digicert®

VERIFIED MARK CERTIFICATES

Put your mark on email marketing—and your secure identity on display

Everyone uses email, every day. Which is exactly what makes it both extremely useful and especially prone to attack—particularly identity-targeted attacks like phishing. In fact, 96% of all phishing attacks use email as a delivery method, and 75% of global organizations were targeted in 2020.

Why? In large part, because organizations have lacked an effective means of immediately and concretely identifying themselves to users, nor has there been a reliable method to rapidly identify and isolate malicious content masquerading as a legitimate send.

Verified Mark Certificates (VMCs), in conjunction with BIMI and DMARC enforcement, change that dynamic, offering a new, highly visual avenue for brand promotion alongside strong phishing prevention measures that help to protect both the consumer and the organization from identity-targeted attacks.

How does verified email work?

DMARC enforcement + BIMI + VMC = Logo-verified Email

What are VMCs?

VMCs are a new, innovative type of certificate that allow companies to place a certified brand logo next to the "sender" field in customer inboxes—even before the message is opened. When you purchase a VMC, DigiCert® thoroughly validates the identity of the purchaser, including checking that the logo is officially trademarked.

See the approved list of trademark offices for VMC

What is DMARC?

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email authentication policy that builds on SPF and DKIM protocols. It adds linkage to the author, published policies for recipient handling of authentication failures, and reporting from receivers to senders in order to improve visibility and offer additional protection of the domain from fraudulent phishing and spoofing attacks.

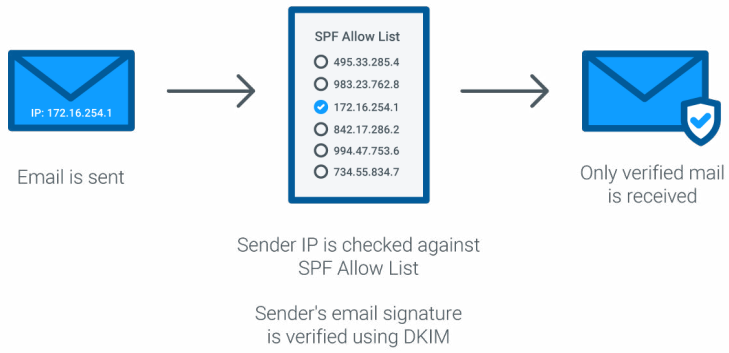
Download our step-by-step DMARC deployment guide

What is BIMI?

BIMI stands for Brand Indicators for Message Identification, and is an email specification that enables the display of brand logos within supporting email clients to encourage the widespread deployment of DMARC protection.

How do they work together?

Your organization's DMARC enforcement is validated by the email client via confirmation of your BIMI record and VMC-ensconced logo. If everything checks out, your logo is displayed, serving as a visual indicator of your message's authenticity, increasing engagement and building brand recognition.



Benefits to IT

Better visibility, security and control with DMARC

- Enhance security through DMARC enforcement
- Lower the risk of phishing attacks targeting you and your brand
- Get better visibility and control over the messages sent and received by your domain
- Gain clear insight into the types and frequency of attacks targeting your brand
- Ensure legitimate emails are delivered reliably—and are easily identifiable

Benefits to marketers

Take back the inbox

- Improve engagement by 10+%[1]
- Build brand awareness with every message you send
- Associate your brand with DMARC enforcement and improved email security
- Deliver a more authentic, trusted and memorable brand experience
- Visually differentiate your messages on the most effective and widely used medium

Benefits to consumers

Less phishing. More trust.

As more brands enforce DMARC, consumers can expect an overall decrease in the number of phishing emails that make it into their inboxes. This means less risk, less clutter and a better overall user experience.

Validation Requirements

In order to get a VMC, organizations must go through a series of validation procedures similar to getting an EV SSL. During the process, an individual's identity validation is required as well as face-to-face confirmation by a notary, lawyer or via a video call directly with a member of DigiCert's validation team. DigiCert's validation team will also have a video call with the applicant where they hold their ID in front of the camera. Finally, DigiCert must also validate that your logo is officially and legally trademarked and formatted correctly.

Learn how to put your logo into the correct .SVG format

Purchasing a VMC

VMC certificates can be purchased via CertCentral®.

Note: you must have an active account to complete the purchase.

Buy now

Installation

1. After you have submitted your SVG logo file to DigiCert, you will receive a file containing a PEM-encoded certificate chain
2. Both the SVG and the certificate chain file must be placed on a publicly accessible server and be accessible via https (HTTP will cause a failure)
3. You will then need to update your BIMI record with the correct URL and file location

Frequently asked questions

How many VMCs will I need?

This typically depends on the number of logos in use within your organization. See our blog post for more information.

May I use a wordmark instead of a logo?

Yes. You can choose to use a wordmark instead of a logo, however it must also be registered at a participating trademark agency.

How do I know if my organization is DMARC compliant?

Check to see if you're DMARC compliant here.

How do I check to see if I am trademarked, and where do I go to get approval?

Your logo must be registered with an approved trademarking body.

See our blog post for more information about the trademarking process

Which email client displays VMC?

Gmail, Yahoo, FastMail, Verizon, and more.

As VMCs are new, the list of supporting email clients continues to grow. See our website for the most up-to-date list.

What happens if I stop enforcing DMARC after the purchase of VMC?

Your certificate will remain valid, but your logo will not display. In order to continue to display your logo, you must be actively enforcing DMARC, as indicated by your BIMI record.

How often do I need to renew and re-validate?

Customers must renew their certificate every year. Once a customer has validated their organization, they will not need to go through the notarization process again, but they will need to re-validate every 398 days, similarly to a standard EV TLS/SSL certificate, and will need to log into CertCentral to renew the certificate.

We're an official organization, but our logo is not trademarked. Can we use a VMC?

Unfortunately, not at this time. Only officially trademarked logos will display.

Have more questions?

Learn more and get in touch at
https://www.digicert.com/tls-ssl/verified-mark-certificates