sectigo

DATASHEET

Verified Mark Certificates (VMC)

Increase inbox trust by displaying your registered logo

The authentication gap: Lack of trust in the inbox

Email remains the #1 digital communication channel for customer engagement, but it's also one of the riskiest vectors for cybercrime. Phishing attacks, business email compromise (BEC) fraud and brand impersonation scams have cost business a staggering $55 billion over the last decade, according to the United States Federal Bureau of Investigation (FBI).

With the explosion of this type of digital crime, it is no wonder that consumers are wary of fraudulent emails and are less likely to open emails that don't land in their primary inbox.

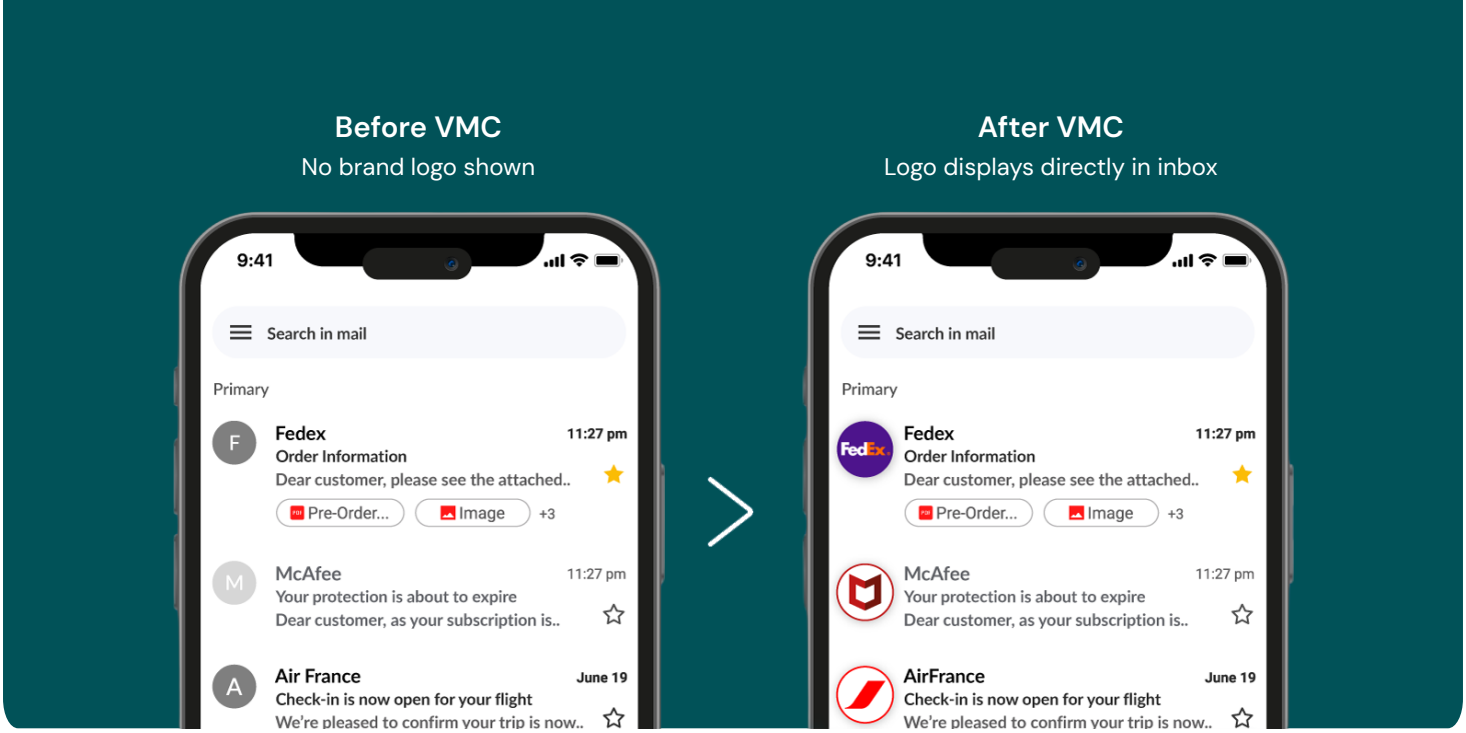
Benefits

- Defend your brand against impersonation
- Strengthen your defenses against phishing and spoofing
- Win the inbox wars with your registered logo next to your email
- Improve email deliverability rates and customer engagement

Bridging the gap with visual brand validation

How are brands combatting this trust issue? The answer is with Verified Mark Certificates (VMCs). A Verified Mark Certificate is a digital certificate that confirms an organization owns the rights to a specific logo. VMCs allow your organization to display your registered logo next to your emails in inboxes that support Brand Indicators for Message Identification (BIMI).

BIMI is the display mechanism that participating mailbox providers like Gmail (which displays a blue check mark to further validate legitimacy), Apple Mail and Yahoo use to display the trademarked logo. And VMC is the verified proof behind it.



Why VMCs matter for businesses

VMCs build on the investments you have made in email security and authentication technologies like Domain-based Message Authentication Reporting Conformance (DMARC), which works in the background to prevent attackers from sending fake emails using your domain and tell incoming servers how to handle faked emails. But these controls are not visible to the recipient, and this lack of trust can deter customers from opening legitimate emails.As inbox providers, such as Gmail, Apple Mail and Yahoo evolve toward authenticated, email-first user experiences, VMCs are no longer an option.

Without VMCs, brands risk:

- Falling behind competitors who display their verified logo and gain inbox prominence.
- Being perceived as less trustworthy or outdated.
- Suffering lower open and click-through rates, undermining email marketing ROI.
- Missing out on the Gmail blue checkmark program — a clear differentiator tied directly to VMC and DMARC.

With Sectigo VMCs you can build digital trust signals that can help you drive higher email engagement:

- Achieve Gmail blue checkmark to instantly differentiate your brand
- Advance your sender reputation and domain health
- Improve email open rates, brand recall and purchase likelihood
- Align email experience with your trusted website experience

Sectigo: The Smart Choice for VMCs

Easy self-service purchase through Sectigo.com

Other providers make you wade through lengthy procurement cycles.

Built-in validation

Sectigo provides proactive validation tracking so that your team can address issues immediately.

Multi-domain support

Easily purchase additional domains to support complex email architectures.

Guided onboarding

Clear support content, including onboarding checklists and FAQs.

Simple, clear pricing

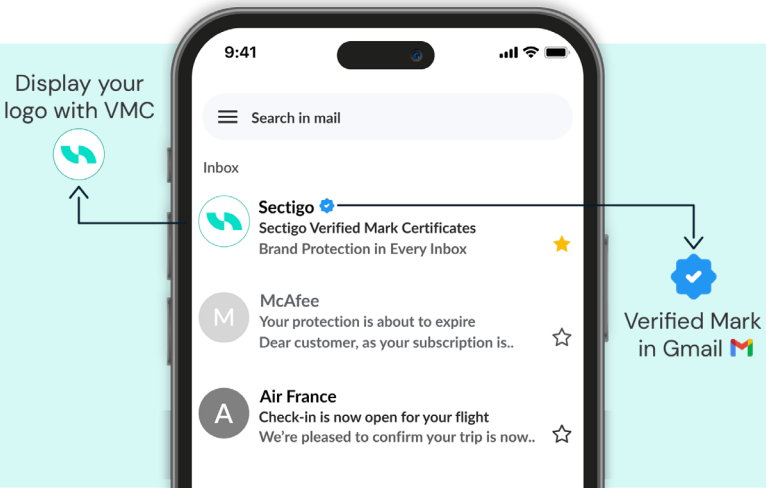
Annual subscription-based pricing. Multi-year discounts available.

Renewal reminders

Automated renewal reminders ensure that your logo will continue to be displayed in recipients' inboxes.

Delivered through a fast, self-service online experience, Sectigo VMCs provide a simple, proven path to:

- Strengthen defenses against phishing and spoofing
- Defend your brand from impersonation
- Win the inbox wars with brand differentiation
- Improve email marketing performance



Verified Mark Certificates with Sectigo Certificate Manager (SCM)

Sectigo also makes VMCs available through SCM, our industry leading certificate lifecycle management (CLM) platform.

This allows you to centralize issuance, renewal, monitoring, and governance in one platform, Sectigo CLM helps reduce operational risk, eliminate certificate related outages, and streamline compliance. This integrated approach ensures that your VMCs remain validated, current, and aligned with your broader digital trust strategy—without adding complexity for your security or IT teams.

Getting Started With Sectigo VMCs

Secure your email domain with DMARC

Set your DMARC policy to “quaratine” or “reject”. Ensure these DMARC rules have been in place at 30 days before applying for a VMC.

Provide your trademarked logo*

Your logo must be registered in a recognized trademark database. The logo must be in a square SVG format.

**If your logo is not trademarked, you may consider a Common Mark Certificate (CMC) instead. See below.*

Verify your business identity

We check your business registration and legal documents. This validation process ensures only legitimate business can display their logo in inboxes.

VMCs vs CMC: Finding the right Mark Certificate for your business

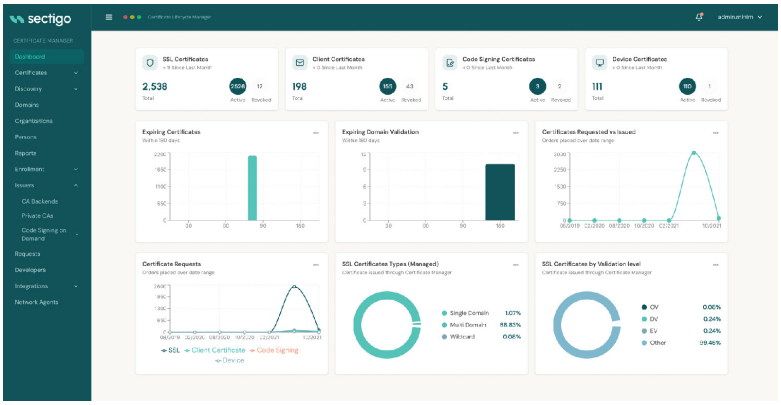
The Common Mark Certificate is a more accessible version of BIMI that doesn’t require a trademarked logo. CMCs are ideal for smaller companies, startups and brands with unregistered logos. While it doesn’t provide the blue checkmark, it does enable logo display in participating mailboxes to help your brand stand out in the crowd with visible trust. Click here for more information on Sectigo CMCs.

Order your Sectigo VMC today!

Ordering your VMC your way:

Sectigo.com
Email
Phone

- USA/CAN: +1 888 266 6361
- International: +1 914 732 8446



About Sectigo

Sectigo is a leader in certificate lifecycle management (CLM), providing innovative and comprehensive solutions to secure both human and machine identities for some of the world’s most prominent brands. Its cloud-native, automated, and universal CLM platform simplifies and enhances enterprise security by issuing and managing digital certificates from all trusted certificate authorities (CAs). With over two decades of experience, Sectigo stands as one of the largest and most established CAs, serving more than 700,000 customers worldwide.

By delivering unparalleled digital trust, Sectigo continues to empower organizations to implement robust securityprotocols with efficiency and confidence.