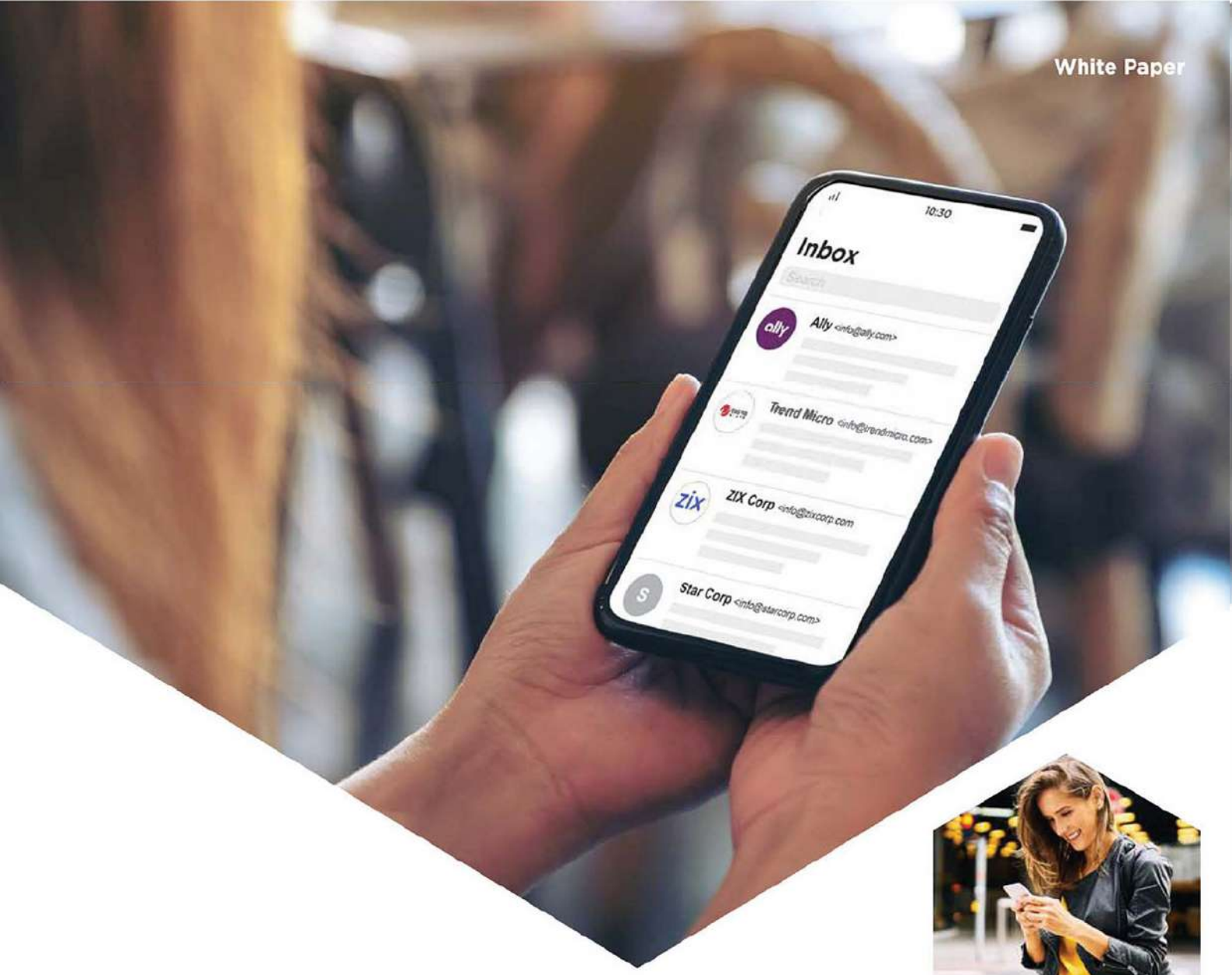
White Paper



Rethink Your Outbound Email Strategy- Display Your Brand Logo on Emails

Here's what you need to know about the BIMI standard and technology behind it

INDUSFACE™

ENTRUST
SECURING A WORLD IN MOTION

Table of Contents

INTRODUCTION

Finding a ubiquitous way to authenticate email has been confounding IT groups for years. Organizations that use Domain-based Message Authentication, Reporting, and Conformance (DMARC) protection can help solve this problem.

BIMI (Brand Indicators for Message Identification) was created to help accelerate DMARC adoption by offering an incentive to adopt properly implemented DMARC, which can enable an organization's verified logo to appear in email messages. To use BIMI at the highest level of validation, organizations are required to use a Verified Mark Certificate (VMC) from an authorized certification authority (CA), which works alongside an organization's DMARC protocol policy. There are two ways for email service providers to display a logo alongside email messages 1) link to an SVG file or 2) with a verified logo that is embedded in a cryptographically signed VMC.

Mailbox providers like Google now support VMCs to convey these organizational logos in their Gmail platform. VMC requires four checks to enable the logo to display: 1) that brand logos be verified against trademark registration authorities by a CA, then 2) authenticated using a high assurance validation process plus 3) a notary validation process, and 4) have a DMARC policy set to reject or 100% quarantine. Once verified, the process results in the issuance of a VMC, and a registered logo automatically appears on mailbox providers that support it.

VMC brings with it three unique qualities:

- Ability to show an organization's registered trademark logo alongside emails appearing in the participating receiver's inbox
- Control of the logo that displays in these participating receiver inboxes
- Cultivate immediate brand recognition for an enhanced user experience

Read on to learn how you can show your brand logo on email communications.

BIMI history and players

BIMI is a standardized way for inboxes to receive brand logos to display in email messages. It is the culmination of an industry-wide standards effort brought about in collaboration with: email service providers, CAs, DMARC providers, and other stakeholders to establish the use of brand logos as indicators for email communication, while giving IT and marketing teams a new opportunity to elevate their email strategy by putting their brands in front of consumers.

BIMI was initiated with an effort to insert an unverified SVG file of a brand logo alongside email messages protected by DMARC technology. Contributors to the BIMI standard raised some concern that employing an unverified logo could lead to nefarious activity, and therefore it failed to gain traction with some of the email service providers. The VMC was created to bring legitimacy to the logo inserted into the BIMI record and has since proven to be a key accelerator to BIMI adoption.

In 2017, a leading CA, Entrust proposed to Google and other members of a group called the AuthIndicators Working Group – a group of companies representing the email ecosystem including mailbox providers, security companies, Entrust and others – a new type of digital certificate that would contain cryptographically verifiable brand information for use by mailbox providers and others. During this development period, Entrust helped guide this new offering to market, created the first version of the VMC Requirements, and issued the world's first VMC to a customer during a Gmail pilot program.

These organizations continue to collaborate on creating a richer, more trustworthy inbox experience for all email users worldwide, while increasing the use of authentication to reduce email fraud. BIMI is a standard that enables brands to showcase their brand identity in outbound emails, so long as both the email and the registered logo are properly verified along with the proper DMARC protocol, giving brands a powerful opportunity to build a more immersive email experience with consumers.

Let's take a look at the key technology partners for BIMI.

DMARC providers

One of the main components of BIMI authorization is the DMARC provider. Domain owners are required to have a specified DMARC policy set to *100% quarantine or reject* to prevent email domains from being spoofed, protecting your domain from unauthorized use. Agari, Red Sift, Validity, and Valimail support the BIMI standards and are top players in the DMARC space.

Mailbox providers

Google is the largest provider of business-to-consumer email and is the mailbox provider spearheading the current BIMI standard - this effort requires the use of a high assurance VMC along with an SVG file of the brand's registered logo, and DMARC technology. Google, a proponent of secure-by-default experiences, announced their general support for the BIMI standard in Gmail in July 2021 following a successful pilot program stating, "BIMI provides email recipients and email security systems increased confidence in the source of emails, and enables senders to provide their audience with a more immersive experience."

Verizon Media, on the other hand, was the first email technology company to begin a BIMI trial across all web and mobile Yahoo Mail properties in 2018. This initial BIMI trial took place prior to the new standard, which requires the use of a high assurance VMC. "We saw two immediate benefits as the result of our BIMI beta in Yahoo Mail," said Marcel Becker, Director of Product Management for Verizon Media. "We were able to provide better and more accurate brand logos as part of our consumer mail experience and BIMI clearly provided an incentive to accelerate the adoption of DMARC among those brands. Expanding the adoption of BIMI beyond that beta will be a clear win for senders and consumers."

For maximum compatibility including Gmail support, the recommendation is to adopt the full BIMI standard, which requires the use a VMC.

Certification Authorities

Another key technology provider necessary for the implementation of BIMI is the CA.

A CA that issues VMCs can provide the requirements that meet the BIMI standards. The CA is responsible for vetting the applicant to validate the information provided for verification. Digital certificates are commonly used to verify jurisdiction and website domains, and a lot of organizations already use them. A leading CA like Entrust verifies and issues digital certificates for an applicant who may not already have an active one in service. The CA can also validate the existence of a registered trademark, which once confirmed, can issue a VMC completing the process for BIMI implementation.

What is a VMC?

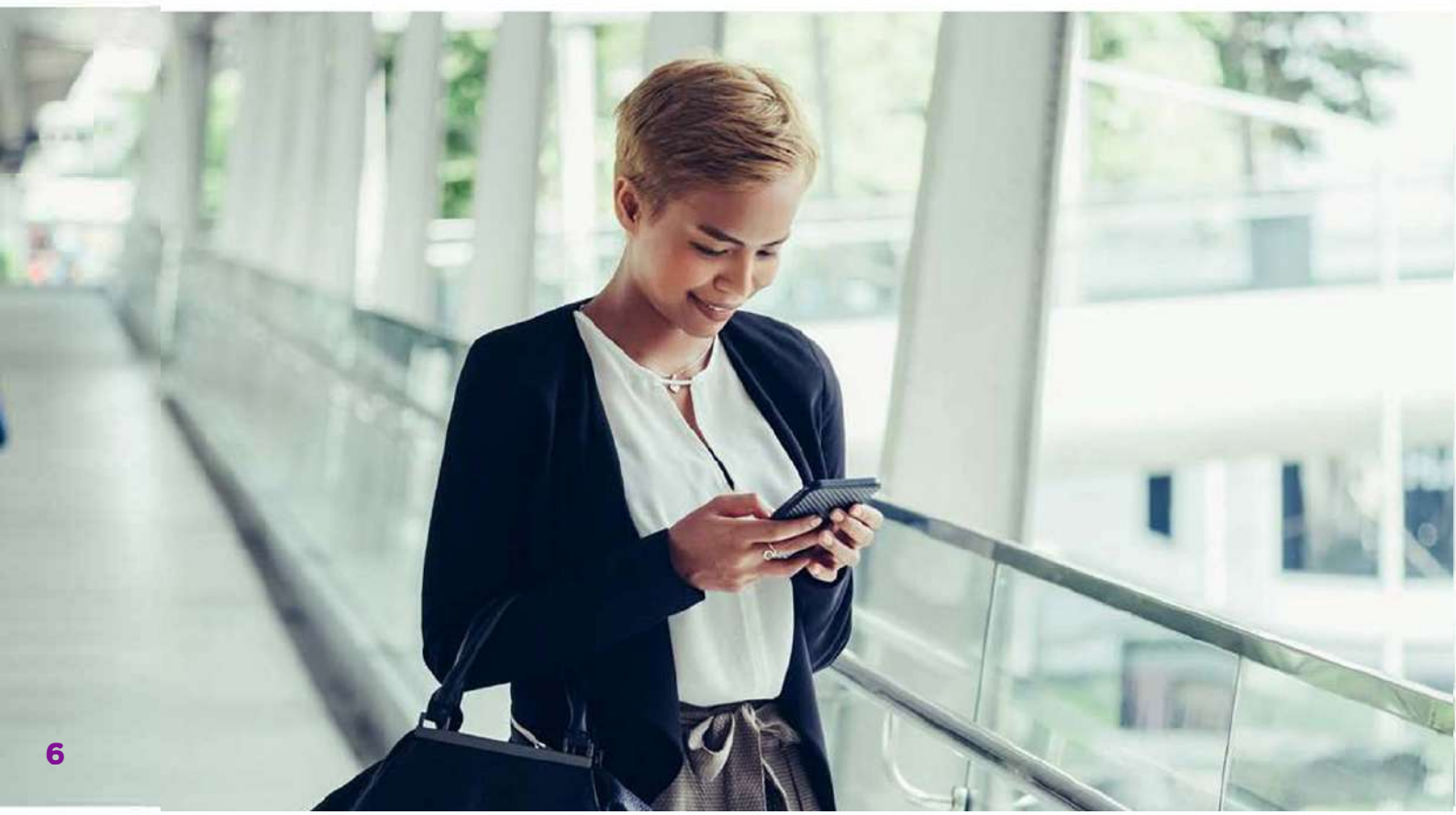
Digital certificates have been used for decades to identify people, devices, organizations, and other entities in the digital world. Verified Mark Certificates (VMCs) can be leveraged by various players in the digital ecosystem to provide identity and trust for organizations when sending emails out to their customers, partners, and users. VMCs include verified registered logos that are displayed in emails and along with DMARC can help to provide assurance to end-users regarding the origin and validity of the email as part of the new BIMI standard.

How does it work?

VMCs are issued by a CA who is responsible for performing an industry standard verification process on the organization and the applicant who is requesting the certificate on behalf of the organization. VMCs work by verifying the existence of a secure connection between a company domain and a particular sender-designated brand logo included within an email.

VMCs are built upon secure verification methods; when an applicant applies for a VMC, the process includes the following steps:

1. The issuing CA examines an organization's registered trademarks and confirms their registration and ownership by verifying it against local registration authorities.
2. All of the verified information, including the organization's legal business name, address, and registered trademark information will be included in the certificate once it is issued.



3. The verified certificates are signed cryptographically by the CA, allowing mail applications to rely on and trust the VMC.

4. Once the VMCs are issued, organizations must configure their domain DNS DMARC record policy to "100% Quarantine" or "Reject" mode and point to the issued VMC so that the verified organization information and logo can be applied to emails that are sent for the requested domain.

Only trusted CAs who comply with the VMC Requirements are trusted by mail applications.

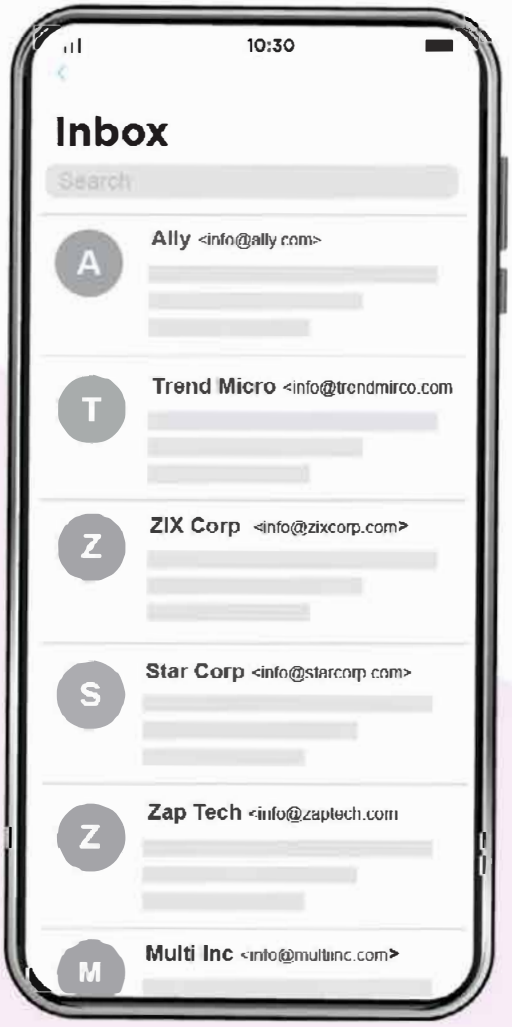
Here are the trademark offices currently used to verify trademarked logos:

Country/ Region	Trademark Offices Authorized for Verified Mark Certificates	String Value for a Trademark Under Sec. 4.5.2.4.1 and 4.5.2.4.2
United States (US)	United States Patent and Trademark Office (USPTO) uspto.gov/	US
Canada (CA)	Canadian Intellectual Property Office canada.ca/en/intellectual-property-office.html	CA
European Union (EM)	European Union Intellectual Property Office euipo.europa.eu/ohimportal/en	EM
United Kingdom (GB)	UK Intellectual Property Office gov.uk/search-for-trademark	GB
Germany (DE)	Deutsches Patent- und Markenamt dpma.de/	DE
Japan (JP)	Japan Trademark Office ipo.go.jp/	JP
Australia (AU)	IP Australia ipaustralia.gov.au/	AU
Spain (ES)	Spain – Oficina Española de Patentes y Marcas oepm.es/es/index.html	ES

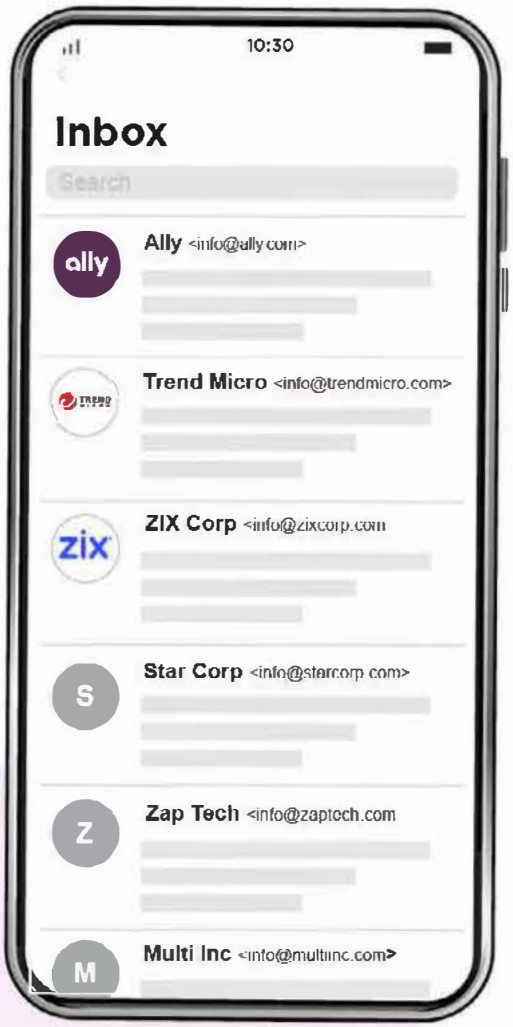
How are VMCs displayed?

VMCs are automatically displayed on mailbox providers, like Google, that support it once all of the required checks are in place.

Email without VMC



Email with VMC Properly Enabled



VMC enabled emails appear in the mailbox provider's avatar slot.

Why should I get a VMC?

VMCs help to bring a more personalized email experience for all companies by creating a more consistent and visually compelling email experience for both businesses and consumers.

By following the BIMI protocol, VMCs have:

- ability to show an organization's registered logo alongside emails appearing in the receiver's inbox
- control over the logo that displays with your organization's email messages
- opportunity to cultivate immediate brand recognition and enhanced user experience

Looking ahead

VMCs are a foundational technology that once set up could be leveraged for additional use cases. Looking into the future, it's possible to reimagine how brands can personalize their messages particularly on other platforms where brand impressions and identification can have a positive impact on consumer experiences.

Conclusion

VMC relies on organizations to put into place DMARC protection and high assurance verification to gain control over the logo displayed. VMCs provide maximum compatibility with mailbox providers that support BIMI's VMC standard. Once these checks are complete, your brand's registered logo will automatically appear in the mailbox provider's avatar slot, which can make your outbound emails stand out in a user's inbox.

Something to consider when planning for BIMI adoption is that the requirements for VMCs are well thought out and for some organizations, may require a noteworthy lead time to get one in place.

For more information

+91 9825496989
+91 265 6133011/316
jigar.shinde@indusface.com
indusface.com

ABOUT INDUSFACE

Indusface is a leading application security SaaS company that secures critical Web, Mobile & API applications of 3000+ global customers using its award-winning fully managed platform that integrates a web application scanner, web application firewall, DDoS &, BOT Mitigation, CDN, and threat intelligence engine. The company has been funded by Tata Capital Growth Fund, is Great Place to Work certified, mentioned by analysts like Gartner, Forrester, etc in their reports, and has been the recipient of many awards such as the Economic Times Top 25, NASSCOM DSCI Top Security Company, Deloitte Asia Top 100 , and several other such prestigious recognitions.

Learn more at

indusface.com

VADODARA | MUMBAI | BENGALURU | DELHI | SAN FRANCISCO | LONDON

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223