digicert®

CERTIFICATS VMC (VERIFIED MARK CERTIFICATES)

Apposez votre marque sur vos communications marketing par e-mail et affichez votre identité validée.

Les e-mails font partie de notre quotidien. Ils sont donc aussi utiles que vulnérables, en particulier aux attaques de phishing et par usurpation d'identité. Pour preuve, 96 % des attaques de phishing se font par e-mail et, en 2020, 75 % des entreprises opérant à l'international y ont été exposées.

Pourquoi ? Essentiellement parce que les entreprises manquent d'une part d'outils nécessaires pour s'authentifier clairement et instantanément auprès des utilisateurs, et d'autre part d'une méthode fiable permettant d'identifier et d'isoler rapidement un contenu malveillant déguisé en contenu légitime.

Les certificats VMC (Verified Mark Certificates) changent aujourd'hui la donne. Associés aux protocoles BIMI et DMARC, ils permettent d'afficher clairement le logo de votre marque dans vos emails, tout en dressant un rempart solide contre les attaques de phishing et par usurpation d'identité.

Comment fonctionne l'authentification d'e-mails ?

DMARC + BIMI + VMC = E-mail vérifié

Qu'est-ce qu'un VMC ?

Les VMC sont des certificats d'un nouveau genre qui permettent aux entreprises d'afficher le logo certifié de leur marque en regard du champ « expéditeur » dans les boîtes mail de leurs destinataires, ce avant même que le message ne soit ouvert. Lorsque vous achetez un certificat VMC, DigiCert procède à une vérification draconienne de votre identité et vérifie que votre logo a été officiellement déposé.

Consultez la liste des offices des marques agréés pour les certificats VMC

Qu'est-ce que le DMARC ?

DMARC (Domain-based Message Authentication, Reporting and Conformance) est un protocole de politiques, de reporting et d'authentification d'e-mail basé sur les protocoles SPF et DKIM. Il établit un lien vers le nom de domaine de l'expéditeur, les politiques publiées pour le traitement des échecs d'authentification par le destinataire et des rapports « destinataires à expéditeurs » pour renforcer la visibilité et consolider la protection du domaine contre les attaques malveillantes.

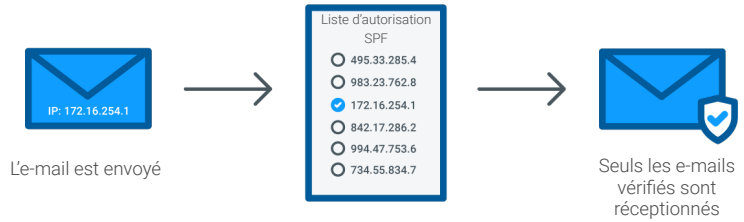
Téléchargez notre guide pratique du déploiement DMARC

Qu'est-ce que le BIMI ?

Le BIMI (Brand Indicators for Message Identification) est une norme de messagerie qui permet d'afficher le logo d'une marque dans des clients de messagerie, favorisant ainsi le déploiement à grande échelle de la protection DMARC.

Comment fonctionnent-ils ensemble ?

L'application du protocole DMARC est validée par le client de messagerie après confirmation de votre enregistrement BIMI et vérification de la validité du logo associé au certificat VMC. Si tous les feux sont au vert, votre logo est affiché. Cet indicateur visuel instantané de la légitimité de vos messages permet d'augmenter la notoriété de votre marque et le taux d'engagement de vos clients.



Atouts des certificats VMC pour les équipes IT

Renforcement de la visibilité, de la sécurité et du contrôle via DMARC

- L'application du protocole DMARC renforce votre sécurité.
- Vous réduisez le risque d'attaques de phishing contre votre marque.
- Vous gagnez en visibilité et en contrôle sur les messages entrants et sortants.
- Vous obtenez des éclairages sur les attaques (types et fréquence) qui ciblent votre marque.
- Vos e-mails légitimes arrivent à bon port et sont facilement identifiés.

Atouts des certificats VMC pour les marketeurs

Maîtrise de votre politique de marque jusque dans les boîtes mail

- Votre taux d'engagement bondit de 10 %[1].
- Chaque message envoyé œuvre pour la notoriété de votre marque.
- Le certificat apporte une preuve irréfutable de votre conformité au protocole DMARC et de la sécurité de vos e-mails.
- Vous offrez une expérience de marque sûre et authentique dont vos clients gardent un bon souvenir.
- Vos messages se démarquent clairement de la masse d'e-mails reçus par vos clients.

Atouts des certificats VMC pour les clients

Moins de phishing. Plus de confiance.

À mesure que le protocole DMARC entrera dans les usages, les consommateurs recevront de moins en moins d'e-mails de phishing sur leur boîte mail, avec pour résultat une moindre exposition au risque, une messagerie moins encombrée et une meilleure expérience utilisateur.

Procédure de validation

Pour obtenir un certificat VMC, les entreprises doivent se soumettre à un ensemble de procédures de validation semblables à celles d'un certificat TLS/SSL EV. L'identité d'un fondé de pouvoir de l'entreprise devra notamment être validée et confirmée en présence d'un représentant légal (notaire, avocat…). En outre, l'équipe de validation de DigiCert s'entretiendra par visioconférence avec le demandeur, qui devra présenter sa pièce d'identité devant la webcam. Enfin, DigiCert devra vérifier que votre logo est officiellement et légalement déposé, et qu'il a été créé au bon format.

Comment convertir votre logo au format .SVG

Acheter un certificat VMC

Vous pouvez acheter un certificat VMC via CertCentral.

NB : cette opération nécessite un compte actif

Acheter un certificat

Installation

1. Après réception de votre logo au format SVG, DigiCert vous fait parvenir un fichier avec une chaîne de certificat PEM.
2. Ajoutez le fichier SVG et la chaîne de certificat sur un serveur accessible publiquement par https (pas par HTTP).
3. Indiquez l'URL et l'emplacement du fichier sur votre enregistrement BIMI.

Questions fréquentes

Combien de certificats VMC me faudra-t-il ?

La réponse dépend du nombre de logos associés à votre entreprise. Pour plus d'infos, consultez notre blog.

Puis-je utiliser un wordmark à la place d'un logo ?

Oui. Vous pouvez utiliser un wordmark comme logo, mais il doit également être enregistré auprès d'un office des marques agréé.

Comment savoir si mon entreprise est conforme au protocole DMARC ?

Vérifiez votre conformité DMARC.

Comment vérifier si mon logo est déposé et quelle est la démarche à suivre pour le déposer légalement ?

Votre logo doit être déposé auprès d'un office des marques agréé.

Pour plus d'infos sur le dépôt des marques, consultez notre blog

Quels sont les clients de messagerie compatibles avec les certificats VMC ?

Gmail, Yahoo, FastMail, Verizon, et bien d'autres.

Les certificats VMC étant relativement nouveaux, la liste des clients de messagerie compatibles est appelée à s'étoffer. Consultez la liste à jour sur notre site.

Que se passe-t-il si j'arrête d'appliquer le protocole DMARC après avoir acheté un certificat VMC ?

Votre certificat reste valable, mais votre logo ne sera pas affiché. Pour continuer d'afficher votre logo, vous devez appliquer le protocole DMARC, comme indiqué par votre enregistrement BIMI.

À quelle fréquence dois-je renouveler et revalider mon certificat ?

Les clients doivent renouveler leur certificat tous les ans. Une fois validée, une entreprise n'a pas à repasser par toute la procédure légale (notaire, avocat…). Elle doit néanmoins renouveler sa validation tous les 398 jours (comme pour un certificat TLS/SSL EV), puis réémettre un certificat via CertCentral.

Notre entreprise est immatriculée au registre du commerce, mais notre logo n'est pas déposé. Pouvons-nous utiliser un certificat VMC ?

Malheureusement, non. Seuls les logos officiellement déposés sont affichés.

D'autres questions ?

Rendez-vous sur :
https://www.digicert.com/tls-ssl/verified-mark-certificates