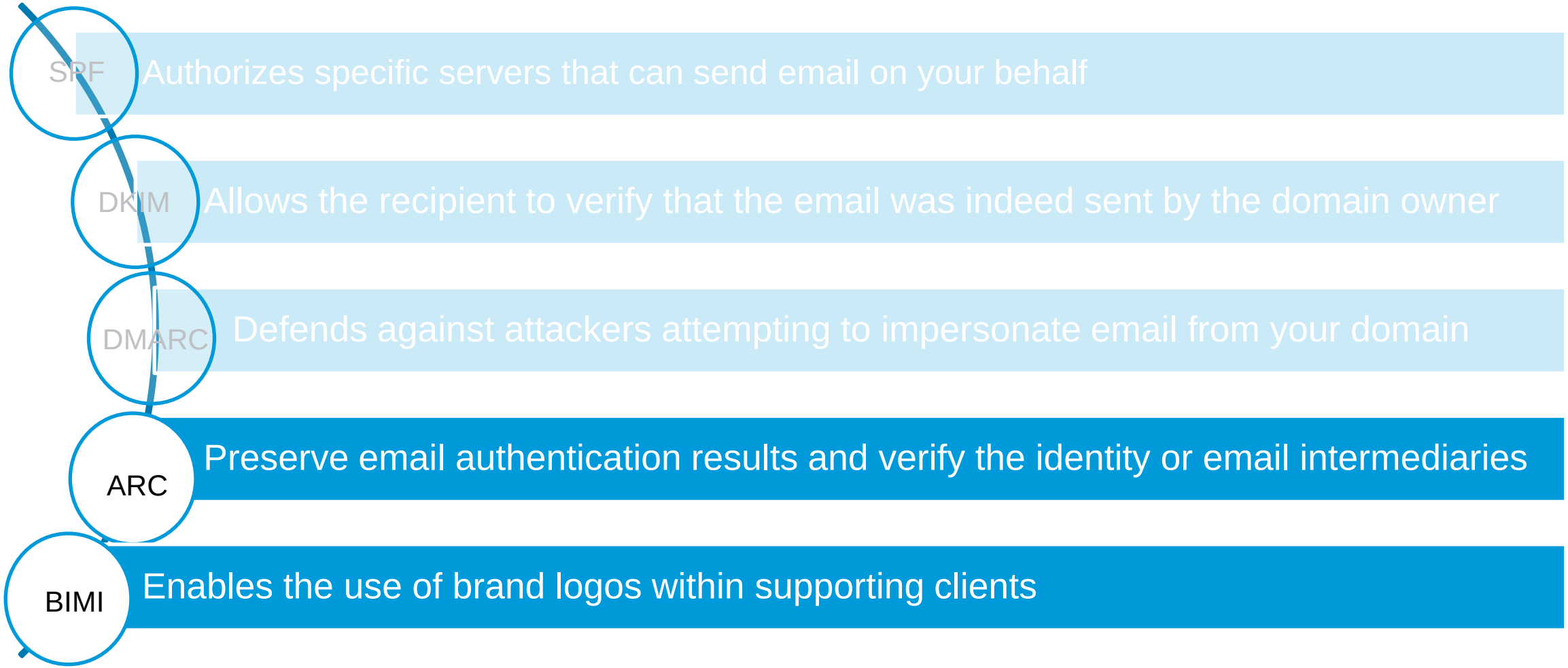
proofpoint®

Future of Email Authentication

November 2022

Hackim Farrell, Dir Product Management

Email Authentication Standards



ARC

proofpoint.

What is ARC?

Authenticated Received Chaining (ARC) is a specification designed to address the problem of DMARC verification being broken by an email intermediary sender.

Problem: Intermediaries can break DMARC verification when handling the message and re-sending it

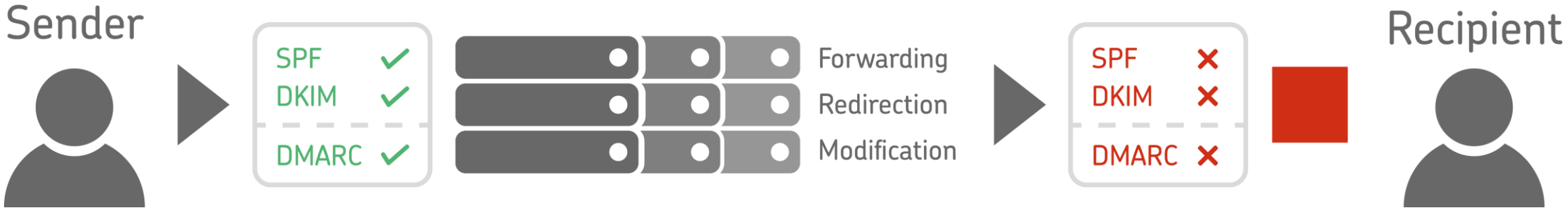
What are intermediaries?

- Systems that receive an email, process it, then re-send it to final recipients as if it came directly from the original sender.
- Example: Email from O365 to Proofpoint(scan for malicious content) delivers to recipient

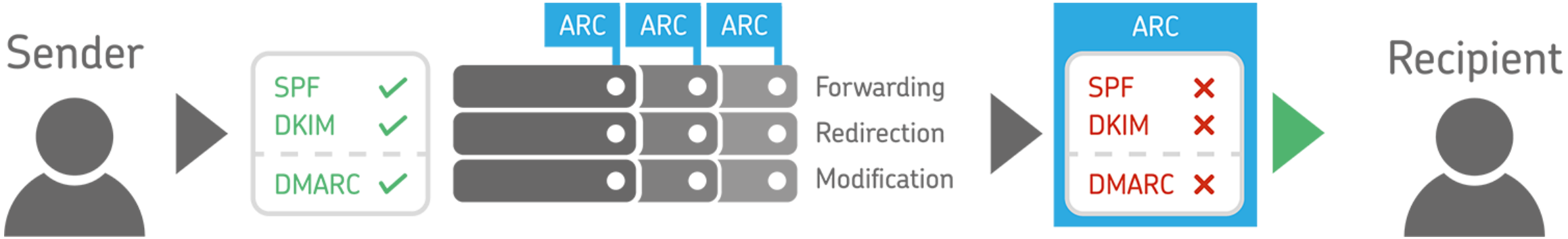
Solution: Intermediaries can can assert their authentication results when received for evaluation by subsequent receivers

ARC: *How It Works*

The SPF and/or DKIM check fails and also results in the DMARC validation fail



The ARC signing preserves the previous successful SPF and DKIM checks, resulting in delivery

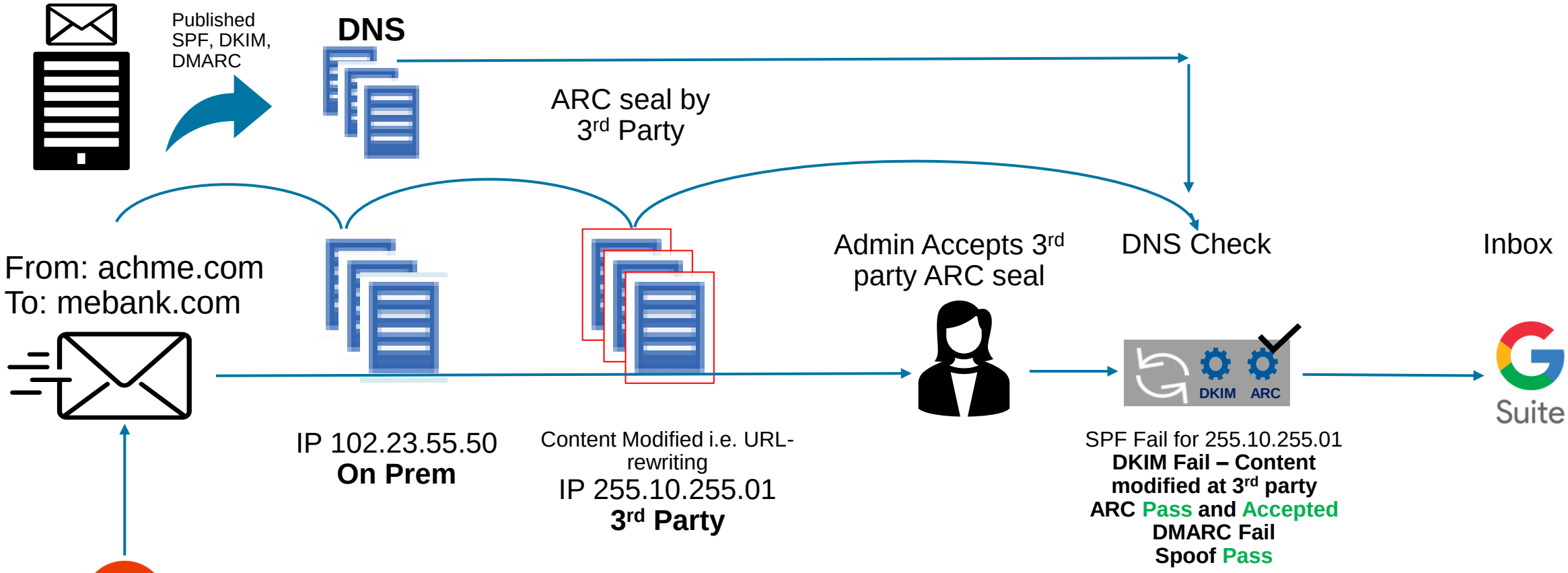


proofpoint.

ARC: *Who Should be Interested*

- To protect your domain against spam and phishing you set DMARC with a security policy of **“reject”**
- To improve the **legitimacy** and **compliance** of your emails
- The domain uses **intermediaries to scan and protect your incoming email** from malicious content and they perform things such as URL-rewriting

ARC: *ARC Seal mailflow*



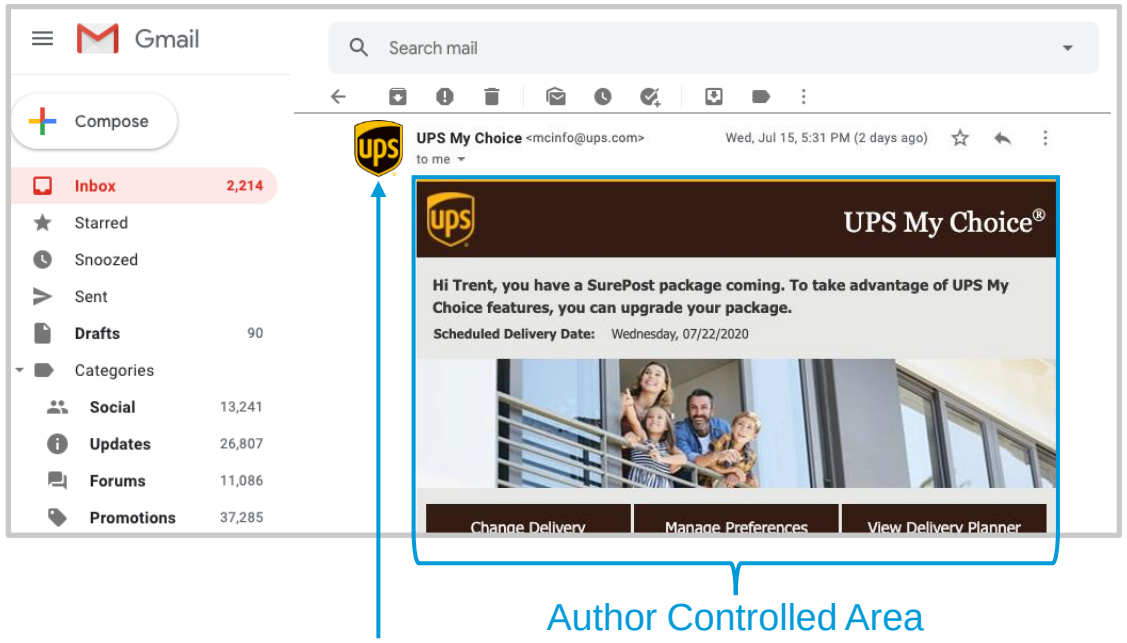
proofpoint.

BIMI

proofpoint.

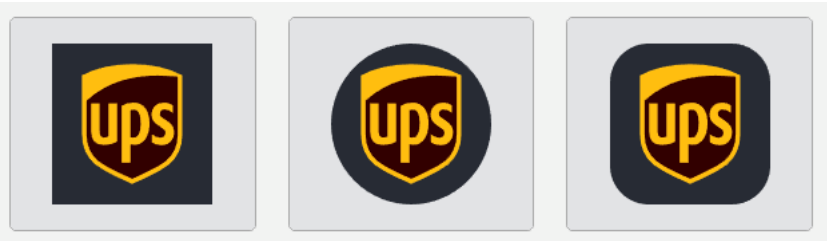
What is BIMI?

Brand Indicators for Message Identification or BIMI *(pronounced: Bih-mee)* is an emerging email specification that enables the use of brand-controlled logos within supporting email clients. BIMI leverages the work an organization has put into deploying DMARC protection, by bringing brand logos to the customer's inbox. For the brand's logo to be displayed, the email must pass DMARC authentication checks, ensuring that the organization's domain has not been impersonated.



Standard Mode Examples:

Dark Mode Examples:



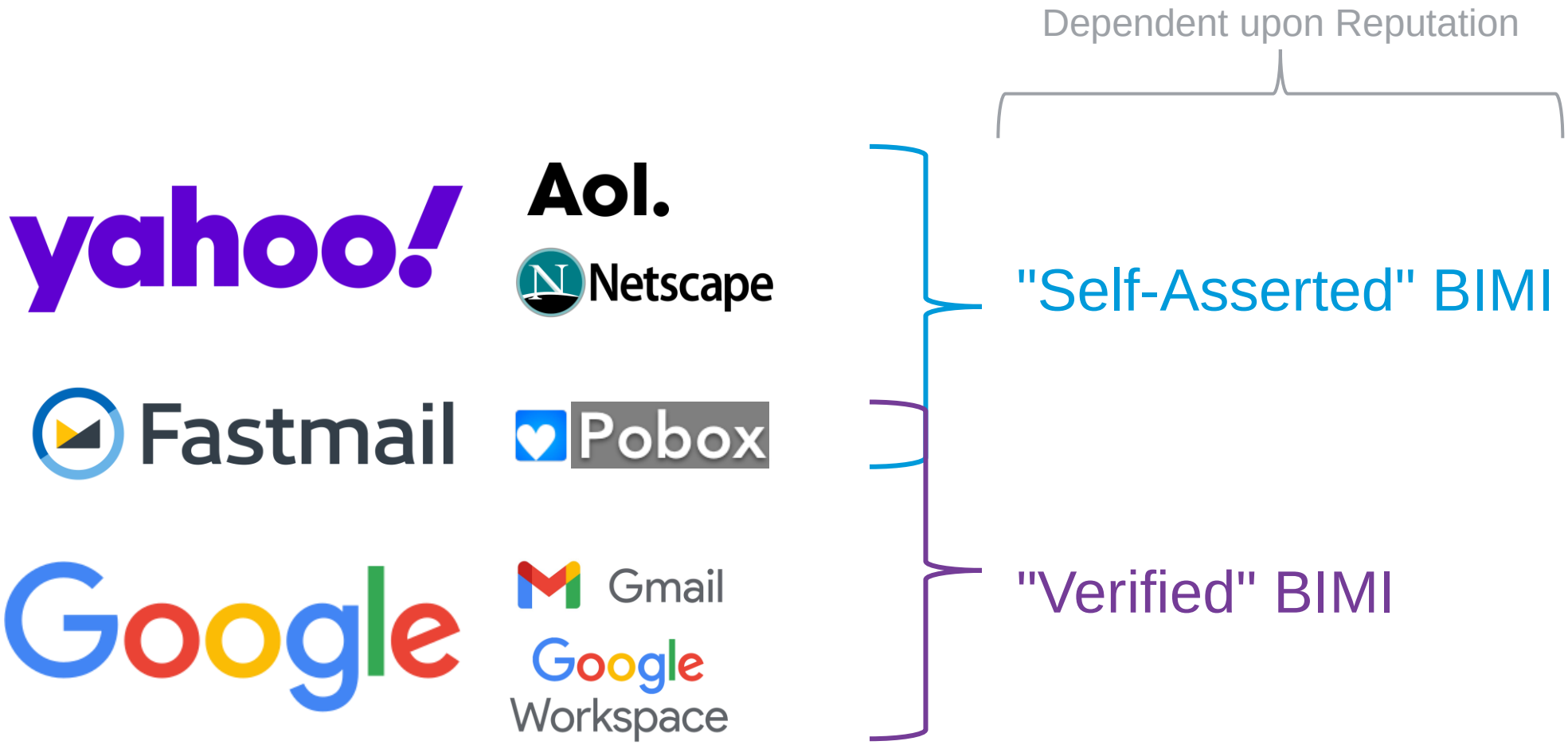
** These examples use a transparent background.*

BIMI: *Current + Planned Adoption*

Currently Supporting BIMI

Planning to Support BIMI

BIMI: *What Mailbox Providers Support It?*



BIMI: *Who Should be Interested*

- All domains that have a **consumer-recognizable logo** should be interested in deploying BIMI.

- Mailbox providers focused on serving end consumers. As such, early adoption of BIMI is likely limited to domains that send large volumes of email to consumers.

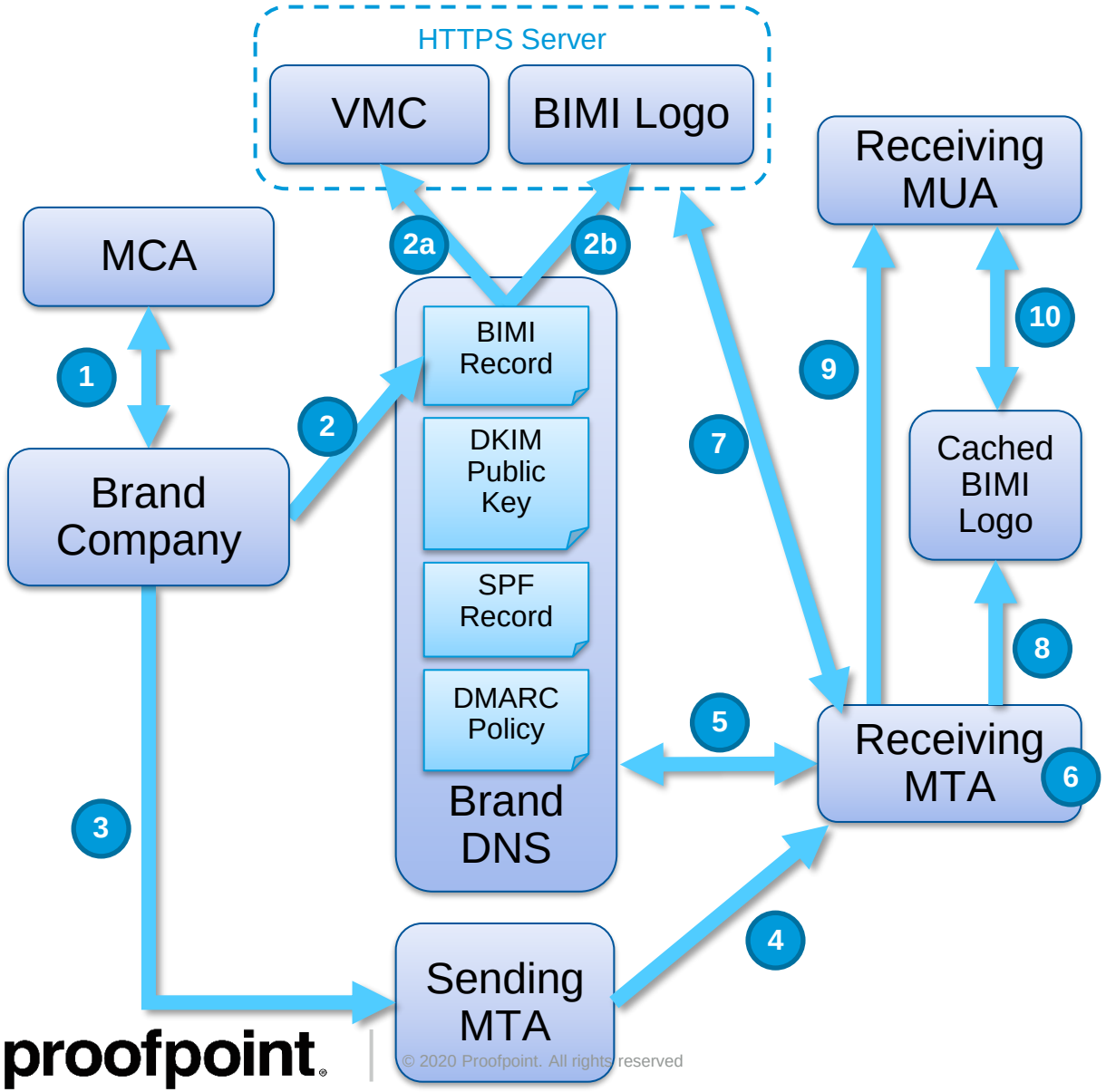
- Enterprise domains that focus primarily on sending business-to-business email are unlikely to be interested in early adoption of BIMI.

- Customers that have already published **DMARC “quarantine”** or **“reject”** policies, or intend to.

BIMI: *Terminology*

- **Brand Indicators for Message Identification** *(BIMI)* – Specifications and processes that define how authorized images can be associated with a domain, verified as legitimate by mailbox receivers, and displayed by mail user agents.
- **Certificate Authority** *(CA)* – The only organizations currently recognized to act as an MVA and issue VMCs. Currently limited to Digicert and Entrust
- **Mark Verifying Authority** *(MVA)* – The entity that is recognized to issue VMCs. While only select CAs are currently authorized to issue VMCs, the BIMI specification itself doesn't require that an MVA be a CA (e.g. Proofpoint may be authorized to act as an MVA for our customers).
- **Verified Mark Certificate** *(VMC)* – The document issued by the MVA indicating that the proffered image is authorized for use with BIMI. The VMC is currently defined as a profile of a typical Extended Validation (EV) X.509 Cert stored in Privacy Enhanced Mail (PEM) format.
- **Scalable Vector Graphic** *(SVG)* – A graphic format represented by vectors and stored as an XML document.
- **X.509 Certificate** *(Cert)* – A standard format for presenting public key certificates that are used in many Internet protocols (e.g. TLS, HTTPS). When issued by a recognized CA, they act as a trust anchor. In most cases they are invisible to the end user, but in some cases they provide visual trust indicators (e.g. EV Certs).

BIMI: *Operational Flow*



1. **Brand Company** applies for a **VMC** from the **MCA**.
2. **Brand Company** places a **BIMI Record** in the **Brand DNS**, pointing to the
   a. **VMC** and
   b. **BIMI Logo** published to an HTTPS server.
3. **Brand Company** triggers email to be sent by its own **Sending MTA**, or via a vendor sending on their behalf.
4. **Sending MTA** authenticates and sends the email on behalf of the **Brand Company** (optionally identifying the specific **BIMI Logo** to be used).
5. **Receiving MTA** checks the **Brand DNS** for the **SPF Record**, **DKIM Public Key**, **DMARC Policy** and **BIMI Record**.
6. **Receiving MTA** verifies the authenticity of the email using **SPF**, **DKIM**, **DMARC.**
7. If the email is verified, **Receiving MTA** retrieves and verifies the **VMC** and retrieves the **BIMI Logo**.
8. **Receiving MTA** stores the **BIMI Logo** in a local cache to be served to the **Receiving MUA**.
9. **Receiving MTA** passes the message along to the **Receiving MUA**, indicating that the message authenticated and can display the referenced **BIMI Logo**.
10. **Receiving MUA** retrieves and displays the **Cached BIMI Logo**.

proofpoint.

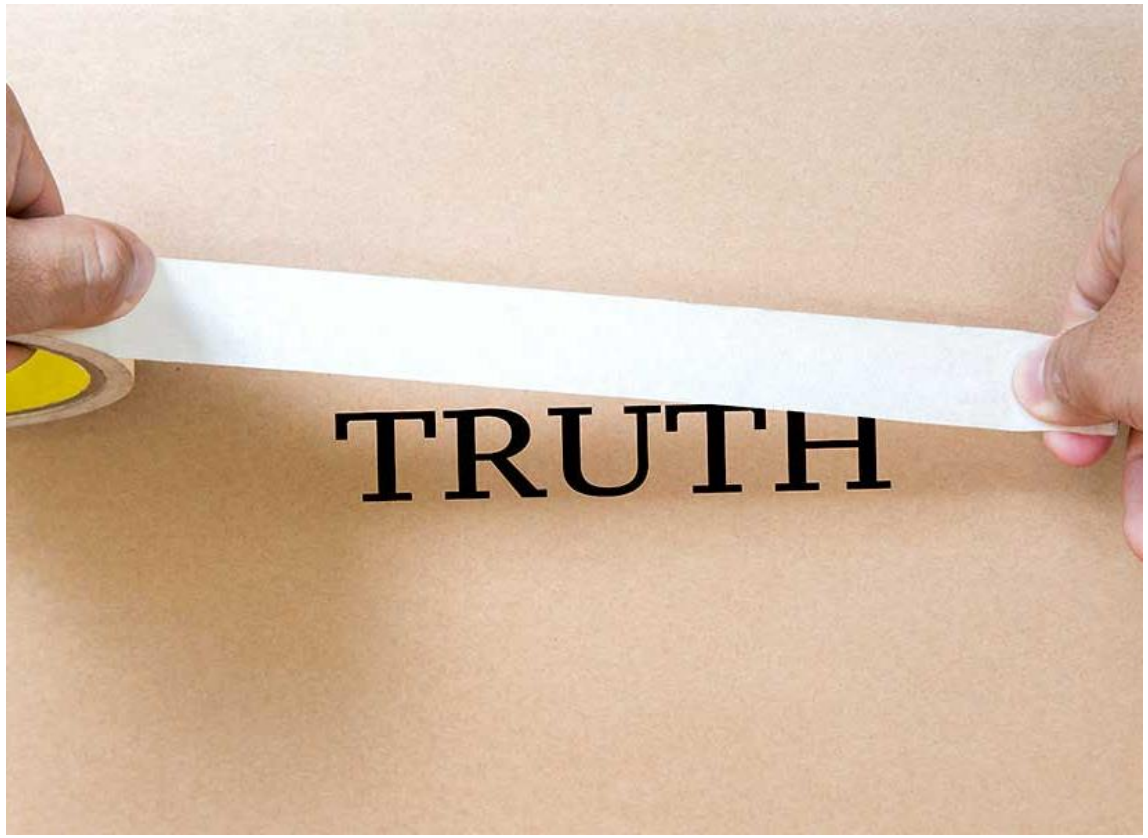
BIMI: *VMC Requirements*

- VMCs are offered by two MVAs: Digicert & Entrust
  - Accepted Jurisdictions: US, Canada, EU, UK, Germany, Japan, Australia, and Spain
- The logo must be a registered “Design Mark” (not a “Word Mark”).
- The logo must be saved in a specific SVG Portable/Secure format.
- The SVG logo and VMC must be served from a secure web server via HTTPS.
- The customer must publish a BIMI TXT record at their sending domain that point to the SVG logo and VMC document.
- The FQDN sending the email, the organizational domain, and all subdomains must be covered by a DMARC “reject” (or 100% "quarantine) policy.

BIMI: *Misconceptions*

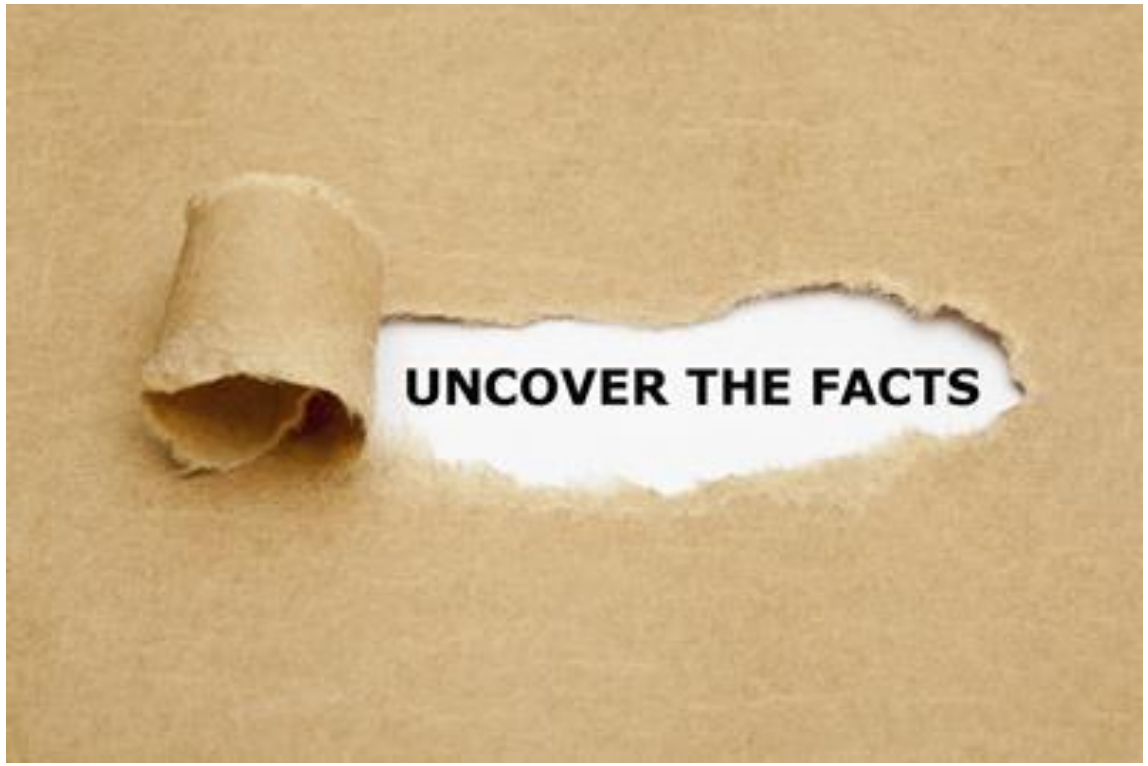
- **Myth:** BIMI is a security technology.
- **Truth:** BIMI is a marketing tool designed to
  - provide the brand control over the logo being displayed with email sent by their domains,
  - improve brand engagement within the mailbox, and
  - drive stronger email authentication.

BIMI: *Misconceptions*



- **Myth:** Users make decisions whether to trust an email based on visual indicators.
- **Truth:** Users do not change their behavior based on visual trust indicators.

BIMI: *Misconceptions*



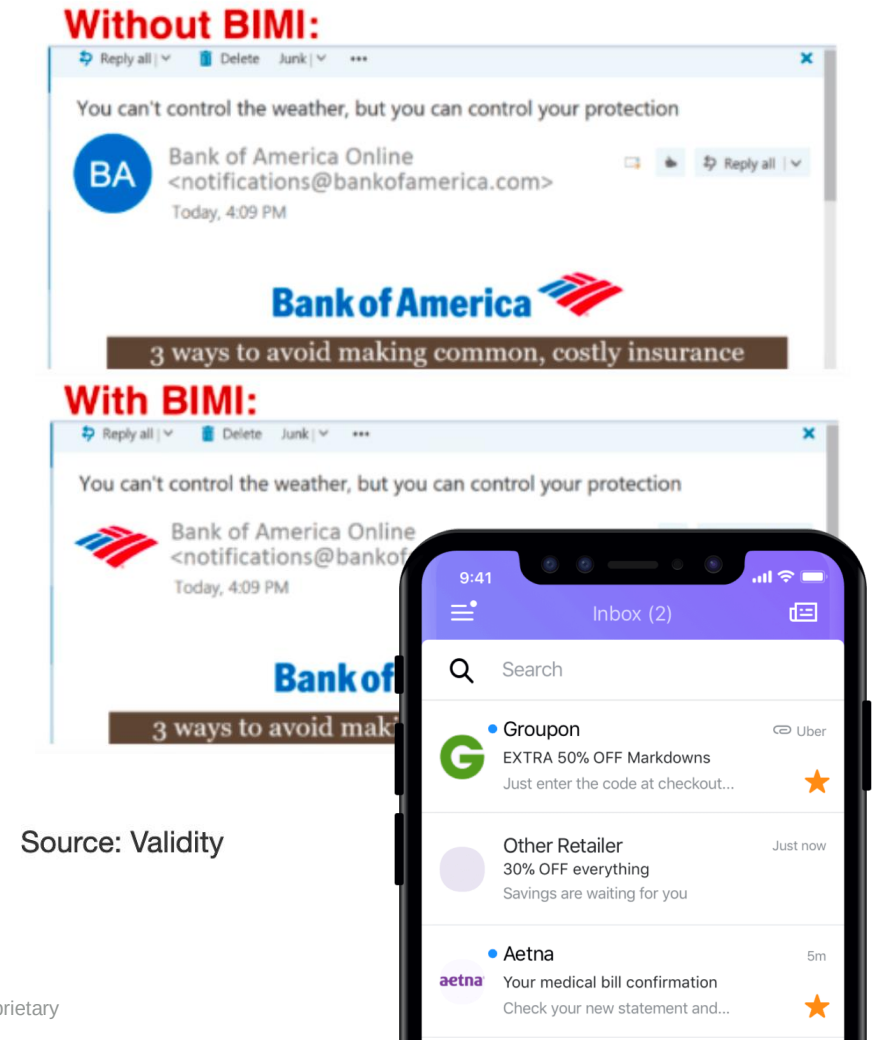
- **Myth:** BIMI logo once published will automatically be displayed.
- **Truth:** BIMI logo will only be displayed if
  - the mail client supports BIMI, and
  - the sender has sufficient positive reputation for the client to decide to display the logo.

Inbound BIMI Validation (Cloudmark Support Example)

Brand Indicators for Message Identification (BIMI)

Released

- Benefits
  - Enables brands to control the logos to be displayed in association with authenticated email.
  - Provides opportunity for brand engagement within the inbox.
  - Helps brands drive adoption of secure authentication protocols.



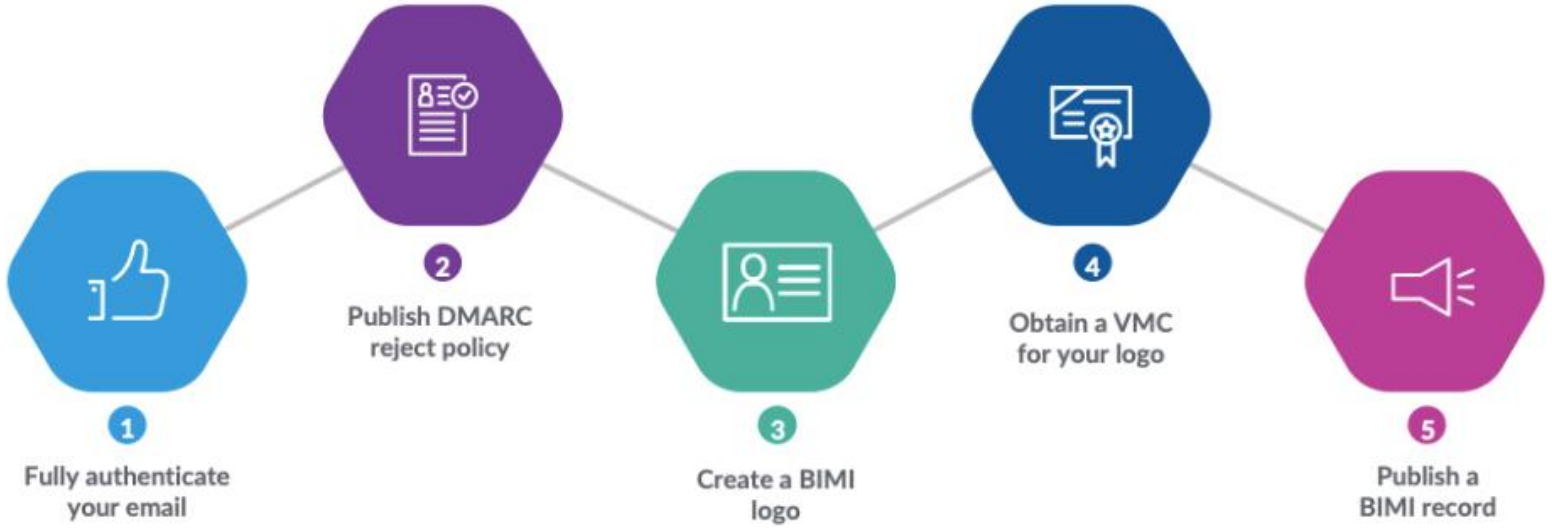
Source: Validity

Inbound BIMI Validation (Cloudmark Support Example)

Released

Brand Indicators for Message Identification (BIMI)

- How it Works
  - Leverages SPF, DKIM, and DMARC for sender validation as part of the MTA workflow
  - If DMARC passes, BIMI records are validated
  - If BIMI validation passes, authentication headers updated
  - The mailbox provider or email client can determine if the sender has high enough reputation to display logo.



proofpoint.