Network
Internet-Draft
Intended status: Standards Track
Expires: 2 November 2026

S. Blank
P. Goldstein
Valimail
T. Loder (ed)
Skye Logicworks LLC
T. Zink (ed)

J. Bradshaw (ed)
Fastmail
A. Brotman (ed)
Comcast
W. Chuang (ed)
Google
1 May 2026

Brand Indicators for Message Identification (BIMI)
draft-brand-indicators-for-message-identification-14

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 interpreted by MTAs and MUAs. MUAs and mail-receiving organizations are free to define their own policies for making use of BIMI data and for Indicator display 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 2 November 2026.

Table of Contents

1. Introduction 4
2. Overview 5
2.1. High-Level Goals 7
2.2. Security 8
2.3. Out of Scope 8
3. Terminology and Definitions 8
3.1. BIMI Assertion 9
3.2. Indicator 9
3.3. Mark Verifying Authority (MVA) 9
3.4. BIMI Evidence Document 9
3.5. Mark Certificate (MC) 9
3.5.1. Verified Mark Certificate (VMC) 9
3.5.2. Common Mark Certificate (CMC) 9
3.6. Protocol Client 10
3.7. Verifying Protocol Client 10
3.8. Local-part 10
4. BIMI DNS Records 10
4.1. MUA Obligations 11
4.2. Personal Avatars and BIMI 11
4.3. Assertion Record Definition 11
4.3.1. Declination to Publish 14
4.3.2. Supported Image Formats for l= tag 14
4.4. Selectors 15
4.5. Local-part Selectors 16
5. BIMI Header Fields 17
5.1. BIMI-Selector Header 18
5.2. BIMI-Location Header 18
5.3. BIMI-Indicator Header 19
5.4. BIMI-Logo-Preference Header 20
5.5. Header Signing 20

5.6. Header Removal 20
6. Domain Owner Actions 21
6.1. Determine and Publish Indicator(s) for Use 21
6.2. Publish Assertion Records 21
6.3. Manage multiple uses of the same Indicator(s) within a trust boundary 21
6.4. Set the headers on outgoing email as appropriate 21
7. Receiver Actions 22
7.1. Authentication Requirements 22
7.2. Assertion Record Discovery 23
7.3. Indicator Discovery. 24
7.4. Indicator Discovery With Evidence. 24
7.5. Indicator Discovery Without Evidence. 24
7.6. Indicator Validation 25
7.7. Affix BIMI Status to Authentication Results Header Field 25
7.8. Handle Existing BIMI-Location and BIMI-Indicator Headers 27
7.9. Construct BIMI-Location URI 27
7.10. Construct BIMI-Indicator header 27
7.11. Construct BIMI-Logo-Preference header 28
8. Security Considerations 28
8.1. Indirect Mail Flows 28
8.2. Lookalike Domains and Copycat Indicators 28
8.3. Large files and buffer overflows 28
8.4. Slow DNS queries 29
8.5. Unaligned Indicators and asserting domains 29
8.6. Unsigned BIMI-Selector Header 29
8.7. CGI scripts in Indicator payload 29
8.8. Metadata in Indicators 29
9. IANA Considerations 30
9.1. Permanent Header Field Updates 30
9.2. Registry for Supported BIMI Formats 30
9.3. Other IANA needs 31
10. Under Discussion 31
11. Normative References 31
12. Informative References 32
Appendix A. Example Selector Discovery (INFORMATIVE) 32
A.1. No BIMI-Selector Header 32
A.2. With BIMI-Selector Header 33
A.3. Without BIMI-Selector Header on a subdomain 33
A.4. With BIMI-Selector Header on a subdomain 33
A.5. Invalid BIMI-Selector Header 33
Appendix B. Example Authentication-Results entry (INFORMATIONAL) 33
B.1. Successful BIMI lookup 34
B.2. No BIMI record 34
B.3. Declination to Publish 34

B.4. Subdomain has no default record, but organizational domain does 34
B.5. Subdomain and organizational domain have no record for selector, but organization 34
B.6. Subdomain has no record for selector, but organization domain does 34
Appendix C. Example BIMI Headers Construction (INFORMATIONAL) . 35
C.1. MTA Receives an email 35
C.2. MTA does its authentication checks 35
C.3. MTA performs BIMI Assertion 35
C.4. MTA appends to Authentication-Results 36
C.5. MTA Constructs BIMI-Location and BIMI-Indicator headers 36
C.6. The MUA displays the Indicator 36
Appendix D. Acknowledgements 36
Authors' Addresses 36

1. Introduction

RFC EDITOR: PLEASE REMOVE THE FOLLOWING PARAGRAPH BEFORE PUBLISHING: The source for this draft is maintained in GitHub at: https://github.com/BLAHBLAHBLAH (https://github.com/BLAHBLAHBLAH)

This document defines Brand Indicators for Message Identification (BIMI), which enables Domain Owners to coordinate with Mail Box Providers (MBPs), Mail Transfer Agents (MTAs), and Mail User Agents (MUAs) in the display of brand-specific Indicators next to properly authenticated messages.

BIMI is designed to be open and to work at Internet scale. BIMI is intended to drive adoption of email authentication best practices by leveraging existing DMARC [RFC7489] policies, the supporting authentication methods DKIM [RFC6376] and SPF [RFC7208], and other associated standards such as ARC [RFC8617].

The approach taken by BIMI is heavily influenced by the approach taken in DKIM [RFC6376], 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.

To participate in BIMI, Domain Owners MUST have a strong [DMARC] policy (quarantine or reject) on both the Organizational Domain, and the RFC5322.From Domain of the message. Quarantine policies MUST NOT have a pct less than pct=100.

This document defines how Domain Owners specify their desired indicators through the BIMI Assertion Record in DNS and how that record is to be interpreted by MTAs and MUAs. 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) can be extended to work with BIMI. Other documents may cover these topics. MUAs and Mail Box Providers (MBPs) are free to define their own policies for making use of BIMI data and for indicator display as they see fit.

2. Overview

The Sender Policy Framework (SPF [RFC7208]), DomainKeys Identified Mail (DKIM [RFC6376]), "Domain-based Message Authentication, Reporting, and Conformance" (DMARC [RFC7489]), and Authenticated Received Chain (ARC [RFC8617]) provide mechanisms for domain-level authentication of 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 Indicators to indicate the identity of the sender of a message. While a discussion of the merits of doing this is beyond the scope of this document, at present there are no open standards for publishing and aiding discovery of preferred Indicators or for tying display of them to authentic messages only.

Because of the desire to have brand-specific Indicators available, some mail-receiving organizations have developed closed systems for obtaining and displaying Brand Indicators for select domains. While this has enabled these mail-receiving organizations to display brand Indicators for a limited subset of messages, this closed approach has a number of 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 any ability they do have is likely to be dependent upon direct coordination with each of 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 standardized manner or optimized for their user interfaces.

This shows 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 MUAs and MBPs, and allows each domain owner to manage their own Indicators. As an additional benefit, mail-originating organizations are incentivized to authenticate their email as doing so will enable them to influence how email and Indicators from the organization are displayed.

The structure of BIMI is as follows:

1. Domain Owners:
    * Fully implement the DMARC [RFC7489] mechanism, to include:
        - Creating and publishing in DNS [RFC1035] a DMARC [RFC7489] policy record that meets the following criteria:
            o The policy record MUST express either a Requested Mail Receiver policy of "quarantine" with an effective percentage of 100%, or a Requested Mail Receiver policy of "reject" (with any percentage value).
            o If a subdomain policy is published it MUST NOT be "none"
            o Be published for the Organizational Domain, and any subdomains thereof
        - Deploying authentication technologies to ensure Identifier Alignment
    * Publish their preferred Brand Indicators via the DNS [RFC1035].
2. Senders: Ensure mail is properly authenticated, and has a sufficiently strict DMARC [RFC7489] policy.
3. MTAs and MBPs:

    * Confirm authenticity of the message using DMARC [RFC7489] and whatever other authentication mechanisms they wish to apply.
    * Check for a corresponding BIMI record, obtaining references to the indicator media and optional substantiation of indicator ownership rights
    * If both the message is authentic and the logo is deemed acceptable, the receiver adds a header to the message which can be used by the MUA to obtain the Domain Owner’s preferred brand indicator.
4. 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. It is also to consolidate validation and Indicator selection operations into the MTA, so that Domain Owners need only publish a few simple records and MUAs only need simple display logic.

It is expected that MBPs implementing BIMI will do so in both their MTAs and MUAs.

#Requirements {#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.

An overview of the security challenges and design decisions is documented at [BIMI-OVERVIEW].

2.1. 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.
* Encourage the adoption of Email Authentication Best Practices.

2.2. 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 the different verification and reputation mechanisms available, but BIMI relies upon them to be in deployed in order to control abuse.

2.3. 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.

3. 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 BCP 14 (https://tools.ietf.org/html/bcp14) [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Readers are encouraged to be familiar with the contents of [RFC5598]. 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 responsibility for providing preferred brand indicators 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) [RFC5234].

"Author Domain", "Domain Owner", "Organizational Domain", and "Mail Receiver" are imported from DMARC [RFC7489] Section 3.

3.1. 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.

3.2. Indicator

The icon, logo, image, mark, or other graphical representation of the brand. The Indicator is defined in a common image format with restrictions detailed in the Assertion Record Definition (#assertion-record-definition).

3.3. Mark Verifying Authority (MVA)

An entity or 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 (i.e., size, trademark, content, etc).

3.4. BIMI Evidence Document

A document published by a Mark Verifying Authority to assert evidence of verification. These are defined in a separate document.

3.5. Mark Certificate (MC)

A certificate issued by a Certificate Authority in accordance with the Minimum Security Requirements for Issuance of Mark Certificates. These requirements are defined in a separate document.

A Mark Certificate is one type of a BIMI Evidence Document, and there are two types of Mark Certificates.

3.5.1. Verified Mark Certificate (VMC)

A Verified Mark Certificate is an MC issued by an MVA in support of BIMI Indicators that are representations of either Registered Trademarks or Government Marks.

3.5.2. Common Mark Certificate (CMC)

A Common Mark Certificate is an MC issued by an MVA in support of BIMI Indicators that are representations either of Prior Use Marks or Modifications of Registered Trademarks.

3.6. Protocol Client

An entity designed to obtain and correctly interpret the records defined in this specification for the purpose of discovering and fetching published Indicators.

3.7. Verifying Protocol Client

A Protocol Client that uses optional capabilities to obtain and evaluate evidence concerning the Domain Owner’s rights to use the published Indicators.

3.8. Local-part

The locally interpret string part of an email address which appears before the at-sign character ("@", ASCII value 64) which is then followed by an Internet domain.

4. BIMI DNS Records

Domain owners publish BIMI policies by adding BIMI Assertion Records in the DNS as TXT records.

Published policies are interpreted and applied by Protocol Clients. A Domain Owner signals intended BIMI participation for one or more of its domains by publishing an Assertion Record in a subdomain under it. In doing so, Domain Owners make specific requests of MUAs regarding the preferred set of Indicators to be displayed with messages that are confirmed to be authorized to appear from the Domain Owner’s domain.

The use of BIMI is opt-in. Receivers default to performing no BIMI-specific message handling until they choose to do so, and then only if a BIMI record for the sender’s domain is found.

BIMI’s use of the DNS is driven in part by BIMI’s use of domain names as the basis of sender identity and message authentication. Use of the DNS as the policy publication service also 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 via one or more email headers. This serves three purposes:

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

2. Operational complexity is reduced. MTAs only need to check a single record in a consistent manner to discover and enforce policy.
3. Indicators SHOULD be verified and cached in advance, so that malicious headers cannot be used as an attack vector.

Per DNS [RFC1035], 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 (https://tools.ietf.org/html/rfc7208#section-3.3).

4.1. MUA Obligations

MUAs 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.

4.2. Personal Avatars and BIMI

Some mailbox providers both participate in BIMI and offer the option of showing personal avatars associated with the sender of an email message delivered to their platforms, and in fact the support for personal avatar display predates BIMI. Some domain owners wishing to participate in BIMI may also desire to have personal avatars displayed for some classes of mail sent using their domain. BIMI offers two options for this - an optional BIMI-Selector header (#bimi-selector), a local-part selector tag, or avatar preference tag in the BIMI Assertion Record (#assertion-record-definition).

4.3. Assertion Record Definition

All Domain Owner BIMI preferences are expressed in DNS TXT records published in subdomains named "_bimi". Multiple sets of preferences can be associated with a single RFC5322.From domain. To distinguish between these different preferences, BIMI defines and uses [selectors]{#selectors}. Senders declare which selector to use for a given message by specifying the selector in an optional BIMI-Selector header (#bimi-selector).

For example, the Domain Owner of "example.com" would post BIMI policy in a TXT record at "default._bimi.example.com". Similarly, a Mail Receiver wishing to query for BIMI policy regarding mail with an RFC5322.From Author Domain of "example.com" and a selector "default" (the default) would query the TXT record located at the subdomain of "default._bimi.example.com". The DNS-based BIMI policy record is referred to as the "BIMI Assertion Record" or "Assertion Record".

BIMI Assertion Records follow the extensible "tag-value" syntax for DNS-based key records as defined in DKIM [RFC6376].

Assertion Records are defined precisely. Mail receivers MUST NOT attempt to fix syntactical or capitalization errors. If a required tag is missing, or its value not well-formed, it is an error.

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 the 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 match or it is absent, the entire retrieved record MUST be ignored. It MUST be the first tag in the list.

ABNF:

```
bimi-version = "v" *WSP "=" *WSP "BIMI1"
```

a= Authority Evidence Location (plain-text; URI; OPTIONAL). If present, this tag MUST have an empty value or its value MUST be a single URI. An empty value for the tag is interpreted to mean the Domain Owner does not wish to publish or does not have authority evidence to disclose. The URI, if present, MUST contain a fully qualified domain name (FQDN) and MUST specify HTTPS as the URI scheme ("https"). The URI SHOULD specify the location of a publicly retrievable BIMI Evidence Document. The format for evidence documents is defined in a separate document.

If the a= tag is not present, it is assumed to have an empty value.

ABNF:

```
bimi-evidence-location = "a" *WSP "=" *WSP [bimi-uri]

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

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

l= location (URI; REQUIRED). The value of this tag is either empty indicating declination to publish, or a single URI representing the location of a Brand Indicator file. The only supported transport is HTTPS.

ABNF:

```
bimi-location = "l" *WSP "=" *WSP [bimi-uri]
```

lps= Local-Part as selector if this tag is present. The value of this tag is zero, one or more local-part string prefixes that are comma separated. When one or more string prefixes are specified, then one of the prefixes MUST prefix match the sending email address local-part. If no string prefix is specified, then the local-part always matches. When the prefix match is successful, then the MBP MUST lookup a selector derived from the local-part of the sending email address. String prefix character set contains ALPHA and DIGIT which are defined in [RFC5234], and '-'.

ABNF:

```
local-part-selector = "lps" *WSP "=" *WSP *1local-part-prefix-list

local-part-prefix-list = local-part-prefix *[ *WSP ',' *WSP local-part-prefix ]

local-part-prefix = 1*63local-part-text

local-part-text = ALPHA / DIGIT / '-'

; ALPHA is A-Z and a-z, DIGIT is 0-9
```

avp= Avatar Preference (plain-text; OPTIONAL; default is "brand"). For mail sent to those mailbox providers that both participate in BIMI and support the display of personal avatars, this flag is a way for the Domain Owner to express its preference as to whether to show the BIMI logo or the personal avatar. If the tag is not present in an otherwise syntactically valid BIMI record, then the record is treated as if it included "avp=brand". Allowed values are:

personal: If BIMI is in place for the sending domain and the sender of the email has a personal avatar, then the mailbox provider SHOULD display the personal avatar for the message when shown in the recipient's mailbox. If the sender has no personal avatar, then the BIMI logo should be shown if the message qualifies for such display.

brand: If BIMI is in place for the sending domain and the sender of the email has a personal avatar, then the mailbox provider SHOULD display the BIMI logo for the domain if the message qualifies for such display.

Any other values MUST be ignored and not included in and added headers. A mailbox provider MAY choose to treat an invalid preference value as a failing record.

ABNF:

```
bimi-logo-preference = "avp" *WSP "=" *WSP %s "personal"/"brand" bimi-sep
```

Therefore, the formal definition of the BIMI Assertion Record, using ABNF [RFC5234], is as follows:

```
bimi-sep = *WSP ";" *WSP

bimi-record = bimi-version (bimi-sep bimi-location) [(bimi-sep bimi-evidence-location)] [
(local-part-selector)] [(bimi-sep bimi-logo-preference)] [bimi-sep]

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

4.3.1. Declination to Publish

If both the "l=" and "a=" tags are empty, it is an explicit refusal to participate in BIMI. This is distinct from not publishing a BIMI record. For example, an empty BIMI record enables a Domain Owner to decline BIMI participation for a subdomain 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=;
```

If the sender wishes to only enable BIMI on specific selectors utilizing the local-part selector mechanism, but decline BIMI for the default case then the BIMI record may look like:

```
v=BIMI1; l=; a=; lps=brand-indicators-;
```

As the string prefix list contains brand-indicators-, any local-part that prefix matches brand-indicator- will continue with a BIMI assertion record lookup using the local-part selector.

4.3.2. 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 URI ends with any other image format suffix, or if the document retrievable from the location(s) in the l= tag are of any other format, the evaluation of the record MUST be treated as a permanent error.

As of the publishing of this document, only SVG and SVGZ, as defined in RFC6170 section 5.2 (https://tools.ietf.org/html/rfc6170#section-5.2) is acceptable in the l= tag. Further restrictions apply to the SVG; these are documented elsewhere.

4.4. Selectors

To support publishing and display of more than one distinct Brand Indicator per domain, the brand Indicator namespace is subdivided for publishing of multiple Assertion Records using "selectors". Selectors allow the Domain Owner to choose the brand Indicator, for example, by type of recipient, by message source, or by other considerations like seasonal branding. BIMI selectors are modeled after DKIM selectors (https://tools.ietf.org/html/rfc6376#section-3.1).

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 (#bimi-selector), or by utilizing Local-part Selectors (#local-part-selectors).

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.

4.5. Local-part Selectors

To support the case where a domain owner may wish to display more than one distinct Brand Indicator per domain, or decline to publish a Brand Indicator for specific messages, but is unable to easily add BIMI-Selector headers to the relevant outbound mail, the BIMI assertion record may include the tag lps= (local-part selector). The following are examples including string prefixes:

lps=

lps=brand-indicator-

lps = brand-one-noreply , brand-two-noreply

If the lps= tag is present then a supporting MBP MUST perform the following actions.

1 - Each time a BIMI assertion record is queried, either for the RFC5322 domain or for the Organizational domain thereof.

2 - Lookup the BIMI assertion record and check for the lps= tag, if this is not present then processing continues as normal.

3 - Normalize the local-part of the sending email address using the following algorithm

* Remove any Subaddress Extension ([RFC5233]) part (sometimes called plus addressing) from the local-part address. If the local-part contains the plus character ("+", ASCII value 43) then remove this character along with all following characters from the string.

* Replace all underscores ("_", ASCII value 95) and periods (".", ASCII value 46) with a dash ("-", ASCII value 45). If more than 1 of these occur sequentially then replace the group with a single dash. Dashes at the beginning and end of the string are removed.

* If the remaining local-part contains only letters ("A-Z", ASCII value 65-90) ("a-z", ASCII value 97-122), digits ("0-9", ASCII value 48-57), and dashes ("-", ASCII value 45, and is at most 63 characters long, then the string is in normalized form and may be used as a selector.

* If the remaining local-part contains any other characters then it may not be used as a selector, There are several RFCs which discuss potential solutions to this, including ([RFC3492]), ([RFC7929]) and ([RFC6530]), however to simplify the selector name and resulting DNS record, it is recommended that only the above mentioned characters be used in sending email addresses for BIMI local-part selectors.

* While the local-part may be considered case sensitive, the selector is case insensitive. This must be taken into consideration when choosing the local-part for sending BIMI selector enabled mail.

4 - If the lps= tag has a value string, the sender indicates to preform string prefix matching. Split the value string by the comma ',' separator and strip off any whitespaces into a list of string prefixes. Then prefix match the local-part against each of the string prefixes and if any matches, then continue to step 5 otherwise stop here. If no value string is present, continue to step 5.

5 - Using the normalized local-part as a selector, lookup the BIMI assertion record from the domain at which the lps= tag was found with the new local-part selector present.

6 - If this record is found then processing MUST continue as if this was the record found at step 1

7 - If this record is not found then processing MUST continue using the original record as discovered at step 1

Proper usage of the local-part string prefixes can reduce or eliminate non-matching local-part selector lookups, meaning unnecessary DNS lookups. A receiver MAY mandate its usage with a mininmum prefix length before performing the local-part selector lookups.

5. BIMI Header Fields

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

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

5.1. BIMI-Selector Header

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 Assertion Record is located in the DNS at default._bimi.example.com. However, a Domain Owner may override the use of the default selector and specify the use of an alternative using the RFC5322-compliant 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 \[bimi-sep\]

5.2. BIMI-Location Header

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 follows:

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, he entire header 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; OPTIONAL if a bimi-evidence-location-header-uri is specified, otherwise REQUIRED.). Inserted by the MTA after performing the required checks and obtaining the applicable domain’s published Assertion Record. The value of this tag is a URI representing the location of the Brand Indicator file. HTTPS is the only supported transport.

ABNF:

```
bimi-location-header-uri = "l" *WSP "=" bimi-uri
```

a: location of the BIMI Evidence Document (URI; REQUIRED if the BIMI Evidence Document was verified). Inserted by the MTA after performing the required checks and obtaining the applicable domain’s published Assertion Record. The value of this tag is a URI representing the location of the BIMI Evidence Document. HTTPS is the only supported transport.

ABNF:

```
bimi-evidence-location-header-uri = "a" *WSP "=" bimi-uri
```

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

```
bimi-location-header-location-only = bimi-location-header-uri

bimi-location-header-evidence-only = bimi-evidence-location-header-uri

bimi-location-header-both = bimi-location-header-uri bimi-evidence-location-header-uri

bimi-location-options = bimi-location-header-location-only / bimi-location-header-evidenc
e-only / bimi-location-header-both

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

5.3. BIMI-Indicator Header

BIMI-Indicator is the header a Mail Receiver inserts to pass a verified Indicator to the MUA.

The header contains the SVG of the Indicator encoded as base64, and is inserted by the MTA after performing the required checks and obtaining the applicable domain’s published Assertion Record. The contents of this tag MUST match the SVG Indicator content retrieved from the URI specified in the BIMI-Location header. If he Indicator was supplied as a gzipped SVGZ file then the MTA MUST uncompress the file before base64 encoding.

```
base64string    =  ALPHADIGITPS *([FWS] ALPHADIGITPS)
                   [ [FWS] "=" [ [FWS] "=" ] ]
```

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

```
bimi-indicator-header = base64string
```

5.4. BIMI-Logo-Preference Header

BIMI-Logo-Preference is the header a Mail Receiver inserts to pass the Domain Owner’s preference for personal avatar display to the MUA.

The syntax of the header is as follows:

ABNF:

```
bimi-logo-preference-header = "avp" *WSP "=" *WSP %s "personal"/"brand" bimi-sep
```

5.5. Header Signing

If present, the BIMI-Selector header SHOULD be included in the DMARC-aligned DKIM signature used to confirm authenticity of the message. If it is not included in the DMARC-compliant DKIM signature, the header SHOULD be ignored.

Receivers MAY choose to apply additional methods to validate the BIMI-Selector header, for example by evaluating a trusted [ARC] chain. In this case the Receiver MAY choose to treat the message as if the BIMI-Selector header was signed.

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

5.6. Header Removal

When a site is BIMI-aware, the receiving MTA MUST remove the MTA-produced headers (BIMI-Location, BIMI-Indicator, BIMI-Logo-Preference) when those headers originate from outside the current site. For example, a multi-stage platform will likely want to leave those in place. However, when the message arrives from another site with those headers available, they MUST be removed.

When a site is not BIMI-aware, they SHOULD remove those headers. If the receiving site has no awareness of that evaluation, the headers should be treated as suspect, and removed.

6. 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.

6.1. Determine and Publish Indicator(s) for Use

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

6.2. 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.

6.3. 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.

6.4. 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.

7. Receiver Actions

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

7.1. Authentication Requirements

Before applying BIMI processing for a message, a receiver MUST verify that the message passed the following BIMI authentication requirements:

1. If more than 1 RFC5322.From header is present in the message, or any RFC5322.From header contains more than 1 email address then BIMI processing MUST NOT be performed for this message.
2. Start with the DNS domain found in the RFC5322.From header in the message. Define this DNS domain as the Author Domain.
3. Find the Organizational Domain for the Author Domain. Define this DNS domain as the Author Organizational Domain. If the Author Domain is an Organizational Domain then this will be identical to the Author Domain.
4. Evaluate the DMARC [RFC7489] result for the Author Domain. Define the result as the BIMI DMARC Result.
5. If the BIMI DMARC result is not ’pass’, then the receiver MAY choose to apply additional authentication methods, for example by evaluating a trusted ARC [RFC8617] chain, a list of trusted forwarders, or by applying a local policy. In this case the Receiver MAY choose to treat the message as if the BIMI DMARC Result was ’pass’.
6. If the DMARC [RFC7489] result for the Author Domain is not ’pass’, and the message could not be authenticated by any additional authentication method, then BIMI processing MUST NOT be performed for this message.
7. If the DMARC [RFC7489] policy for the Author Domain or Author Organizational Domain is p=none then BIMI processing MUST NOT be performed for this message.
8. If the DMARC [RFC7489] record for the Author Domain or Author Organizational Domain includes a subdomain policy, and that subdomain policy is sp=none then BIMI processing MUST NOT be performed for this message.
9. If the DMARC [RFC7489] policy for the Author Domain or Author Organizational Domain is p=quarantine, and the DMARC [RFC7489] record defines a percentage tag, then that tag MUST be pct=100, otherwise BIMI processing MUST NOT be performed for this message.

7.2. Assertion Record Discovery

Through the BIMI Assertion Record (#assertion-record-definition), Domain Owners use DNS TXT records to advertise their preferences. Preference discovery is accomplished via a method similar to the method used for DMARC [RFC7489] records. This method, and the important differences between BIMI and DMARC [RFC7489] mechanisms, are discussed below.

Assertion Record Discovery MUST NOT be attempted if the message authentication fails 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 (#bimi-selector), 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 resulting record includes the Local-part Selector (#local-part-selectors) tag lps= then the client MUST first normalize the local-part of the RFC5322.From header as detailed in Local-part Selector (#local-part-selectors), and if this differs from any selector and domain combination already queried, MUST query DNS for the BIMI TXT record at the domain constructed by concatenating the normalized selector, the string '_bimi', and the Author domain. If a valid BIMI record is found then this should be used, if not then the BIMI record retrieved in step 3 MUST be used instead.
6. 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, the string '_bimi', and the Organizational Domain (as defined in DMARC [RFC7489]) corresponding to the Author Domain. A custom selector that does not exist falls back to <selector>._bimi.<organizationalDomain>. A possibly empty set of records is returned.
7. Records that do not start with a "v=" tag that identifies the current version of BIMI MUST be discarded.

8. If the resulting record includes the Local-part Selector (#local-part-selectors) tag lps= then the client MUST first normalize the local-part of the RFC5322.From header as detailed in Local-part Selector (#local-part-selectors), and if this differs from any selector and domain combination already queried, MUST query DNS for the BIMI TXT record at the domain constructed by concatenating the normalized selector, the string '_bimi', and the Organizational domain. If a valid BIMI record is found then this should be used, if not then the BIMI record retrieved in step 6 MUST be used instead.
9. If the remaining set contains multiple records or no records, Assertion Record Discovery terminates and BIMI processing MUST NOT be performed for this message.
10. If the remaining set contains only a single record, this record is used for BIMI Assertion.

7.3. Indicator Discovery.

1. If the retrieved Assertion Record does not include a valid bimi-location in the l= tag, then Indicator Discovery has failed, and the Indicator MUST NOT be displayed. The bimi-location entry MUST be a URI with a HTTPS transport.
2. If the retrieved Assertion Record includes a bimi-evidence-location entry in the a= tag, and the receiver supports BIMI Evidence Document validation, then proceed to the Indicator Discovery With Evidence (#indicator-discovery-with-evidence) step.
3. If the receiver does not support BIMI Evidence Document validation, or the retrieved Assertion Record does not include a bimi-evidence-location entry, then proceed to the Indicator Discovery Without Evidence (#indicator-discovery-without-evidence) step.

7.4. Indicator Discovery With Evidence.

Individual types of BIMI Evidence Document MAY specify extra discovery and validation steps. These will be defined in separate documents.

7.5. Indicator Discovery Without Evidence.

If an Assertion Record is found, and it has empty bimi-location and bimi-evidence-location then this is a Declination to Publish record. BIMI processing MUST not occur on this message and the MTA SHOULD reflect this in the Authentication-Results header by adding a bimi=declined entry.

If an Assertion Record is found, and has an empty or missing bimi-evidence-location entry then no evidence has is presented, and the Indicator MUST be retrieved from the URI specified in the bimi-location entry using the following algorithm:

1. Retrieve the SVG Indicator from the URI specified in the l= tag. This MUST be a URI with a HTTPS transport.
2. If the TLS server identity certificate presented during the TLS session setup does not chain-up to a root certificate the Client trusts then Indicator validation has failed and the Indicator MUST NOT be displayed.
3. Proceed to the Indicator Validation (#indicator-validation) step.

7.6. Indicator Validation

1. Check the file size of the retrieved Indicator against recommended maximum sizes as defined in this document, and in the BIMI SVG document. A receiver MAY choose to implement their own file size restrictions. If the Indicator is larger than the maximum size the the receiver MAY choose not to display the Indicator. A receiver MAY choose to implement the size limit as a retrieval limit rather than retrieving the entire document and then checking the size.
2. If the SVG Indicator is missing, or is not a valid SVG or SVGZ document then validation has failed and the Indicator MUST NOT be displayed.
3. Check the retrieved Indicator against the SVG validation steps specified in this document, and in the BIMI SVG document.
4. If Indicator verification has passed, and the Indicator is from a trusted source, then the Indicator MAY be displayed per receiver policy.

7.7. Affix BIMI Status to Authentication Results Header Field

Upon completion of Assertion Record Discovery, Indicator Discovery, and Indicator Validation, 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, failure in Discovery or Validation steps, or some other error), 'temperror' (DNS lookup problem), 'declined' (The domain owner published an explicit declination record), or 'skipped' (BIMI check was not performed, 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=fail (Invalid SVG)", "bimi=skipped (sender not trusted)" or "bimi=skipped (message failed DMARC)".

header.d: Domain of the BIMI Assertion Record which was evaluated (plain-text; REQUIRED if bimi=pass). For example, this will be the organizational domain if the BIMI lookup used the fallback record, otherwise it will be the RFC5322.From domain.

header.selector: Selector of the BIMI Assertion Record which was evaluated (plain-text; REQUIRED if bimi=pass). For example, if a BIMI-Selector Header was present and used to discover a BIMI Assertion Record then this will be the Selector used, otherwise this will be 'default'.

policy.authority: Authority verification status of the Brand Identifier (plain-text; REQUIRED if the BIMI Evidence Document was checked). If the Authority Evidence presented in the BIMI Assertion Record was checked and found to be valid then this MUST be set to pass. If the validation failed then this MUST be set to fail. If no Authority Evidence was presented, or the MTA did not check the Authority Evidence then this SHOULD be set to none.

policy.authority-uri: The URI of the BIMI Evidence Document checked, as found in the a= tag of the BIMI Assertion Record (plain-text; OPTIONAL).

policy.indicator-uri: The URI of the BIMI Indicator, as found in the l= tag of the BIMI Assertion Record (plain-text; OPTIONAL).

policy.indicator-hash: In order to prevent MUAs from displaying indicators from the BIMI-Indicator header which have been modified since delivery, the MTA MAY add a hash of the data referenced in that header into the Authentication-Results entry such that the hash can be signed by, and verified by an ARC aware MTA/MUA pair. The raw uncompressed data of the SVG Indicator is hashed with SHA-256, the resulting hash is truncated to the final 8 (at least) characters, and added to the Authentication-Results entry. If this entry is added then the MTA MUST also add the BIMI-Indicator header.

policy.logo-preference: Contains the Domain Owner's preference for personal avatar display as defined in the BIMI-Logo-Preference header (plain-text; OPTIONAL). The MTA MUST NOT add this entry if the value discovered in the BIMI record was invalid.

7.8. Handle Existing BIMI-Location and BIMI-Indicator Headers

Regardless of success of the BIMI lookup, if a BIMI-Location, BIMI-Indicator, or BIMI-Logo-Preference header is already present in a message it MUST be either removed or renamed. This is because the MTA performing BIMI-related processing immediately prior to a Mail Delivery Agent (or within the same administrative realm) is the only entity allowed to specify the BIMI-Location, BIMI-Indicator, and BIMI-Logo-Preference headers (e.g. not the sending MTA, and not an intermediate MTA). Allowing one or more existing headers through to a MUA is a security risk.

If the original email message had a DKIM signature, it has already been evaluated. Removing the BIMI-Location, BIMI-Indicator, or BIMI-Logo-Preference headers at this point should not invalidate the signature since it should not be included within it per this spec.

7.9. Construct BIMI-Location URI

This header MUST NOT be added if Discovery or Validation steps failed.

The URI used to retrieve the validated SVG Indicator. If the receiver extracted the Indicator from the BIMI Evidence Document then this SHOULD be the bimi-evidence-location added with a a= tag, otherwise it SHOULD be the bimi-location added with a l= tag. If both a= and l= tags are included then the MTA MUST perform checks to ensure that the SVG Indicator referenced by the bimi-location is identical to the SVG Indicator extracted from the BIMI Evidence Document.

7.10. Construct BIMI-Indicator header

This header MUST NOT be added if Discovery or Validation steps failed.

Encode the SVG Indicator retrieved and validated during the Indicator Discovery and Indicator Validation steps as base64 encoded data. If the Indicator was compressed with gzip when retrieved then the data MUST be uncompressed before being base64 encoded.

The MTA MUST fold the header to be within the line length limits of SMTP [RFC5321].

7.11. Construct BIMI-Logo-Preference header

This header MUST NOT be added if Discovery or Validation steps failed.

This contains the policy from the BIMI record indicating the domain owners preference for logo display.

The MTA MUST fold the header to be within the line length limits of SMTP [RFC5321].

The MTA MUST NOT add this header if the value discovered in the BIMI record was invalid.

8. Security Considerations

The consistent use of Brand Indicators is valuable for Domain Owners, Mail Receivers, and End Users. However, the routine display of brand Indicators represents an attractive target for abuse, especially for determined malicious actors. Great care is warranted. The discussion following as an incomplete list of considerations.

8.1. Indirect Mail Flows

If a mail store ingests a message from another mail store through some other means, the message may or may not have BIMI headers added already. If the receiving store trusts the other mail store, it may simply use existing headers. Or, it may re-evaluate BIMI policy and requirements, and create or replace the BIMI-Location header.

8.2. Lookalike Domains and Copycat Indicators

Publishing BIMI records is not sufficient for an MTA to signal to the MUA to load the BIMI Indicator. For example, the Domain Owner may also need to have a sufficiently strong reputation with the MTA. The receiver may use a manually maintained list of large brands, it may import a list from a third party of acceptable domains, or it may apply its own reputation heuristics before deciding whether or not to load the BIMI Indicator. BIMI does not specify what MTAs may bring to bear as additional factors.

8.3. 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.

8.4. 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 Indicators 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 Indicators.

8.5. 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.

8.6. 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.

8.7. 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.

8.8. 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.

9. IANA Considerations

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

9.1. Permanent Header Field Updates

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

Header field name: BIMI-Indicator

Applicable protocol: mail

Status: standard

Author/Change controller: IETF

Specification document: This one

9.2. Registry for Supported 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.

9.3. Other IANA needs

10. Under Discussion

NOTE: Items currently being discussed

o Can the MUA validate BIMI directly? What hints are needed? How can it be validated with some semblance of trust?

11. Normative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[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>.

[RFC3492] Costello, A., "Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)", RFC 3492, DOI 10.17487/RFC3492, March 2003, <https://www.rfc-editor.org/info/rfc3492>.

[RFC5233] Murchison, K., "Sieve Email Filtering: Subaddress Extension", RFC 5233, DOI 10.17487/RFC5233, January 2008, <https://www.rfc-editor.org/info/rfc5233>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <https://www.rfc-editor.org/info/rfc5321>.

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

[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>.

[RFC6530] Klensin, J. and Y. Ko, "Overview and Framework for Internationalized Email", RFC 6530, DOI 10.17487/RFC6530, February 2012, <https://www.rfc-editor.org/info/rfc6530>.

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014, <https://www.rfc-editor.org/info/rfc7208>.

[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>.

[RFC7929] Wouters, P., "DNS-Based Authentication of Named Entities (DANE) Bindings for OpenPGP", RFC 7929, DOI 10.17487/RFC7929, August 2016, <https://www.rfc-editor.org/info/rfc7929>.

[RFC8617] Andersen, K., Long, B., Ed., Blank, S., Ed., and M. Kucherawy, Ed., "The Authenticated Received Chain (ARC) Protocol", RFC 8617, DOI 10.17487/RFC8617, July 2019, <https://www.rfc-editor.org/info/rfc8617>.

12. Informative References

[BIMI-OVERVIEW] "An Overview of the Design of BIMI", <http://tools.ietf.org/html/draft-bkl-bimi-overview-00.html>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Appendix A. 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=myselector;
```

The MTA would lookup myselector._bimi.foo.example.com for the BIMI DNS record. If it did not exist, it would fall back to the lookup myselector._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=myselector;
```

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=myselector;
Authentication-Results: example.com; bimi=pass header.d=example.com header.selector=mysel
ector
```

B.2. No BIMI record

```
From: sender@sub.example.com
Authentication-Results: example.com; 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. Declination to Publish

```
From: sender@example.com
Authentication-Results: example.com; bimi=declined
```

In this example the record found at default._bimi.example.com was "v=BIMI1; l=; a=;", indicating a Declination to Publish a BIMI Assertion Record, and so indicating that BIMI processing should not occur on this message.

B.4. Subdomain has no default record, but organizational domain does

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

B.5. Subdomain and organizational domain have no record for selector, but organization

domain has a default

```
From: sender@sub.example.com
BIMI-Selector: v=BIMI1; s=myselector;
Authentication-Results: example.com; bimi=none
```

In this example, the sender specified a DNS record at myselector._bimi.sub.example.com but it did not exist. The fallback is to use myselector._bimi.example.com, which also does not exist. The assertion record does exist for the default selector at the organizational domain default._bimi.example.com, however this is not used as the sender specified a selector of myselector.

B.6. Subdomain has no record for selector, but organization domain does

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

In this example, the sender specified a DNS record at myselector._bimi.sub.example.com but it did not exist. The fallback is to use myselector._bimi.example.com.

Appendix C. Example BIMI Headers 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.

The MTA knows it has previously retrieved the Indicator referenced by the BIMI DNS record, and had already successfully checked this Indicator against the published SVG profile. The MTA retrieves the Indicator from the cache.

C.4. MTA appends to Authentication-Results

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

```
Authentication-Results: example.com; 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 header.selector=brand
```

C.5. MTA Constructs BIMI-Location and BIMI-Indicator headers

The MTA base64 encodes the retrieved Indicator and constructs a new BIMI-Indicator header.

The MTA constructs a BIMI-Location header with a version tag, and an l tag indicating the URL from which the Indicator was retrieved.

Finally, the MTA removes any existing BIMI-Location and BIMI-Indicator headers, and stamps the new ones:

BIMI-Location: v=BIMI1; l=https://image.example.com/bimi/logo/

BIMI-Indicator: PD94bW...8L3N2Zz4K

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.

C.6. The MUA displays the Indicator

The mail is opened from the mail store in an MUA. The MUA performs locally defined checks to make sure that it can trust the BIMI-Indicator header. Finally, the MUA extracts the Indicator from the BIMI-Indicator header and displays it to the user.

Appendix D. Acknowledgements

Many people have contributed to the development of BIMI. Along with thanks to members of the current AuthIndicators Working Group, the editors wish to acknowledge the efforts of Sri Somanchi, Don Cardinal, Steve Jones, and John Levine.

Authors' Addresses

Seth Blank
Valimail
Email: seth@valimail.com

Peter Goldstein
Valimail
Email: peter@valimail.com

Thede Loder
Skye Logicworks LLC
Email: thede@skyelogicworks.com

Terry Zink
Email: tzink@terryzink.com

Jemma Bradshaw
Fastmail
Email: jemma@fastmailteam.com

Alex Brotman (ed)
Comcast
Email: alex_brotman@comcast.com

Wei Chuang (ed)
Google
Email: weihaw@google.com