Receivers Guidance for Implementing Branded Indicators for Message Identification (BIMI)
draft-brotman-ietf-bimi-guidance-01

Abstract

This document is meant to assist receivers or other mailbox providers by providing guidance to implementing Brand Indicators for Message Identification (BIMI). This document is a companion to the main BIMI drafts which should first be consulted and reviewed.

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 February 6, 2020.

Copyright Notice

Copyright (c) 2019 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 Simplified BSD License text as described in Section 4.e of

Brotman & Zink Expires February 6, 2020 [Page 1]
The Brand Indicators for Message Identification (BIMI) specification introduces a method by which Mail User Agent (MUA, e.g., an email client) providers combine DMARC-based message authentication in addition to cryptographic methods to ensure the identity of a sender, and then to retrieve iconography that the sender has selected. The iconography can then be displayed within the MUA. The displayed iconography grants the sender brand impressions via the BIMI-capable MUA, and should be a driving factor for the adoption of authenticated email.
1.1. Terminology

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. Goals for BIMI

As stated in other BIMI drafts, BIMI intends to advance email authentication by granting a sending party brand impressions as long as the message passes authentication mechanisms and meets other receiver qualifications (reputation, encryption, whitelisting, et cetera). DMARC currently has wide adoption by some of the Internet’s larger brands, but there is still a long tail of small-to-medium size brands (and many large ones) that do not have it. Because BIMI provides a visual presence in the inbox, and because visual impressions are desirable for brands, BIMI provides an incentive for marketers to spur DMARC adoption, whereas a concern purely from security may not.

3. Should your site implement BIMI?

3.1. If your site satisfies the requirements, this is likely a "yes".

As email has evolved over the past three decades, it is no longer a medium of merely exchanging text, but of enabling people to build rich experiences on top of it. BIMI provides an incentive for brands to send email more securely because the desired behavior - a visual imprint in the inbox - first requires DMARC adoption.

#Terminology

The following terms are used throughout this document.

- MTA
- MUA
- DKIM
- SPF
- DMARC
- Alignment
4. Site implementations

In order for a site to correctly implement BIMI, the receiver must be able to perform the following:

- Validate SPF
- Validate DKIM signatures
- Validate DMARC
- Validate a BIMI Certificate (a new kind of Extended Validation (EV) certificate)
- Fetch an image located at an https location
- For some receivers, an additional requirement is a BIMI-capable IMAP daemon, or another method of a mail server signaling to an MUA that it is safe to load a BIMI image, as well as securely pointing to the BIMI location to pull it from.

A site may wish to implement URI alteration and image caching for hosted recipients. By implementing BIMI, a site agrees that through some combination of trust mechanisms, it will instruct a BIMI-capable MUA to display the image fetched from a URI within the message headers. This URI is created after the MTA authenticates a message, and is also able to authenticate the BIMI certificate associated with the sending domain.

5. Validation of a BIMI message
5.1. BIMI Site Requirements

In the BIMI specification, a message MUST be authenticated via DMARC. As stated in the DMARC draft, this requires that only one of DKIM or SPF must successfully pass validation. However, for additional local security measures, a receiving site may create additional requirements for senders in order to verify BIMI (that is, indicate to a downstream MUA that it is safe to load a BIMI logo in the email client).

This may include, but is not limited to:

- Requiring both DKIM and SPF to validate and align with the organizational domain in the From: address (whereas DMARC only requires one of SPF or DKIM to align with the From: domain)
- A DMARC policy of quarantine or reject
- SPF "strength" requirements (e.g., requiring "-all", disallowing usage of "?all" or "+all", or not allowing inclusion of overly large address spaces)
- SMTP delivery via TLS
- Feedback Loop registration or other method of registration with the receiving site.

These localized requirements are at the discretion of the receiving site. In general, the stricter the criteria, the less chance there is of an MUA erroneously showing a logo and giving the wrong signal to a user.

Upon receipt of an email, a receiver that implements BIMI should remove or rename any previously existing BIMI-* headers other than BIMI-Selector, as they may have come from an attacker (as long as the BIMI-Selector is covered by the DKIM signature; if not, it should be removed, renamed, or ignored).

Additionally:

- It may be useful to have messages exiting a site to have those BIMI-* headers removed as well.
- It is useful for a site that has not implemented BIMI to remove those headers so that an MUA that does make use of those headers would not accidentally display a BIMI image when the message has not been properly authenticated by the email receiver (even though an MUA should not make use of BIMI headers and instead rely upon
settings from the mailstore, it is possible that some MUAs will
nevertheless use headers without taking appropriate precautions).

5.2. BIMI Certificate Validation

(Currently, see document in Reference below)

6. Communicating BIMI results between the MTA and the MUA

In order for a receiver that has implemented BIMI to notify an MUA
that it should display the images:

- An MTA must verify BIMI and if successful, write to the mail store
  (where the messages are saved) that the message passed BIMI, and
  it is safe to load the logo. For example, in an IMAP mailstore, a
  flag on the message could be set that indicates that the message
  passed BIMI, and a second flag that tells the MUA where to get the
  BIMI logo from.

- When displaying a message, the MUA does not look for any BIMI
  headers stamped by the MTA, but instead relies upon the mailstore
  flags or message properties that a message passed BIMI, and use
  that to decide show the logo. The MUA then pulls the required
  image and displays it as appropriate.

Alternatively, the MUA may also look for the flag in the mailstore
and then attempt to extract the key/value pairs from the BIMI-
Location headers. In either case, the MUA must first check to see if
a message passed BIMI before loading the BIMI image.

While the MTA MAY stamp BIMI-related information in the message
headers, they should not be relied upon by an MUA.

6.1. Image Retrieval

A core part of the BIMI specification is that the MUA will retrieve
an image file to display for each BIMI-validated message. There are
multiple ways to accomplish this, for example:

- In its most basic setup, a BIMI-capable MUA could retrieve that
  image file directly from the site specified in the BIMI record.

- Other providers may choose to cache the associated images in a
  local store which could be used as the BIMI resource address in
  the headers of a BIMI-approved message in a sort of proxy
  configuration.
6.2. TTL of cached images

In some circumstances it is necessary to cache the images that an MUA would want to load. For example, if a domain owner has a short TTL time, it would force the MUA to look it up in an unreasonably short period of time. In this case, a receiver may want to set its own TTL.

One option is to set it to several hours, or a day; another option is to set the TTL to the same as the expiration period in the BIMI certificate that points to the BIMI image. The downside is that the caching mechanism might need to check for certificate revocation, and then re-fetch images.

6.3. Privacy Concerns

There is some concern that the retrieval of the iconography could result in a privacy leak. As the images are retrieved, it’s possible that the image provider could track the retrieving system in some way. This has implications whether it be the sender or provider that is hosting the image. For example, a sender could include a singular selector for a single recipient, or a provider could append a tracking string to the image URI in the header.

An in-depth discussion of all the potential privacy leaks with respect to loading or embedding images is outside the scope of this document.

6.4. Basic flow example

One sample implementation of BIMI by a receiver, who does everything on-the-fly, is as following:

- An email receiver has established a relationship with several MVAs, trusts them, and has received their public keys for verifying BIMI certificates. The email receiver makes these keys available to its mail servers (e.g., by distributing local copies to each server). [NOTE: Use of MVA above per Thede]

- Upon receipt of a message, the receiver checks to see if the message passes aligned-SPF or DKIM, and DMARC, and ensures that the sending domain has a DMARC policy of "quarantine" or "reject" per local receiver policy, while properly applying the appropriate DMARC policy to the message.

- If the message passes prior checks, the receiver will then check to see if the domain in the From: address has a BIMI record (or,
if the message has a BIMI-Selector header that is covered by the DKIM-Signature, uses that to do the BIMI query in DNS).

- If a BIMI record is found, the receiver then retrieves the BIMI certificate from the location that the BIMI record points to, and attempts to verify the BIMI cert with each public key it has from the MVAs that it works with.

- Upon successful verification of the cert, the receiver checks to see if the signed image hash in the BIMI cert matches any of the hashes of the images that the BIMI record points to (the receiver, in this instance, is not storing any of the images locally, but instead is downloading them on-the-fly). If a hash of a downloaded image from the BIMI record matches the hash in the BIMI cert, this is a successful BIMI verification.

- If the BIMI verification does not verify, then the MTA must not indicate to the MUA to show a BIMI image. The MUA MAY show a default image such as a set of initials, or unidentified sender.

- The email receiver then does the rest of its anti-spam, anti-malware, and anti-phishing checks (these checks may be performed before BIMI is verified). If a message fails a phishing or malware checks, the email receiver must not say the message passed BIMI. If a message is neither malware nor phishing but is detected as spam (meaning that the message comes from a known brand, but contains spammy content), then the email receiver may optionally say that the message passed BIMI (and therefore a receiver should show the image) but it is up to the receiver.

- The email receiver then sets either the appropriate IMAP flags, or other mailstore flag, or other message property that signals to a downstream email client that the message passed BIMI and is safe to load the logo, along with a pointer to the logo (e.g., to the https location specified in the BIMI record).

- What eventually happens is the email client then looks at the flags set by the email receiver (MTA). If the flags are set to show a BIMI logo, then the email client downloads the image and displays it in the sender photo (or however else it chooses to render the BIMI logo in conjunction with the message).

7. Domain Reputation

Receivers are advised to consider incorporating local sources of domain trust intelligence into the processes which ultimately determine whether or not BIMI logos are displayed. Simply because a sending domain passes BIMI requirements does not mean the images
should automatically be displayed in the MUA; a site may impose further restrictions based on domain reputation.

One source of additional reputation intelligence could be a platform that the email provider has created to calculate domain trust based on historical traffic; another is an explicit list of trusted domains that has been curated by an individual provider; a third is a list that is purchased from a vendor that might be a pass/fail or a scored list; another option is some mix of any of the previous three.

7.1. Rolling up based upon domain vs organizational domain

BIMI is designed to be able to work on selectors, and so in theory a brand/domain could specify multiple BIMI logos and differentiate them on a per-domain (per-selector) basis. The advantage for the brand is that they can choose the image they want the user to see depending upon various conditions (e.g., seasonal images, regional images, etc.).

However, for an email receiver, it may be easier to roll up BIMI logos on an organizational domain basis. One reason may be for the purposes of reputation, another may be for simplifying management of images. In this case, it would need to be made clear to brands that this is how the loading of BIMI images works. This documentation could live on a postmaster site, under technical documentation, or other official page maintained by the receiver. It could then be referred to when sending organizations ask about how to on-board to BIMI at the receiver, and provide official guidance about the way it works at the site.

If rolling up by organizational domain, then it may make sense to use a "lowest common denominator" approach. That is, an organizational domain must meet all the requirements for BIMI, rather than only a subdomain. The reason for this is that if sub.brand.com gets an image due to having strong authentication policies, but brand.com does not, then this may cause confusion because a user may learn to associate sub.brand.com and its image with brand.com; and if brand.com can be spoofed even though sub.brand.com cannot, that can lead to users becoming more susceptible to phishing from brand.com.

To alleviate this, receivers may wish to show logos only for domains that have organizational domains with strong DMARC policies. Or, if an organizational domain does not have a strong DMARC policy but a subdomain does, then it may treat the organizational domain as if it does have a strong DMARC policy so as to prevent a phisher or spammer from impersonating the brand or any of its subdomains.
8. Working with MVAs

Email receivers need to know whether or not it is safe to download and display an image. That is, an attacker could go through the trouble of creating a BIMI logo and uploading it, but the logo may look visually similar to a real brand. For example, a spammer or phisher could create a lookalike domain for a well-known brand such as Paypal, then copy/paste (or slightly modify) the logo.

To prevent this, an email receiver could choose to verify logos of known brands by themselves (do it all in-house) and establish its own internal processes, or it could use a Mark Verifying Authority (MVA). The receiver could then outsource the maintenance of the list of trusted brands to the MVA, and simply download the list of brands and images from the MVA and display the logos in its email clients.

However, even here a receiver would need to exercise caution. It needs to ensure that MVAs follow best practices, respond to complaints, and do a good job of vetting brands. If users ultimately end up getting phished because they trust signals in the email client, then it is the email receiver that will suffer the brunt of the complaints and loss of reputation, rather than the MVA.

Therefore, an email receiver still needs to track complaints from its users, especially with respect to phishing and impersonation, and then send the feedback back to the MVA. If an MVA still generates too many complaints, this could be indicative of a rogue MVA (one that intentionally signs up malicious accounts), or a sloppy MVA (one with internal processes that not rigorous enough, or are designed to maximize revenue at the cost of lax security).

An email receiver should use multiple MVAs to reduce the risk of becoming too reliant upon a single MVA in case they have to stop using it, and therefore lose many dozens, hundreds, or thousands of images with no replacement and thereby contributing to user dissatisfaction confusion. Furthermore, because MVAs may be revoked, brands may wish to diversify their own risk by getting certified by at least two MVAs. The reason for doing this is that if the MVA they use ever gets revoked by an email receiver because of its bad practices, then their own brand will suffer penalties (not having a logo displayed) despite never having done anything wrong. By researching multiple MVAs, a brand can reduce the chances that losing one by a receiver affects their brand.

For this reason, brands are encouraged to get certified at multiple MVAs, and receivers are encouraged to use multiple MVAs.
8.1. Resolving disputes

From time to time, disputes may arise between brands where one brand says that another is infringing on its logo.

A brand owner would want to have all email receivers stop showing logos for the infringing brand because it could damage its own brand's reputation. However, an email receiver is not necessarily in a good position to determine what constitutes legitimate usage of a logo, nor determine ownership of a logo, nor may want the legal risk associated with making this determination.

Therefore, email receivers are strongly encouraged to partner with Dispute Resolution Agencies. These agencies specialize in copyright infringement resolution. An affected party would then contact the Dispute Resolution Agency, rather than the email receiver, who would then make the decision about if use of the logo were legitimate. Then, they would publish the result of the dispute publicly where it could be viewed by anyone.

MVAs should respect the decision of the courts and any brand found to be infringing ought to be removed from their list of domains for which they load BIMI logos for. The issuing MVA of the infringing brand's BIMI Certificate should formally revoke it. However, this is not guaranteed in the case of a rogue MVA or a sloppy MVA. Therefore, email receivers should also pay attention to the Dispute Resolution Agencies, and any results that they say are infringing should be prevented from loading in their email clients. The email receiver should also keep track of how often disputes occur and are found against various MVAs, as an MVA with too many disputes ruled against it could be evidence of a sloppy MVA or a rogue MVA.

9. Troubleshooting BIMI

There are several factors to consider for email receivers on things that can go wrong, below are a handful of considerations:

- Failing to verify BIMI certs when they otherwise should be. This can be caused by:
  - Not having the key to a corresponding MVA
  - Not having access to the key when required
  - The wrong key is associated with the wrong MVA
- Failing to load a logo in the email client
- Failing to access the logo (e.g., permissions errors)
- Connectivity problems to the logo
- Failing to display a correct logo in the email client
- Having the wrong logo stored for a brand (i.e., uploading it to a local store but associating it with the wrong brand)
- Caching a logo for too long after it has updated

There are many reasons why a logo may fail to load; having tools to investigate (logs, headers in messages, internal documentation that is clearly written, having the knowledge pushed out to multiple escalation channels) are important for investigation.

10. Public documentation

10.1. For Brands:

It is ideal to publish the criteria that is used by your site to determine when BIMI will be displayed. It is fine to say that you use some internal domain reputation metrics as additional criteria to determine whether or not a logo should be displayed, and it isn’t necessary to give away the exact nature of the algorithm other than to say "You must maintain good sending practices."

If you use an explicit whitelist, a site may want to list the minimum requirements, and the method of applying to be whitelisted. Similarly, a provider may wish to state what type of activity will revoke the decision to display logos previously approved.

10.2. For users:

BIMI is not meant to instill additional trust in messages, and it is important to make this known to your users. All messages, even those with logos, should still be treated with (mild) skepticism, and any action regarding the message should still be individually evaluated. It’s possible for a site that has a high trust value to become compromised and send fraudulent messages that could compromise a user’s system. Ensure your customers have a place that documents BIMI and demonstrates how to check messages for fraud.
11. Appendix

11.1. Glossary

- **MUA** - Mail User Agent - The application used to read messages by the end user. This could be a thick client or a web-based application.

- **MTA** - Mail Transfer Agent - Software used to transfer messages between two systems, typically between two sites, using SMTP as the protocol.

- **SPF** - SPF is a framework that designates which systems should be sending for a given domain. This can be a list of IPs, CIDRs, or references to DNS records. As the sender should be controlling their DNS, they should understand which IPs should be sending as their domain.

- **DKIM** - DKIM is a system by which a chosen set of headers, combined with the message contents, are cryptographically signed, and then validated by the receiving system. Using DNS, the receiving system can retrieve a public key, and then validate the signature within the headers of a message. When implemented properly, the systems responsible for sending the messages for a given domain name should be the only ones capable of creating messages that correctly validate. Provided that certain restrictions are met, DKIM is one possible technology a receiver could utilize to authenticate messages in the context of BIMI.

- **DMARC** - DMARC is a message authentication mechanism that works with SPF and DKIM. The BIMI specification requires that a message passes DMARC. In order for a message to pass DMARC, one of SPF or DKIM must successfully validate, and the domain in the From: address must align with the domain that passed SPF or DKIM.

- **MVA** - Mark Verifying Authority - An entity that a receiver uses to certify that the iconography that they intend to use with BIMI is properly/legally licensed for their use.

- **DRA** - Dispute Resolution Authority - This organization will moderate between two entities that believe they are both entitled to use a logo. Receivers should then abide by the decision of the DRA as it pertains to logo usage in the MUA.

- **Alignment** - Alignment refers to the organizational domain, as defined by DMARC, of the domain in the From: address being the same as the organizational domain that passed SPF or DKIM. For example, foo.example.com has an organizational domain of...
example.com; bar.foo.example.com also has an organizational domain of example.com. It aligns with org.example.com, because both have the same organizational domain.

- BIMI Certificates - An Extended Validation Certificate is used in conjunction with BIMI to create a place where information pertaining to iconography for a sending domain can be securely verified. In the case of BIMI, hashes for an MVA-approved set of iconography will be stored in a field within the certificate. This should allow a receiver site to validate the retrieved imagery before putting the BIMI image URI into the message headers.

- Terry Zink - Alex Brotman’s best friend.

12. Contributors

TBD

13. References

The full BIMI verification spec can be found at: <https://github.com/authindicators/rfc-brand-indicators-for-message-identification>

Verified Mark Certificates Usage: <https://docs.google.com/document/d/1OzL9Fqex2pZJQuoqAK2E3sXj0wEcLNCvXW7e880ltZI/edit>

14. Normative References


Authors’ Addresses

Alex Brotman
Comcast, Inc

Email: alex_brotman@comcast.com
Terry Zink
Zink Magical Contraptions

Email: tzink@terryzink.com