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

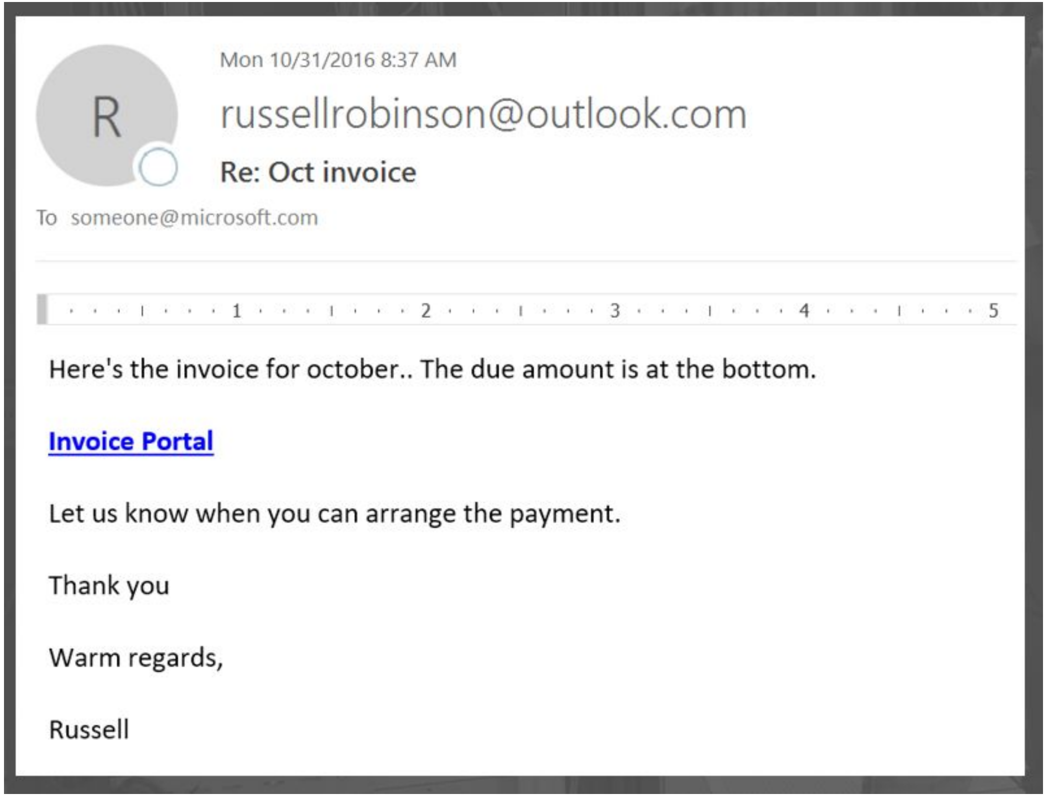
3. **Current Proposal**
   a. Shortcomings
   b. Proposal and requirements
   c. VMC / JWT API
   d. Abuse Vectors

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

OVERVIEW

1. WHY DO THIS?
2. USE CASES + IMPLEMENTERS
3. WHY COME TO THE IETF?
4. COMMON CONCERNS

Context: Auth Helps



Mon 10/31/2016 8:37 AM

russellrobinson@outlook.com

Re: Oct invoice

To someone@microsoft.com

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

Invoice Portal

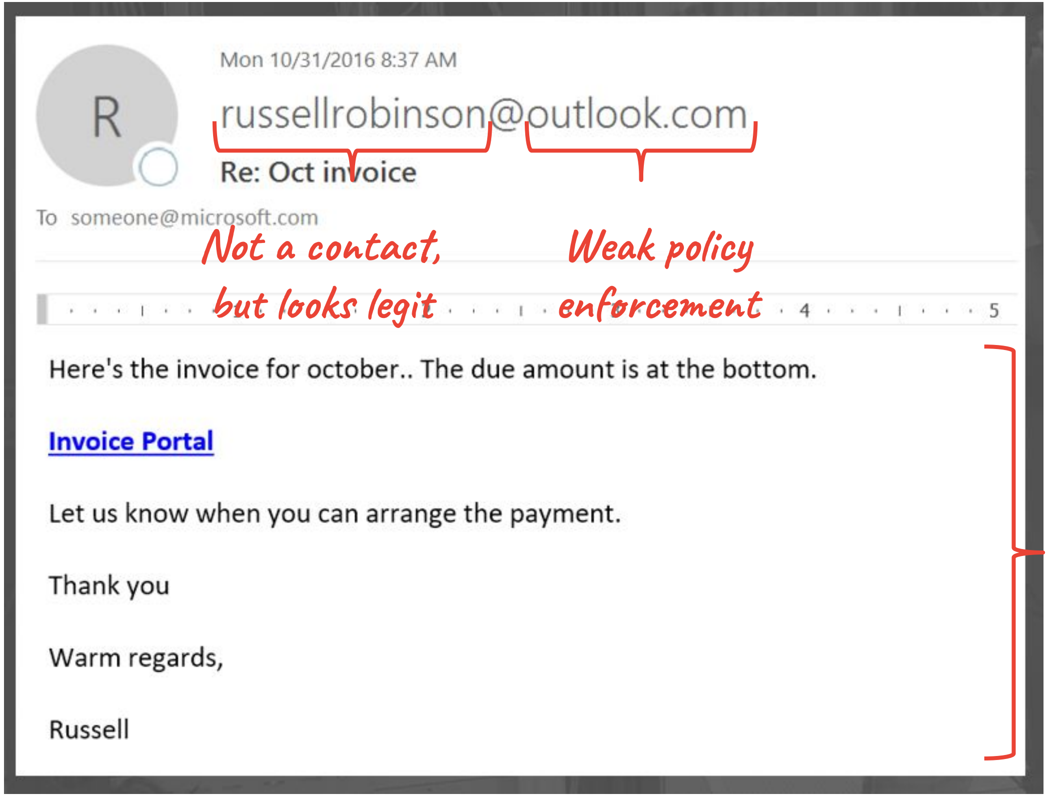
Let us know when you can arrange the payment.

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

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

Not a contact, but looks legit

Weak policy enforcement

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- Quickly outdated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) 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

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

Validation Options

	Reputation	Centralized Registry	Third Party	Sender
Participation	Large senders	Registered marks	Most senders	Everyone
Initialized/ Openness	No- history based / Closed proprietary	Yes / Partial	Yes / Yes	No / Yes
Standardization Effort	Low	High	Medium	Low
Cost	Receiver pays	Maybe: Owner pays	Yes: Owner pays	None
Weaknesses	Reputation hijacking	Inconsistency and participation	Weak/corrupt validation	😱

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

https://tools.ietf.org/html/draft-blank-ietf-bimi-00

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

	CA issued certificate	Validator API
Standard	RFC5280 (ASN.1)	RFC7519 (JWT)
Governance	VMC-GL, CABF BR, EVGL, WebTrust/ETSI Audit	**Needs to be defined**
TTL	1 year cert expiry	Short expiry
Revocation	CRL	Wait for expiry
Transparency	CT logs	**Needs to be defined**

Shortcomings: Recent EV attacks

- Stripe Inc of Delaware vs Kentucky

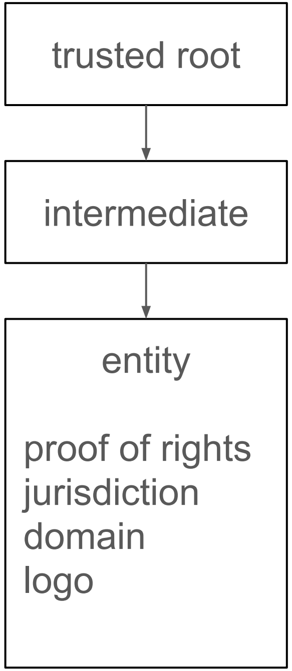
- "Identity Verified"

- 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



trusted root

intermediate

entity

proof of rights
jurisdiction
domain
logo

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
    - 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

DISCUSSION

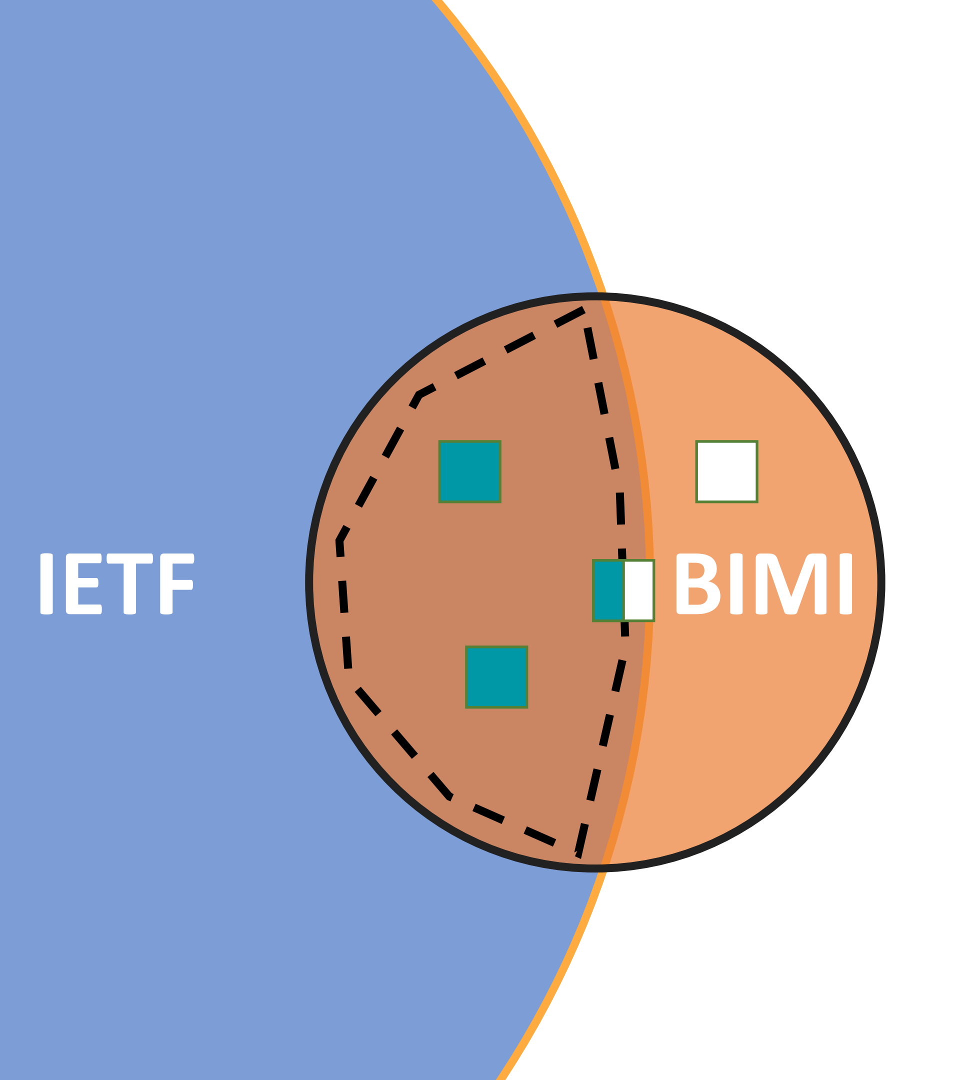
OUTCOMES

LOGO ATTACKS

OTHER THREATS

GLOBAL ACCESSIBILITY

IETF APPETITE FOR STANDARDIZATION



■ **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

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

Current Proposal: Consumption

https://datatracker.ietf.org/doc/draft-brotman-ietf-bimi-guidance/

- 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?