Brand Indicators for Message Identification

IETF104
March, 2019

Alex Brotman
Neil Kumaran
Seth Blank
Wei Chuang
Agenda

1. **Overview**
   a. Why do this?
   b. Use cases + Implementers
   c. Why are we here?
   d. Common Concerns

2. **Mechanisms (Options, Threats, Thoughts)**
   a. Publishing Options
   b. Validation Options
   c. Consumption
   d. Reporting
   e. Remediation

3. **Current Proposal**
   a. Shortcomings
   b. Proposal and requirements
   c. VMC / JWT API
   d. Abuse Vectors

4. **Discussion/Questions**
   a. IETF problems?
OVERVIEW

1. WHY DO THIS?
2. USE CASES + IMPLEMENTERS
3. WHY COME TO THE IETF?
4. COMMON CONCERNS
Here's the invoice for October. The due amount is at the bottom.

**Invoice Portal**

Let us know when you can arrange the payment.

Thank you

Warm regards,

Russell
Context: Auth Helps

Mon 10/31/2016 8:37 AM

russellrobinson@outlook.com

Re: Oct invoice

To: someone@microsoft.com

Not a contact, Weak policy but looks legit enforcement

Here's the invoice for october. The due amount is at the bottom.

Invoice Portal

Let us know when you can arrange the payment.

Thank you

Warm regards,

Russell

Reasonably worded, grammatically correct. Could be real.
Why Do this?

- SPF/DKIM/DMARC are important, and increase security
  - But adoption is low, growth is slow
- The ecosystem can speed up adoption by increasing incentives
- Receivers want to incent strong authentication. Senders want their logos displayed to their customers. Logos already exist on a number of mail platforms (albeit inconsistently implemented)
- BIMI proposes tying validated logos to authenticated messages
## Logo Display: The State of the World

### Receivers
- Closed systems
  - Inconsistent
  - Limited coverage
  - High overhead
  - Not very scalable
  - Quickly outdated

- Many different closed systems
  - No consistency
  - No interoperability
  - Not necessarily tied to auth

### Senders
- No direct control over logos and usage
- Limited ability to influence
  - Relationship driven
  - Must coordinate with many different receivers
  - Unknown requirements

- Most can’t participate
  - No relationships
  - Insufficient scale

¯\_(ツ)_/¯
Use Cases

As a sender, I’d like to:

● Have my customers see my logo as they interact with my messages
● Avoid going through a different logo verification process with each receiver
● Ensure my logo is only used on messages I’m sending
● Have the ability to change the version of my logo that receivers are using

As a mailbox, I’d like to have:

● More incoming traffic be authenticated, to better protect my users
● Senders provide their logos in a scalable and standardized way
● Some assurances that senders are providing logos that are actually theirs
Overview

**BIMI**: A way to publish, validate, and retrieve logos tied to a domain

tl;dr:

1. Sender implements DMARC ([RFC7489](https://tools.ietf.org/html/rfc7489)) at quarantine or reject
2. Sender gets logo validated
3. Sender publishes a DNS record pointing to their logo and its validation
4. Mailboxes can retrieve the logo, confirm validation, and display the logo

**Why?**

- For senders: A standardized approach to publishing logos.
- For mailboxes: A standardized approach to retrieving logos.
What BIMI IS

1. An incentive to adopt email authentication
   SPF (RFC7208), DKIM (RFC6376), and DMARC (RFC7489)

2. A mechanism for mail senders to suggest to mailboxes the proper logos to display alongside a message

3. A validation method for a sender to assert they are authorized to use the logo they want to display
What BIMI IS NOT

1. About improving user trust

2. Anti-phishing (beyond incenting auth)

3. Arbitrary logo display (i.e. gravatars or favicons)

4. A guarantee of logo display
   (Receiver anti-abuse infrastructure may still choose not to display a logo)

5. Solely about email
   (Other services that need a domain ⇒ logo link should be able to use BIMI)
Some Known Implementations

**Receivers:**

- Google
- Verizon Media (Yahoo!)
- Microsoft
  (Business Profiles, not BIMI)
Some Known Implementations and Adoption

Receivers:

- Google
- Verizon Media (Yahoo!)
- Microsoft
  (Business Profiles, not BIMI)

Many other interested parties:

- Numerous other receivers
- Brands of all sizes
- Major ESPs
- Organizations like JIPDEC

And... plenty of circumstantial evidence that BIMI incentivizes adoption of email authentication.
Why are we here?

- To engage IETF with our work
- To get feedback on our approach before implementation
- To seek advice and opinions on the challenges we’re facing

With the goal of ensuring that BIMI is globally accessible
Common Concerns

General concerns

- This will create a web bug that allows for tracking of users
- This turns email into a post-apocalyptic-advertising-hellscape
- Small senders/mailboxes won’t be able to use BIMI
- Logo payload based attacks will still be possible
- BIMI becomes mandatory for inbox placement

Validation problems

- Adequate vetting will require humans
- Laws around brand imagery vary around the world
- Existing validation ecosystems (e.g., EV) are brittle and prone to abuse
MECHANISMS

BIMI requires a suite of mechanisms to function

draft-bkl-bimi-overview-00

Publishing: how a domain asserts its logo

Validation: how a domain proves it can assert the logo

Consumption: how a receiving system can utilize asserted logos

Reporting: feedback to ensure the previous mechanisms are working

Remediation: method to remove fraudulent or invalidly asserted logos from the wider ecosystem
## Policy Publishing options

Goal: lightweight, transparent, flexible, and extensible

<table>
<thead>
<tr>
<th>Policy</th>
<th>Value</th>
<th>Concerns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message header field</td>
<td>• Straight-forward</td>
<td>• Requires sending systems to be aware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Requires per-message validation of the field</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Can’t pre-fetch or cache effectively</td>
</tr>
<tr>
<td>S/MIME</td>
<td>• Self-validating</td>
<td>• Lack of ecosystem support for S/MIME</td>
</tr>
<tr>
<td></td>
<td>• Works offline</td>
<td>• Certificate Authority problems well known</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Most senders don’t have the skill to implement</td>
</tr>
<tr>
<td>VBR</td>
<td>• Standard</td>
<td>• Same issues as message header field</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Not widely deployed</td>
</tr>
<tr>
<td>DNS record</td>
<td>• Simple</td>
<td>• Forces BIMI to be domain-based</td>
</tr>
<tr>
<td></td>
<td>• Allows for caching</td>
<td>• DNS hijacking</td>
</tr>
<tr>
<td></td>
<td>• Feels like DMARC</td>
<td></td>
</tr>
</tbody>
</table>
# Validation Options

<table>
<thead>
<tr>
<th></th>
<th>Reputation</th>
<th>Centralized Registry</th>
<th>Third Party</th>
<th>Sender</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Participation</strong></td>
<td>Large senders</td>
<td>Registered marks</td>
<td>Most senders</td>
<td>Everyone</td>
</tr>
<tr>
<td><strong>Initialized/ Openness</strong></td>
<td>No- history based / Closed proprietary</td>
<td>Yes / Partial</td>
<td>Yes / Yes</td>
<td>No / Yes</td>
</tr>
<tr>
<td><strong>Standardization Effort</strong></td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Cost</strong></td>
<td>Receiver pays</td>
<td>Maybe: Owner pays</td>
<td>Yes: Owner pays</td>
<td>None</td>
</tr>
<tr>
<td><strong>Weaknesses</strong></td>
<td>Reputation hijacking</td>
<td>Inconsistency and participation</td>
<td>Weak/corrupt validation</td>
<td>🙈</td>
</tr>
</tbody>
</table>
Consumption

- MTAs validate
  - SPF/DKIM/DMARC validation
  - BIMI validation

- Logo is retrieved as needed
  - Logo is cached

- Logo display is still up to receiver on a per-message basis
Reporting

Provide feedback loops for understanding and fixing any issues with published logos.

Intended as an add-on to DMARC reporting, providing information about:

- whether configuration is correct
- how many were eligible for BIMI upon receipt

Must **NOT**:

- Create a web bug
- Number of displayed logos
- Expose mail system internals
Remediation

If one receiver determines a domain is using an logo fraudulently, the entire ecosystem should be able to prevent this fraud.

- How could this work at scale?
  - In practice, this generally doesn’t work
- Revocation?
- Penalizing third parties?

**Must NOT:**

- Allow fraudulent logos to continue to be displayed
- Create a web bug through revocation checks
- Limit participation by smaller mailboxes
CURRENT PROPOSAL

1. Shortcomings
2. Proposal and Requirements
3. VMC / JWT API
4. Scary problems
Shortcomings of the current proposal

- Originating working group individuals are from the US and large companies
  - Both for senders and receiving organizations
  - Unclear how this scales to every market
- No way to automate logo validation
  - This means it requires a human
- Receivers still have to determine whom to trust
  - Have to pick and choose third parties to trust
- No global solution for lookalike logos
- Failure to cache logos results in a web bug
Current proposal


DNS Publishing: (TXT record on default._bimi.[domain])

v=BIMI1; l=[HTTPS URL to SVG]; a=[mechanism]:[HTTPS URL for validation]

And validation:

- Third party (Indicator Verifying Authority):
  - Certificates + CAs
  - JWT API
- Self-attestation
  - Please don’t display these unless your reputation system works really well
Third Party Attestation

Verified Indicator Certificate (VIC) /
API- JSON Web Tokens
Third Party Validation Requirements

- Organization is a verifiable legal entity
- Domain names are controlled by the organization
- Individual requesting validation is currently authorized to do so by the organization
- Individual requesting the validation is who they say they are
- Organization has the rights to display the logo
## Publication of Third Party Validation

<table>
<thead>
<tr>
<th></th>
<th>CA issued certificate</th>
<th>Validator API</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard</strong></td>
<td>RFC5280 (ASN.1)</td>
<td>RFC7519 (JWT)</td>
</tr>
<tr>
<td><strong>Governance</strong></td>
<td>VMC-GL, CABF BR, EVGL, WebTrust/ETSI Audit</td>
<td><strong>Needs to be defined</strong></td>
</tr>
<tr>
<td><strong>TTL</strong></td>
<td>1 year cert expiry</td>
<td>Short expiry</td>
</tr>
<tr>
<td><strong>Revocation</strong></td>
<td>CRL</td>
<td>Wait for expiry</td>
</tr>
<tr>
<td><strong>Transparency</strong></td>
<td>CT logs</td>
<td><strong>Needs to be defined</strong></td>
</tr>
</tbody>
</table>
Shortcomings: Recent EV attacks

● Stripe Inc of Delaware vs Kentucky

● "Identity Verified"

● Mistaken (or malicious) Issuance e.g. Symantec
Attestation - Verified Indicator Certificate/Token

Indicates validation by trusted Indicator Verifying Authority

- Organization is verifiable legal entity ⇒ validated legal entity registration
- Domain names are controlled by the organization ⇒ validated domain name
- Individual requesting validation is currently authorized to do so by the organization ⇒ validated authorization (audit records)
- Individual requesting the validation is who they say they are ⇒ validated subscriber (audit records)
- Organization has the rights to display the logo ⇒ validated proof of rights to indicator in jurisdiction
Registered Trademarks

Why? Objective means to test
  ● Logos
  ● Ownership
e.g. USPTO and EUIPO registrations (as starting points)

Requirements
  ● Public records
  ● Review with opposition
    ○ "Likelihood of confusion" test
    ○ Objectionable and misleading content
  ● Adjudication process
Logotype in Attestation

- Logo as SVG validated by IVA
  - As specified in [RFC6170 section 5.2](https://tools.ietf.org/html/rfc6170#section-5.2)
    - SVG Tiny profile
    - No JS
    - No external resources
- Jurisdiction
- Name (optional) also validated
- Multiple logos/names for internationalization support
  - Open question?
Recent EV attacks and Potential Remediations

- Stripe Inc of Delaware vs Kentucky
  - National jurisdiction
  - Transparency? (w/preview?)

- "Identity Verified"
  - Registry review process for misleading indicators (maybe)
  - Transparency? (w/preview?)

- Mistaken (or malicious) Issuance e.g. Symantec
  - Transparency? (w/preview?)
Certificate Transparency (RFC6962)

- Transparency to issued certificates
  - If there's a problem helps determine definitive scope of problem
- SCT in extension
  - Receivers checks for presence of SCT
- Integrity of CT log
  - Objectionable content checked by registration
  - Removal of expired or adjudicated trademark content—What!? 
- Token Transparency?
  - Log all the tokens? Short lived tokens flood the log.
Abuse Vectors
Abuse vectors

Lookalike Indicators

● [Very Scary] Lookalike indicator on lookalike domain
  ○ ub3r.com with the same or similar logo to Uber’s

● [Less Scary] Similar legitimate indicators (eg Paypal vs. Pandora)
  ○ Not a phishing or abuse vector
  ○ If there's a conflict, courts 😬

Poor Authentication

● [Semi Scary] If you screw up your auth, anyone could use your logo
Publishing: draft-blank-bimi
Validation: Transparency mechanisms
Consumption: draft-blank-bimi
draft-brotman-bimi-guidance
Reporting: feedback to ensure the previous mechanisms are working
Remediation
THANK YOU!
APPENDIX
50,000 foot

DMARC is the policy a domain owner wants a receiver to take when it receives mail that does not authenticate.

BIMI is the logo policy a domain owner wants a receiver to display when mail is received which does authenticate.

For a logo to be display, the mail must authenticate via DMARC and a validated logo must be provided via BIMI.
## logo types

<table>
<thead>
<tr>
<th></th>
<th>Threats and concerns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered</td>
<td>Jurisdictions differ; trademarks are siloed and not anti-phishing</td>
</tr>
<tr>
<td>Common Use</td>
<td>Lookalikes, jurisdictions, accidentally creating a new type of registry</td>
</tr>
<tr>
<td>New/Rebranded</td>
<td>Same as Common Use but much easier to abuse</td>
</tr>
<tr>
<td>Mildly Altered</td>
<td>Human attestation that alteration is mild</td>
</tr>
<tr>
<td>Multiple</td>
<td>Obscuring logos could be a cause of lookalikes</td>
</tr>
<tr>
<td>Derivative</td>
<td>Obscuration, human attestation</td>
</tr>
<tr>
<td>Co-marketed</td>
<td>Obscuration</td>
</tr>
<tr>
<td>Franchisee</td>
<td>Expiration / termination of franchise</td>
</tr>
</tbody>
</table>
Current Proposal: Consumption


- MTAs validate authentication, validate BIMI
  - DMARC validation: Domain at reject/quarantine and message passes
  - BIMI validation: Headers, record, hash from third party matches
  - Store message on BIMI-compliant mail store, with appropriate tag
  - BIMI-compliant MUA fetches message, displays from cache

- Receiver policy might have additional considerations for display:
  - TLS
  - Site-specific list of domains or trusted third party validators
  - Country of origination
  - Input from external sources/vendors
Spoofing and Content Risk

- 3rd party review to prevent spoofing
- validate content of image and names
Transparency with Preview and Removals

- Proactive indicator review process to prevent mis-issuance?
  - Traditional CT is retrospective only

- Automated fast reviews with monitors
- Complaints stop issuance
  - Allow more time for manual review
  - Start legal adjudication if necessary

- Removal of expired or adjudicated content
  - Don't want CT owner to arbitrarily remove content
  - Complaints justify removals

- Future work?
Validation Open Questions

● X.509 vs JWT?
  ○ JWT transparency?
● Automate binding trademark and domains to tokens?
● Internationalized logos/names?
● Review and removal trademark from CT logs?