Network Working Group
Internet-Draft
Intended status: Experimental
Expires: August 10, 2019

S. Blank
P. Goldstein
Valimail
T. Loder, Ed.
Skye Logicworks
T. Zink, Ed.
February 06, 2019

Brand Indicators for Message Identification (BIMI) draft-blank-ietf-bimi-00

Abstract

Brand Indicators for Message Identification (BIMI) permits Domain Owners to coordinate with Mail User Agents (MUAs) to display brand-specific Indicators next to properly authenticated messages. There are two aspects of BIMI coordination: a scalable mechanism for Domain Owners to publish their desired indicators, and a mechanism for Mail Transfer Agents (MTAs) to verify the authenticity of the indicator. This document specifies how Domain Owners communicate their desired indicators through the BIMI assertion record in DNS and how that record is to be handled by MTAs and MUAs. The domain verification mechanism and extensions for other mail protocols (IMAP, etc.) are specified in separate documents. MUAs and mail-receiving organizations are free to define their own policies for indicator display that makes use or not of BIMI data as they see fit.

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 August 10, 2019.

Copyright Notice

Table of Contents

1. Introduction

This document defines Brand Indicators for Message Identification (BIMI), which permits Domain Owners to coordinate with Mail User Agents (MUAs) to display brand-specific Indicators next to properly authenticated messages.

BIMI is an open system that works at internet scale, so that Domain Owners can coordinate with MUAs to display appropriate Indicators. BIMI has the added benefit of incentivizing Domain Owners to authenticate their email.

The approach taken by BIMI is heavily influenced by the approach taken in DKIM [1], in that BIMI:

- has no dependency on the deployment of any new Internet protocols or services for indicator registration or revocation;
- makes no attempt to include encryption as part of the mechanism;
- is compatible with the existing email infrastructure and transparent to the fullest extent possible;
- requires minimal new infrastructure;
- can be implemented independently of clients in order to reduce deployment time;
- can be deployed incrementally; and
- allows delegation of indicator hosting to third parties.

This document covers the BIMI mechanism for Domain Owners to publish their desired indicators and how Mail Transfer Agents (MTAs) and MUAs should handle this communication. This document does not cover how domains or indicators are verified, how MUAs should display the indicators, or how other protocols (i.e. IMAP, JMAP) should be extended to work with BIMI. Other documents will cover these topics.

2. Overview

The Sender Policy Framework ([SPF]), DomainKeys Identified Mail ([DKIM]), and Domain-based Message Authentication, Reporting, and Conformance ([DMARC]) provide mechanisms for domain-level authentication for email messages. They enable cooperating email senders and receivers to distinguish messages that are authorized to use the domain name from those that are not. BIMI relies on these authentication protocols, but is not a new authentication protocol itself.

MUAs are increasingly incorporating graphical logos to indicate the identity of the sender of a message. While a discussion of the merits of doing this are beyond the scope of this document, at present there are no open standards for publishing and discovery of

preferred logos or of tying these usages only to properly authenticated messages.

Because of this need for brand specific indicators, some mail-receiving organizations have developed closed systems for obtaining and displaying brand indicators for some select domains. While this enabled these mail-receiving organizations to display brand indicators for a limited subset of messages, this closed approach has significant downsides:

1. It puts a significant burden on each mail-receiving organization, because they must identify and manage a large database of brand indicators.

2. Scalability is challenging for closed systems that attempt to capture and maintain complete sets of data across the whole of the Internet.

3. A lack of uniformity across different mail-receiving organizations - each organization will have its own indicator set, which may or may not agree with those maintained by other organizations for any given domain.

4. Domain Owners have limited ability to influence the brand indicator for the domain(s) they own, and such ability they do have is likely to require coordination with many mail-receiving organizations.

5. Many Domain Owners have no ability to participate whatsoever as they do not have the appropriate relationships to coordinate with mail-receiving organizations.

6. MUAs that are not associated with a particular mail-receiving organization are likely to be disadvantaged, because they are unlikely to receive indicators in a manner optimized for their user interfaces.

This all speaks to the need for a standardized mechanism by which Domain Owners interested in ensuring that their indicators are displayed correctly and appropriately can publish and distribute brand indicators for use by any participating MUA.

BIMI removes the substantial burden of curating and maintaining an indicator database from the MUAs, and allows each domain to manage its own indicators. As an additional benefit, mail-originating organizations are more likely to invest the time and effort to authenticate their email, should that come with the ability to influence how email from the organization is displayed.

The basic structure of BIMI is as follows:

1. Domain Owners publish brand indicator assertions for domains via the [DNS].

2. Then, for any message received by a Mail Receiver:

   a. Receivers authenticate the messages using [DMARC] and whatever other authentication mechanisms they wish to apply.

   b. The receiver queries the DNS for a corresponding BIMI record and proof of indicator validation.

   c. If both the email and the logo authenticate, then the receiver adds a header to the message, which can be used by the MUA to determine the Domain Owner's preferred brand indicator.

3. The MUA retrieves and displays the brand indicator as appropriate based on its policy and user interface.

The purpose of this structure is to reduce operational complexity at each step and to consolidate validation and indicator selection into the MTA, so that Domain Owners only need to publish simple rules and MUAs only need simple display logic.

3. Requirements

Specification of BIMI in this document is guided by the following high-level goals, security dependencies, detailed requirements, and items that are documented as out of scope.

3.1. High-Level Goals

BIMI has the following high-level goals:

- Allow Domain Owners to suggest appropriate indicators for display with authenticated messages originating from their domains.

- Enable the authors of MUAs to display meaningful indicators associated with the Domain Owner to recipients of authenticated email.

- Provide mechanisms to prevent attempts by malicious Domain Owners to fraudulently represent messages from their domains as originating with other entities.

- Work at Internet Scale.

3.2. Security

Brand indicators are a potential vector for abuse. BIMI creates a relationship between sending organization and Mail Receiver so that the receiver can display appropriately designated indicators if the sending domain is verified and has meaningful reputation with the receiver. Without verification and reputation, there is no way to prevent a bad actor exxample.com from using example.com's brand indicators and behaving maliciously. This document does not cover these verification and reputation mechanisms, but BIMI requires them to control abuse.

3.3. Out of Scope

Several topics and issues are specifically out of scope for the initial version of this work. These include the following:

- Publishing policy other than via the DNS.
- Specific requirements for indicator display on MUAs.
- The explicit mechanisms used by Verifying Protocol Clients - this will be deferred to a later document.

4. 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", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [KEYWORDS].

Readers are encouraged to be familiar with the contents of [EMAIL-ARCH]. In particular, that document defines various roles in the messaging infrastructure that can appear the same or separate in various contexts. For example, a Domain Owner could, via the messaging mechanisms on which BIMI is based, delegate control over defining preferred brand indicators as the Domain Owner to a third party with another role. This document does not address the distinctions among such roles; the reader is encouraged to become familiar with that material before continuing.

Syntax descriptions use Augmented BNF [ABNF].

"Author Domain", "Domain Owner", "Organizational Domain", and "Mail Receiver" are imported from [DMARC] Section 3.

4.1. BIMI Assertion

The mechanism through which a Protocol Client verifies the BIMI Assertion Record and constructs the URI(s) to the requested indicator(s) to be placed in the BIMI-Location header.

4.2. Indicator

The icon, image, mark, or other graphical representation of the brand. The Indicator is in a common image format with restrictions detailed in the Assertion Record definition (Section 5.1).

4.3. Mark Verifying Authority (MVA)

An entity of organization that can provide evidence of verification of indicators asserted by a Domain Owner to Verifying Protocol Clients. The MVA may choose to uphold and confirm the meeting of certain indicator standards (ie. size, trademark, content, etc).

4.4. Mark Verified Certificate (MVC)

A certificate issued by a CA which has validated the attested logo in accordance with Validated Mark Certificate Guidelines, which are defined in a separate document.

4.5. Protocol Client

An entity that uses the BIMI protocol to discover and fetch published indicators.

4.6. Verifying Protocol Client

A Protocol Client that uses the optional verification capability to inquire about the verification status of published indicators.

5. BIMI DNS Records

BIMI policies are published by Domain Owners and applied by Protocol Clients.

A Domain Owner advertises BIMI participation of one or more of its domains by adding a DNS TXT record to those domains. In doing so, Domain Owners make specific requests of MUAs regarding the preferred set of indicators to be displayed with messages purporting to be from one of the Domain Owner's domains.

A Domain Owner may choose not to participate in BIMI. In this case, the Domain Owner simply declines to advertise participation by not publishing any BIMI assertion record.

An MUA implementing the BIMI mechanism SHOULD make a best-effort attempt to adhere to the Domain Owner's published BIMI policy. However, MUAs have final control over the user interface published to their end users, and MAY use alternate indicators than those specified in the BIMI assertion record or no indicator at all.

BIMI's use of the DNS is driven by BIMI's use of domain names and the nature of the query it performs. Use of the DNS as the query service has the benefit of reusing an extremely well-established operations, administration, and management infrastructure, rather than creating a new one.

BIMI's policy payload is intentionally only published via a DNS record and not an email header. This serves four purposes:

1. There is one and only one mechanism for both simple and complex policies to be published.

2. Operational complexity is reduced, and MTAs only need to check a single record in a consistent manner to enforce policy.

3. MTAs that understand their MUAs have more control over which Indicators they choose for those MUAs.

4. Indicators can be verified and/or cached in advance, so that malicious headers cannot be used as an attack vector.

Per [DNS], a TXT record can comprise several "character-string" objects. BIMI TXT records with multiple strings must be treated in an identical manner to SPF Section 3.3 [2].

5.1. Assertion Record

All Domain Owner BIMI preferences are stored as DNS TXT records in subdomains named "_bimi". BIMI allows the definition of multiple preferences associated with a single RFC5322.From domain. To distinguish between these different preferences, BIMI uses Section 5.2. Senders advertise which selector to use by specifying it in a BIMI-Selector header (Section 6.1).

For example, the Domain Owner of "example.com" would post BIMI preferences in a TXT record at "default._bimi.example.com". Similarly, a Mail Receiver wishing to query for BIMI preferences regarding mail with an RFC5322.From Author Domain of "example.com"

and a selector "default" would issue a TXT query to the DNS for the subdomain of "default._bimi.example.com". The DNS-located BIMI preference data will hereafter be called the "BIMI Assertion Record" or "Assertion Record".

Assertion Records are defined precisely, mail receivers MUST NOT attempt to fix syntactical or capitalization errors. If a required tag is missing, it is an error.

BIMI Assertion Records follow the extensible "tag-value" syntax for DNS-based key records defined in [DKIM].

This section creates a registry for known BIMI tags and registers the initial set defined in this document. Only tags defined in this document or in later extensions, and thus added to that registry, are to be processed; unknown tags MUST be ignored.

The following tags are introduced as the initial valid BIMI tags:

v= Version (plain-text; REQUIRED). Identifies the record retrieved as a BIMI record. It MUST have the value of "BIMI1" for implementations compliant with this version of BIMI. The value of this tag MUST match precisely; if it does not or it is absent, the entire retrieved record MUST be ignored. It MUST be the first tag in the list.

ABNF:

bimi-version = %x76 *WSP "=" *WSP %x42.49.4d.49 1DIGIT

a= Trust Authorities (plain-text; URI; OPTIONAL). A reserved value.

ABNF:

bimi-authorities = %x61 *WSP "=" \[bimi-location-uri\]

NOTE TO WORKING GROUP: This a= tag needs to be extended, to provide validation options. Current expectations are: "self", "cert", and "mva". Where "self" means there is no validation option (perhaps this is best done by simply not supplying an a= tag?), "cert" provides an HTTPS URL to a Mark Verified Certificate that can be used to validate the indicator at the l= tag, and "mva" specifies an HTTPS URL to an API endpoint that can be queried for validation information.

l= locations (URI; REQUIRED). The value of this tag is a comma separated list of base URLs representing the location of the brand indicator files. All clients MUST support use of at least 2 location URIs, used in order. Clients MAY support more locations. The supported transport is HTTPS only.

ABNF:

```
bimi-location-uri = \[FWS\] URI \[FWS\]

; "URI" is imported from [URI]
; HTTPS only
; commas (ASCII ; 0x2C) MUST be encoded

bimi-locations = %x6c *WSP "=" bimi-location-uri *("," bimi-location-uri) \
["\]
```

Therefore, the formal definition of the BIMI Assertion Record, using [ABNF], is as follows:

```
bimi-sep = *WSP %x3b *WSP

bimi-record = bimi-version (bimi-sep bimi-locations) (bimi-sep bimi-
authorities) \[bimi-sep\]

; components other than bimi-version may appear in any order
```

5.1.1. Declination to publish

If both the "l" and "a" tags are empty, it is an explicit refusal to participate in BIMI. This is critically different than not publishing a BIMI record in the first place. For example, this allows a subdomain to decline participation when its organizational domain has default Indicators available. Furthermore, messages sent using a selector that has declined to publish will not show an Indicator while messages with other selectors would display normally.

An explicit declination to publish looks like:

```
v=BIMI1; l=; a=;
```

5.1.2. Supported Image Formats for l= tag

Any format in the BIMI-formats IANA registry are acceptable targets for the l= tag. If an l= tag ends with any other image format, the record MUST be treated as if it has a permanent error.

As of the publishing of this document, only SVG as defined in (RFC6170 section 5.2)[https://tools.ietf.org/html/rfc6170#section-5.2] is acceptable for publishing in the l= tag.

5.2. Selectors

To support multiple brand indicators per domain, the brand indicator namespace is subdivided for the publishing of multiple Assertion

Records using "selectors". Selectors allow the Domain Owner to

better target the brand indicator by type of recipient, message source, or other considerations like seasonal branding. BIMI selectors are modeled after DKIM selectors [3].

The selector "default" is the default Assertion Record. Domain Owners can specify which other selector to use on a per-message basis by utilizing the BIMI-Selector Header (Section 6.1).

Periods are allowed in selectors and are component separators. When BIMI Assertion Records are retrieved from the DNS, periods in selectors define DNS label boundaries in a manner similar to the conventional use in domain names. In a DNS implementation, this can be used to allow delegation of a portion of the selector namespace.

ABNF:

```
selector = sub-domain *( "." sub-domain )

; from [SMTP] Domain,

; excluding address-literal
```

The number of selectors for each domain is determined by the Domain Owner. Many Domain Owners will be satisfied with just one selector, whereas organizations with more complex branding requirements can choose to manage disparate selectors. BIMI sets no maximum limit on the number of selectors.

6. BIMI Header Fields

Once BIMI policies are published in DNS via Assertion Records, additional guidance can be provided from Domain Owners to Mail Receivers, and Mail Receivers to their MUAs through the use of additional BIMI header fields.

BIMI header fields are case insensitive. If a required tag is missing, it is an error.

6.1. BIMI-Selector

BIMI DNS records are placed in <selector>._bimi.<domain>, and by default they are placed in default._bimi.<domain>. That is, for example.com, the default location for all BIMI lookups is default._bimi.example.com. However, a Domain Owner may specify the selector using the RFC 5322 header 'BIMI-Selector'. The BIMI-Selector header consists of key value pairs:

v= Version (plain-text; REQUIRED). The version of BIMI. It MUST have the value of "BIMI1" for implementations compliant with this version of BIMI. The value of this tag MUST match precisely; if it does not or it is absent, the entire retrieved record MUST be ignored. It MUST be the first tag in the list.

ABNF:

bimi-header-version = "v" *WSP "=" *WSP "BIMI" 1DIGIT

s= Selector (plain-text; REQUIRED). The location of the BIMI DNS record, when combined with the RFC5322.From domain.

ABNF:

bimi-selector = "s" *WSP "=" *WSP selector

And the formal definition of the BIMI Selector Header, using ABNF, is as follows:

bimi-selector-header = bimi-header-version bimi-sep bimi-selector \[bimi-sep\]

6.2. BIMI-Location

BIMI-Location is the header a Mail Receiver inserts that tells the MUA where to get the BIMI indicator from.

The syntax of the header is as following:

v= Version (plain-text; REQUIRED). The version of BIMI. It MUST have the value of "BIMI1" for implementations compliant with this version of BIMI. The value of this tag MUST match precisely; if it does not or it is absent, the entire retrieved record MUST be ignored. It MUST be the first tag in the list.

The ABNF for bimi-header-version is imported exactly from the [BIMI Selector Header](#bimi-selector).

l: location of the BIMI indicator (URI; REQUIRED). Inserted by the MTA after parsing through the BIMI DNS record and performing the required checks. The value of this tag is a comma separated list of URLs representing the location of the brand indicator files. All clients MUST support use of at least 2 location URIs, used in order. Clients MAY support more locations. Initially the supported transport supported is HTTPS only.

ABNF:

bimi-header-locations = "l" *WSP "=" bimi-location-uri *("," bimi-location-uri)

\[","\]

And the formal definition of the BIMI Location Header, using ABNF, is as follows:

```
bimi-location-header = bimi-header-version bimi-sep bimi-header-locations \
[bimi-sep\]
```

6.3. Header Signing

The BIMI-Selector SHOULD be signed by DKIM.

The BIMI-Location header MUST NOT be DKIM signed. This header is untrusted by definition, and is only for use between an MTA and its MUAs, after DKIM has been validated by the MTA. Therefore, signing this header is meaningless, and any messages with it signed are either coming from malicious or misconfigured third parties.

7. Domain Owner Actions

This section includes a walk through of the actions a Domain Owner takes when setting up Assertion Records and sending email messages.

7.1. Determine and publish Indicator(s) for use

Domain Owners should consider which Indicator file formats to choose when setting up their BIMI Assertion Records. As a Sender, BIMI provides control over which Indicators are chosen for display, but not the ultimate manner in which the MUA will display the image.

BIMI allows multiple comma separated l= values in the Assertion Record, so that a Domain Owner may publish the same Indicators in multiple world readable locations. This is so Indicators may still be available if there are service or DNS issues for a particular l= value.

7.2. Specify Domain Owner Preference

The ordering of the l= tag is significant, the first location specified should have priority over the second, etc.

This does not guarantee that the first tags specified will be selected as there may be DNS errors, or some clients may not support all formats. However, on average, the first tags specified SHOULD be used to construct the indicator passed to the MUA.

7.3. Publish Assertion Records

For each set of Indicators and domains, publish the appropriate Assertion Record as either "default" or a named selector as a DNS TXT record within the appropriate "_bimi" namespace.

7.4. Manage multiple uses of the same Indicator(s) within a trust boundary

For Domain Owners with multiple domains that wish to share the same set of Indicators within a trust boundary and only manage those Indicators from a single DNS location, it is RECOMMENDED to use DNS CNAMEs.

Using a CNAME here is functionally similar to the SPF redirect modifier. Since BIMI does not require l= tags to be aligned to the Author Domain, CNAMEs present a cleaner solution than extending the protocol.

7.5. Set the headers on outgoing email as appropriate

Once a default Assertion Record has been published for an Author Domain, all emails from this domain should display the appropriate Indicator in participating MUAs.

If a non-default Indicator is desired, the BIMI-Selector header should be set appropriately. If for some reason this selector cannot be accessed by the Protocol Client, the fallback is the default Assertion Record on the Organization domain.

The BIMI-Location header MUST NOT be set by email senders, and Protocol Clients MUST ignore it.

8. Receiver Actions

This section includes a walk through of the actions a Protocol Client takes when evaluating an email message for BIMI Assertion.

8.1. Indicator Discovery

Through the BIMI Assertion Record (Section 5.1), the BIMI mechanism uses DNS TXT records to advertise preferences. Preference discovery is accomplished via a method similar to the method used for [DMARC] records. This method, and the important differences between BIMI and [DMARC] mechanisms, are discussed below.

Indicator Discovery MUST only be attempted if the message authenticates per Receiver policy.

To balance the conflicting requirements of supporting wildcarding, allowing subdomain policy overrides, and limiting DNS query load, Protocol Clients MUST employ the following lookup scheme for the appropriate BIMI record for the message:

1. Start with the DNS domain found in the RFC5322.From header in the message. Define this DNS domain as the Author Domain.

2. If the message for which the indicator is being determined specifies a selector value in the BIMI Selector Header (Section 6.1), use this value for the selector. Otherwise the value 'default' MUST be used for the selector.

3. Clients MUST query the DNS for a BIMI TXT record at the DNS domain constructed by concatenating the selector, the string '_bimi', and the Author Domain. A possibly empty set of records is returned.

4. Records that do not start with a "v=" tag that identifies the current version of BIMI MUST be discarded.

5. If the set is now empty, the Client MUST query the DNS for a BIMI TXT record at the DNS domain constructed by concatenating the selector 'default', the string '_bimi', and the Organizational Domain (as defined in [DMARC]) corresponding to the Author Domain. A custom selector that does not exist falls back to default._bimi.<organizationalDomain>, and NOT <selector>._bimi.<organizationalDomain>. A possibly empty set of records is returned.

6. Records that do not start with a "v=" tag that identifies the current version of BIMI MUST be discarded.

7. If the remaining set contains multiple records or no records, indicator discovery terminates and BIMI processing MUST NOT be performed for this message.

8. If the remaining set contains only a single record, this record is used for BIMI Assertion.

8.2. Indicator Validation

If an Assertion Record is found and has an a= tag, it must be used to validate the indicator using the following algorithm:

1. Use the mechanism in the a= tag to retrieve the validated hash.

2. Compute the hash of the logo in the l= tag.

3. If the hash of the logo does not match the validated hash, then logo validation has failed and then indicator MUST NOT be displayed.

4. If the hashes match, and the validated hash is from a trusted source, then the indicator can be displayed per receiver policy.

8.3. Affix BIMI status to Authentication Results header field

Upon completion of Indicator Discovery, an MTA SHOULD affix the result in the Authentication-Results header using the following syntax, with the following key=value pairs:

bimi: Result of the bimi lookup (plain-text; REQUIRED). Range of values are 'pass' (BIMI successfully validated), 'none' (no BIMI record present), 'fail' (syntax error in the BIMI record, or some other error), 'temperror' (DNS lookup problem), or 'skipped' (BIMI check did not perform, possibly because the message did not comply with the minimum requirements such as passing DMARC, or the MTA does not trust the sending domain). The MTA MAY put comments in parentheses after bimi result, e.g., "bimi=skipped (sender not trusted)" or "bimi=skipped (message failed DMARC)".

header.d: Domain used in a successful BIMI lookup (plain-text; REQUIRED if bimi=pass). If the first lookup fails for whatever reason, and the second one passes (e.g., using the organizational domain), the organizational domain should appear here. If both fail (or have no record), then the first domain appears here.

selector: Selector used in a successful BIMI lookup (plain-text; REQUIRED if bimi=pass). Range of values include the value in the BIMI-Selector header, and 'default'. If the first lookup fails (or has no record) and second passes, the second selector should appear here. If both fail (or have no record), then the first selector should appear here.

8.4. Handle Existing BIMI-Location Headers

Regardless of success of the BIMI lookup, if the BIMI-Location header already exists it MUST be either removed or renamed.

This is because the MTA doing BIMI Assertion is the only entity allowed to specify the BIMI-Location header, and allowing any existing header through is a security risk.

Additionally, at this point, if the original email message had a DKIM signature, it has already been evaluated. Removing the header at this point should not break DKIM, especially because this header should not be signed per this spec.

8.5. Construct BIMI-Location URI(s)

The l= value of the BIMI-Location header is a comma separated list of URIs to Indicators the MTA believes are most applicable to its MUAs. From the options provided by the Assertion Record, MTAs SHOULD choose the Indicators to include based on Receiver policy for optimal performance and user experience for its MUAs from the.

MTAs MAY add as many comma separated URIs to the l= tag in the BIMI-Location header as they wish, MUAs MUST support at least 2 location URIs in the header, and MAY support more.

8.6. Set appropriate flags on the mail store

Once an MTA has finished BIMI Assertion, it needs to deposit the email somewhere where the user can eventually access it with an MUA. Users typically access their email on mail stores through either POP3, IMAP, and MAPI. Separate documents will define protocol-specific BIMI extensions for mail stores.

If a mail store is BIMI-compliant, the MTA SHOULD set a flag on the message when depositing in the mail store. This is to communicate between the MTA and its MUA that the BIMI-Location header was set locally and can be trusted.

If an MUA has a BIMI-compliant mail store, and no appropriate flag is set, the MUA SHOULD ignore the BIMI-Location header.

If a mail store ingests a message from another mail store through some other means, the ingesting mail store may or may not set the protocol-specific BIMI flag when it pulls down the relayed message. If it trusts the other mail store, it may simply set the same flag. Or, it may perform BIMI Assertion from scratch, create or replace the BIMI-Location header, and set its own flag appropriately. Or, it may simply choose not to set the flag at all.

9. Security Considerations

The consistent use of brand indicators is valuable for Domain Owners, Mail Receivers, and End Users. However, this also creates room for abuse, especially for determined malicious actors.

9.1. Lookalike Domains and Copycat Indicators

Publishing BIMI records is not sufficient for an MTA to signal to the MUA to load the BIMI indicator. Instead, the Domain Owner should have a good reputation with the MTA. Thus, BIMI display requires passing BIMI, and passing email authentication checks, and having a

good reputation at the receiver. The receiver may use a manually maintained list of large brands, or it may import a list from a third party of good domains, or it may apply its own reputation heuristics before deciding whether or not to load the BIMI indicator.

9.2. Large files and buffer overflows

The MTA or MUA should perform some basic analysis and avoid loading indicators that are too large or too small. The Receiver may choose to maintain a manual list and do the inspection of its list offline so it doesn't have to do it at time-of-scan.

9.3. Slow DNS queries

All email Receivers already have to query for DNS records, and all of them have built-in timeouts when performing DNS queries. Furthermore, the use of caching when loading images can help cut down on load time. Virtually all email clients have some sort of image-downloading built-in and make decisions when to load or not load images.

9.4. Unaligned indicators and asserting domains

There is no guarantee that a group responsible for managing brand indicators will have access to put these indicators directly in any specific location of a domain, and requiring that indicators live on the asserted domain is too high a bar. Additionally, letting a brand have indicator locations outside its domain may be desirable so that someone sending legitimate authenticated email on the Domain Owner's behalf can manage and set selectors as an authorized third party without requiring access to the Domain Owner's DNS or web services.

9.5. Unsigned BIMI-Selector Header

If a Domain Owner relies on SPF but not DKIM for email authentication, then adding a requirement of DKIM may create too high of a bar for that sender. On the other hand, Receivers doing BIMI assertion may factor in the lack of DKIM signing when deciding whether to add a BIMI-Location header.

9.6. CGI scripts in Indicator payload

MTAs and MVAs should aggressively police Indicators to ensure they are the Indicators they claim to be, are within appropriate size limits, and pass other sanity checks. Additionally, MTAs might cache good Indicators and serve them directly to their MUAs, which would in practice bypass any malicious dynamic payload set to trigger against an end user but not an MTA.

9.7. Metadata in Indicators

Domain Owners should be careful to strip any metadata out of published Indicators that they don't want to expose or which might bloat file size. MTAs and MVAs might wish to inspect and remove such data from Indicators before exposing them to end users.

10. IANA Considerations

IANA will need to reserve two new entries for the "Permanent Message Header Field Names" registry and create a registry for support file formats for BIMI.

10.1. Permanent Header Field Updates

IANA will need to reserve two new entries to the "Permanent Message Header Field Names" registry.

Header field name: BIMI-Selector

Applicable protocol: mail

Status: standard

Author/Change controller: IETF

Specification document: This one

Header field name: BIMI-Location

Applicable protocol: mail

Status: standard

Author/Change controller: IETF

Specification document: This one

10.2. Registry for Support BIMI Formats

Names of support file types supported by BIMI must be registered by IANA.

New entries are assigned only for values that have been documented in a published RFC that has had IETF Review, per [IANA-CONSIDERATIONS]. Each method must register a name, the file extension, the specification that defines it, and a description.

10.3. Other IANA needs

NOTE TO WORKING GROUP: The registry for BIMI tags needs to be properly set up, as does the registry for validation actions.

11. References

11.1. Normative References

[ABNF] Overell, Crocker,., "Augmented BNF for Syntax Specifications: ABNF", January 2008, <http://www.rfc-editor.org/info/rfc5234>.

[Authentication-Results] Kucherawy, M, ., "Message Header Field for Indicating Message Authentication Status", August 2015, <https://tools.ietf.org/html/rfc7601>.

[DKIM] Kucherawy, Ed, Crocker,., "DomainKeys Identified Mail (DKIM) Signatures", September 2011, <http://www.rfc-editor.org/info/rfc6376>.

[DMARC] Zwicky, Ed, Kucherawy,., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", March 2015, <http://www.rfc-editor.org/info/rfc7489>.

[DNS] Mockapetris, P, ., "Domain names - implementation and specification", November 1987, <http://www.rfc-editor.org/info/rfc1035>.

[EMAIL-ARCH] Crocker, D, ., "Internet Mail Architecture", July 2009, <http://www.rfc-editor.org/info/rfc5598>.

[KEYWORDS] Bradner, S, ., "Key words for use in RFCs to Indicate Requirement Levels", March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[SMTP] Klensin, J, ., "Simple Mail Transfer Protocol", October 2008, <http://www.rfc-editor.org/info/rfc5321>.

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

[URI] Masinter, Berners-Lee,., "Uniform Resource Identifier (URI): Generic Syntax", January 2005, <http://www.rfc-editor.org/info/rfc3986>.

11.2. URIs

[1] https://tools.ietf.org/html/rfc6376#section-1

[2] https://tools.ietf.org/html/rfc7208#section-3.3

[3] https://tools.ietf.org/html/rfc6376#section-3.1

Appendix A. Example Selector Discovery (INFORMATIVE)

This section shows several examples of how a receiving MTA should determine which Assertion Record to use depending on the BIMI-Selector header.

A.1. No BIMI-Selector Header

The domain example.com does not send with a BIMI-Selector header.

From: sender@example.com

The MTA would lookup default._bimi.example.com for the BIMI DNS record.

A.2. With BIMI-Selector Header

The domain example.com sends with a BIMI-Selector header:

From: sender@example.com
BIMI-Selector: v=BIMI1; s=selector;

The MTA would lookup selector._bimi.example.com.

A.3. Without BIMI-Selector Header on a subdomain

The domain foo.example.com sends without a BIMI-Selector header:

From: sender@foo.example.com

The MTA would lookup default._bimi.foo.example.com for the BIMI DNS record. If it did not exist, it would lookup default._bimi.example.com.

A.4. With BIMI-Selector Header on a subdomain

The domain foo.example.com sends without a BIMI-Selector header:

```
From: sender@foo.example.com
BIMI-Selector: v=BIMI1; s=selector;
```

The MTA would lookup selector._bimi.foo.example.com for the BIMI DNS record. If it did not exist, it would fall back to the lookup default._bimi.example.com.

A.5. Invalid BIMI-Selector Header

The domain example.com sends with a BIMI-Selector header, but does not include the required field 'v=':

```
From: sender@example.com
BIMI-Selector: s=selector;
```

The MTA would ignore this header, and lookup default._bimi.example.com.

Appendix B. Example Authentication-Results entry (INFORMATIONAL)

This section shows example Authentication-Results stamps based on different BIMI lookup statuses.

B.1. Successful BIMI lookup

```
From: sender@example.com
BIMI-Selector: v=BIMI1; s=selector;
Authentication-Results: bimi=pass header.d=example.com selector=selector;
```

B.2. No BIMI record

```
From: sender@sub.example.com
Authentication-Results: bimi=none;
```

In this example, sub.example.com does not have a BIMI record at default._bimi.sub.example.com, nor does default._bimi.example.com

B.3. Subdomain has no default record, but organizational domain does

```
From: sender@sub.example.com
Authentication-Results: bimi=pass header.d=example.com selector=default;
```

B.4. Subdomain has no record for selector, but organization domain has a default

```
From: sender@sub.example.com
BIMI-Selector: v=BIMI1; s=selector;
Authentication-Results: bimi=pass header.d=example.com selector=default;
```

In this example, the sender specified a DNS record at selector._bimi.sub.example.com but it did not exist. The fallback is to use default._bimi.example.com, not selector._bimi.example.com even if that record exists.

Appendix C. Example BIMI-Location Construction (INFORMATIONAL)

This section shows how an example MTA might evaluate an incoming email for BIMI participation, and how it could share that determination with its MUA(s).

C.1. MTA Receives an email

The MTA receives the following DKIM signed message:

```
DKIM-Signature: v=1; s=myExample; d=example.com; h=From;BIMI-
Selector;Date;bh=...;b=...
From: sender@example.com
BIMI-Selector: v=BIMI1; s=brand;
BIMI-Location: image.example.com/bimi/logo/example-bimi.svg
Subject: Hi, this is a message from the good folks at Example Learning
```

C.2. MTA does its authentication checks

The receiving MTA receives the message and performs an SPF verification (which fails), a DKIM verification (which passes), and a DMARC verification (which passes). The domain is verified and has good reputation. The Receiver proceeds to perform a BIMI lookup.

C.3. MTA performs BIMI Assertion

The MTA sees that the message has a BIMI-Selector header, and it is covered by the DKIM-Signature, and the DKIM-Signature that passed DKIM is the one that covers the BIMI-Selector header. The MTA sees the header validates and contains 'v=BIMI1', and 's=brand'. It performs a DNS query for brand._bimi.example.com and retrieves:

```
brand._bimi.example.com IN TXT "v=BIMI1; l=https://image.example.com/bimi/logo/"
```

The MTA verifies the syntax of the BIMI DNS record, and it, too passes.

C.4. MTA appends to Authentication-Results

The MTA computes and affixes the results of the BIMI to the Authentication-Results header:

```
Authentication-Results: spf=fail smtp.mailfrom=example.com;
  dkim=pass (signature was verified) header.d=example.com;
  dmarc=pass header.from=example.com;
  bimi=pass header.d=example.com selector=brand;
```

C.5. MTA Constructs BIMI-Location header

The MTA knows it has cached the indicator already, and wishes to use this cached indicator instead of a direct reference to the l= tag.

Finally, the MTA removes the existing BIMI-Location header, and stamps the new one:

```
BIMI-Location: v=BIMI1; l=https://cache.mta.example/bimi/logo/bimi-example.com-
sel-brand.svg
```

That the original sender signed a BIMI-Location header against this spec is irrelevant. It was used for DKIM validation and then thrown out by the MTA.

The MTA then sets any relevant BIMI flags on the mail store when it deposits it.

C.6. The MUA displays the indicator

The mail is opened from the mail store in an MUA. The MUA checks to make sure the appropriate BIMI mail store flag has been set, so that it knows it can trust the BIMI-Location header. Finally, the MUA makes a simple determination of which image to show based upon the URI(s) in the BIMI-Location header.

Authors' Addresses

Seth Blank
Valimail

Email: seth@valimail.com

Peter Goldstein
Valimail

Email: peter@valimail.com

Thede Loder (editor)
Skye Logicworks

Email: thede@skyelogicworks.com

Terry Zink (editor)

Email: tzink@terryzink.com