is less simple is the interoperability between an MBP's MTAs and message stores and an independent, or third-party, MUA. In this scenario, there must exist a standard way for an MTA to communicate BIMI and DMARC validation results to the MUA in a way that can be verified by the MUA. In addition, the MBP through its message store may desire to be able to indicate that a BIMI Indicator and/or its Evidence Document has been revoked if circumstances require.

This document describes a method for achieving interoperability between a MBP's MTAs and message stores, and a third-party MUA. Without this link, an attacker could potentially insert messages with existing headers through some other means, SMTP and IMAP are examples here. Using this verifiable method allows for the MUA to understand the validation at the MTA layer.

2. Validation Information

The receiving entity may add two headers, BIMI-Location and BIMI-Indicator. These two headers are meant to aid the MUA with the location of the BIMI-related information, as well as base64-encoded SVG image data. They could also insert an Authentication-Results header at this stage.

Additionally, a receiver employing this method MUST add another header to the message, BIMI-Receiver-Information. This will contain a date-time (from [RFC5322]), and sha256-encoded hash from the local part of the recipient, and then the domain (From the RFC5321 RCPT TO command):

BIMI-Receiver-Information: date: date-time ; rcpt: sha256-local @ domain

date-time: RFC5322

domain: RFC5321

sha256-local: 64(HEXDIG)

An example might be:

BIMI-Receiver-Information: date: Tue, 25 Feb 2023 01:05:55 +0000 ; rcpt: 6d9010b2b7a1483b256ae7477738dba7c530bd9ba53db1d6691441e74b83608a@isp.net

A MBP may choose to add this data without the signature specified below. However, as the data cannot be verified via the signature, the MUA may find the data within the header unsatisfactory to be used.

NOTE: Changed to 5321, instead of 5322

3. BIMI-Receiver-Signature

The MTA or other entity that performed the BIMI validation of the message MUST, if the message passed all BIMI validation checks, insert a BIMI-Receiver-Signature header constructed in a manner consistent with the creation of a DKIM-Signature header as defined in [RFC6376]. This header MUST include all the BIMI-Location, BIMI-Selector, and BIMI-Receiver-Information headers as headers that were signed by this signature. Additionally, the signer should oversign the headers included as part of this signature as defined in [RFC6376].

CLARIFICATION: Is this Receiver-Signature header useful without the other headers? Today, not all MBPs insert these headers. Can this still be useful?

This signature will be validated by the MUA in the same manner that a DKIM-Signature header is validated, and successful validation of this header will indicate that the receiving domain inserted the signed headers.

The public key to support this signing activity will be published in the DNS at a location one or more levels below the name "_bimi.signingDomain", where "signingDomain" is the domain associated with the address in the RCPT TO command. By utilizing a different "namespace", this prevents this particular key from being used in DKIM Replay attacks. For example, an MBP named "isp.net" might publish its public key at "sel_sign._local._bimi.isp.net". For the purposes of this document, we will refer to "sel_sign" as the "True Selector".

The selector specified in the s= tag of this signature will be a pseudo-selector constructed by prepending the FQDN domain from the the BIMI discovery to the "True Selector". In the INFORMATIVE EXAMPLE of a BIMI-Receiver-Signature header shown below, the s= tag is assigned the value "marketing.example.org.sel_sign", which means that the BIMI information for the message was found at the domain "marketing.example.org".

DISCUSS: Terminology around which domain is used above, and how we reference it.

DISCUSS: Other headers? Other information?

BIMI-Receiver-Signature: v=BIMI1; d=isp.net; s=marketing.example.org.sel_sign; c=canonicalization; h=BIMI-Location:BIMI-Selector:BIMI-Receiver-Information; b=<SIGNATURE_BLOB>; t=timestamp

The public key used for validation by the MUA would be:

marketing.example.org.sel_sign._local._bimi.isp.net

The mechanics of the public key publishing are covered in sections below.

3.1. Public Key Publishing

While the above method describing "pseudo-selectors" might seem to require that isp.net publish an infinite number of DKIM public keys in order to support validation of its BIMI-Receiver-Signature headers, that is not the case. Instead, validation of these signature headers will rely on publishing a DNS wildcard record, while revocation of BIMI logos will rely on the publishing of empty records to match the domains for which the MBP no longer wishes to support validation of BIMI logos.

As mentioned in the previous section, the MBP will publish its public key for supporting validation of BIMI-Receiver-Signatures at the name matching this pattern:

<True Selector>._local._bimi.<signing Domain>

In the example above that would mean publishing a DKIM public key as follows:

sel_sign._local._bimi.isp.net TXT "v=BIMI1; p=<public_key_data>"

To support validation of its signatures where the selector is the "pseudo-selector" described in the previous section, the MBP will also publish the following DNS wildcard record:

*.sel_sign._local._bimi.isp.net CNAME sel_sign._local._bimi.isp.net.

When the MUA performs a lookup, the wildcard MUST match and provide the MUA with the proper public key to validate the signature.

4. MUA Validation

NOTE: Stub, needs elaboration

As with DKIM, the MUA will use the cryptographic signature to validate the protected contents. Additionally, the MUA may use a sha-256 hash to validate the message and signature are meant for the recipient using the MUA. By validating the recipient, this could aid with replay protection.

5. Revocation

There could exist any number of reasons for a receiving entity to no longer desire to display iconography related to a given sending domain. This could include certificate revocation from the CA, diminished local reputation, extensive abuse reports, certificate expiration, or anything else.

In the case where this happens, the MBP (again, isp.net) can publish a NULL record at the location where the domain would normally match a wildcard. The MBP may optionally choose to include a string as to the reason for revocation by utilizing the r tag in the record. If we also use marketing.example.org with a selector of "foo", this MUST appear as:

foo._s.marketing.example.org.sel_sign._local._bimi.isp.net TXT ’v=BIMI1;’ foo._s.marketing.example.org.sel_sign._local._bimi.isp.net TXT ’v=BIMI1;"r=Reason String;"’

The DNS response MUST not include a functional public key that could be used to validate the signature. If compared to the wildcard DNS entry defined earlier, there will no longer be a public key that can be used for validation. The DNS record MUST contain only a v tag, MAY contain an optional r tag, and MUST NOT contain a p (public key) tag.

This should ensure the MUA is no longer able to retrieve the public keys necessary to validate the signature. In this case, the MUA MUST NOT utilize the headers, even though they do still exist in the stored message.

See the Appendix for how revocation would look in practice.

5.1. Wildcard Revocation

Three situations could exist here. A MBP would like to revoke multiple third-level domains for a single apex domain. Another could be that the MBP would like to rotate older keys.

5.1.1. Multi-domain Revocation

In a case where the domain example.org sends messages as:

marketing.example.org
billing.example.org

And the MBP would like to revoke for the entirety of example.org, a wildcard record could be published to match multiple:

example.org.sel_sign._local._bimi.isp.net TXT 'v=BIMI1;'
*.example.org.sel_sign._local._bimi.isp.net TXT 'v=BIMI1;'

5.1.2. Multi-selector Revocation

If the MBP would prefer to revoke all selectors for a given domain, it could be published with a wildcard:

*._s.marketing.example.org.sel_sign._local._bimi.isp.net TXT 'v=BIMI1;'

5.1.3. Public Key Revocation/Rotation

The MBP could determine that an older key needs to be retired. In this case the MBP could either remove the DNS record, or continue publishing without a valid public key attached:

```
sel_sign._local._bimi.isp.net TXT 'v=BIMI1;'
*.sel_sign._local._bimi.isp.net CNAME sel_sign._bimi.isp.net
```

For any MUA attempting to validate a signature, this action SHOULD fail. The MBP should rotate keys far ahead of removal of older keys so that recent messages are not disassociated with the imagery the MBP believes should be displayed.

An MUA SHOULD check for revocation daily or upon receipt of the first message for a domain. If the MUA does not intend to display the logo for a given message, it MAY NOT check for revocation. This may happen if the MUA only displays the logo when the message is opened (vs in the "list view").

6. Security Considerations

6.1. Threat Concerns

There are a number of concerns relating to how an independent MUA may use some of this information, or more important, how an attacker may attempt to cause an MUA to improperly display iconography for a user. This document is attempting to address these potential attacks.

6.1.1. Injection of Headers to An Unaware Mailbox Provider

An attacker could attempt to inject a message via normal SMTP methods, however, the message would contain headers that the MUA may believe were added by the receiving Mailbox Provider.

6.1.2. IMAP Append

An attacker could insert messages into a mail store via IMAP commands, and given a reasonable set of information points could induce an MUA to display a logo.

6.1.3. Signature Replay

6.1.4. Revocation

6.2. Key Separation

The key used to sign these BIMI headers MUST NOT be shared with another portion of the receiving platform.

6.3. Header Removal

Any MBP receiving these headers intact SHOULD remove these and perform their own evaluations.

NOTE: Ensure that core document specifies the same for BIMI-related headers

6.4. DNS/Key caching

Care should be taken not to cache public keys retrieved for an excessive amount of time. It's presumed that the MBP has a good reason to revoke the display of related imagery.

NOTE: Require MUA only retain data for TTL duration?

6.5. DNS Query Data

If the MUA queries DNS each time a message is loaded, it's conceivable that the DNS server owner could correlate some information about a user. It's not entirely clear if that data could be tied to a specific user, or what value this data may have.

7. Other Considerations

7.1. Multi-Domain MBP

There exist a large number of MBPs that accept mail for multiple domains. It could be that there is a primary domain with some side aliases, or a large hosting company. These types of entities may wish to explore using a DNAME to link the data between these various domains. One possible solution could be to do something such as:

_local._bimi.companyA.com DNAME _local._bimi.isp.net

This would allow for the same sharing of keys, as well as revocation information across the domains, while only managing one set of data.

8. Appendix A

For purposes below, sending is marketing.example.org, MBP is isp.net, and selector is sel_sign.

8.1. Normal Operational Steps

* ESP sends message to MBP containing appropriate headers for BIMI usage
* MBP performs DKIM/SPF/DMARC steps
* Presuming prior step works properly, MBP evaluates BIMI
* Based on localized requirements, MBP adds headers to email
  - BIMI-Location
  - BIMI-Indicator
* MBP additionally adds header specified in this document

    - BIMI-Receiver-Information
    - Includes time of receipt, sha256 of local rcpt, and the "@isp.net" portion
  * MBP signs all three headers using DKIM-style cryptography
    - Adds new header containing hash, as well as s/d attributes
  * ...
  * MBP stores message in platform
  * MUA retrieves message from message store
  * User opens message or MUA uses data during list view
  * MUA inspects looking for BIMI data
  * MUA sees signature
    - MUA verifies that the destination email address matches the signing domain
    - Looks for public keys at marketing.example.org.sel_sign._local._bimi.isp.net
    - Matches wildcard at *.sel_sign._local._bimi.isp.net
  * MUA validates signature
  * MUA displays BIMI logo as needed (list or message view)

8.2. Revoked Operational Steps

  * ESP sends message to MBP containing appropriate headers for BIMI usage
  * MBP performs DKIM/SPF/DMARC steps
  * Presuming prior step works properly, MBP evaluates BIMI
  * Based on localized requirements, MBP adds headers to email
    - BIMI-Location
    - BIMI-Indicator
  * MBP additionally adds header specified in this document
    - BIMI-Receiver-Information
    - Includes time of receipt, sha256 of local rcpt, and the "@isp.net" portion
  * MBP signs all three headers using DKIM-style cryptography
    - Adds new header containing hash, as well as s/d attributes
  * ...
  * MBP stores message in platform
  * MUA retrieves message from message store
  * User opens message or MUA uses data during list view
  * MUA inspects looking for BIMI data
  * MUA sees signature
    - MUA verifies that the destination email address matches the signing domain
    - Looks for public keys at selector.marketing.example.org.sel_sign._local._bimi.isp.net
    - MUA sees a value of "v=BIMI1;"
  * MUA does NOT display logos for this message (and the domain as a whole)

8.3. Sample headers

```
BIMI-Receiver-Signature: s=our_selector.marketing.example.org.sel_sig
n;d=isp.net;p=<signature_data> BIMI-Receiver-Information: date: Tue,
25 Oct 2022 15:14:12 +00:00 ; rcpt=d1bc8d3ba4afc7e109612cb73acbdddac0
52c93025aa1f82942edabb7deb82a1@isp.net BIMI-Location:
v=BIMI1;a=https://bimi.marketing.example.org/bimi/evidence.pem
(https://bimi.marketing.example.org/bimi/evidence.pem);
l=https://bimi.marketing.example.org/bimi/logo.svg
(https://bimi.marketing.example.org/bimi/logo.svg) BIMI-Indicator:
<base64_SVG_Data> Authentication-Results: spf=pass
marketing.marketing.example.org; dkim=pass (signature was verified)
header.d=marketing.example.org; dmarc=pass
header.from=marketing.example.org; bimi=pass
header.d=marketing.example.org header.selector=our_selector DKIM-
Signature: d=marketing.example.org;s=d_s;h=BIMI-
Selector:From:To:Date:Message-Id; bh=<hash_data>;b=<signature_data>
BIMI-Selector: v=BIMI1;s=our_selector
```

9. Contributors

10. Notes

11. TODO

* Cleanup notes
* Missing a number of references
* Enhance MUA Validation stub

12. References

13. Normative References

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

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/info/rfc6376>.

Author’s Address

Alex Brotman
Comcast, Inc
Email: alex_brotman@comcast.com