

VERIFIED MARK CERTIFICATES

Laat merken dat je merk bestaat en laat zien dat je identiteit beveiligd is.

Iedereen gebruikt e-mail dagelijks. Daarom is e-mail een belangrijk doelwit van hackers en is het gevoelig voor met name identiteitsgerichte aanvallen, zoals phishing. 96% van alle phishingaanvallen verloopt via e-mail en 75% van alle mondiale organisaties was in 2020 doelwit van een aanval.

Hoe kan dat? Dit is voornamelijk mogelijk omdat het organisaties ontbrak aan effectieve methodes om zichzelf onmiddellijk en onomstotelijk voor gebruikers te identificeren. Ook bestond er geen betrouwbare methode om kwaadaardige content die zich voordoe als legitiem snel te identificeren en isoleren.

Dankzij Verified Mark Certificates (VMC's), in combinatie met BIMl en DMARC-naleving, verandert dat patroon. VMC's bieden een nieuwe, zeer zichtbare mogelijkheid om uw merk te promoten en tevens phishing te voorkomen. Daardoor worden zowel de consument als de organisatie beschermd tegen identiteitsgerichte aanvallen.

Hoe werkt het verifiëren van e-mail?

DMARC-naleving + BIMl + VMC = logo-geverifieerde e-mail

Wat zijn VMC's?

Verified Mark Certificates (VMC's) zijn een nieuw soort certificaat waarmee bedrijven een gecertificeerd merklogo kunnen weergeven in het afzenderveld in het postvak van hun klanten, ook voordat het bericht wordt geopend. Wanneer u een VMC aanschaft, valideert DigiCert de identiteit van de koper grondig, onder andere door te controleren dat het logo officieel als handelsmerk is geregistreerd.

[Zie de lijst met voor VMC goedgekeurde merkenbureaus](#)

Wat is DMARC?

Domain-based Message Authentication, Reporting and Conformance (DMARC) is een authenticatienorm die voortbouwt op de SPF- en DKIM-protocollen. Het voegt koppelingen naar de domeinnaam van de auteur toe, gepubliceerde beleidsregels voor het omgaan met mislukte authenticatiepogingen door de ontvanger, en rapportage van ontvangers naar afzenders. Daarmee wordt de zichtbaarheid verbeterd en het domein extra beschermd tegen frauduleuze nep- en phishing-e-mails.

[Download de stapsgewijze DMARC-implementatiegids](#)

Wat is BIMl?

BIMl staat voor Brand Indicators for Message Identification en is een e-mailspecificatie die het afbeelden van merklogo's in ondersteunende e-mailclients mogelijk maakt. Het doel is de wijdverbreide implementatie van DMARC-bescherming te stimuleren.

Hoe werken ze samen?

De DMARC-naleving van uw organisatie wordt door middel van uw BIMl-record en uw met VMC ingebed logo door de e-mailclient gevalideerd. Als dit alles in orde is, wordt uw logo afgebeeld. Dit is de visuele bevestiging dat uw bericht authentiek is, hetgeen het engagement en de merkherkenning vergroot.



Voordelen voor IT

Meer overzicht, beveiliging en controle met DMARC

- Extra beveiliging door middel van DMARC-naleving
- Verklein het risico van phishingaanvallen op u en uw merk
- Krijg een beter beeld van en controle over de berichten die in uw domein worden verzonden en ontvangen
- Krijg meer inzicht in het type en de frequentie van de aanvallen op uw domein
- Garandeer dat legitieme e-mails op betrouwbare wijze worden afgeleverd en eenvoudig te identificeren zijn

Voordelen voor marketeers

Krijg weer controle over de inbox

- Verbeter engagement met meer dan 10%¹
- Verbeter de herkenning van uw merk met ieder bericht dat u verstuurt
- Maak van uw merk een synoniem voor DMARC-naleving en verbeterde e-mailbeveiliging
- Bied een merkervaring die authentiek en betrouwbaarder is, en langer blijft hangen
- Zorg dat uw berichten in het oog lopen op het meest effectieve en gebruikte medium

Voordelen voor consumenten

Minder phishing. Meer vertrouwen.

Naarmate meer merken DMARC inzetten, zullen consumenten zien dat er steeds minder phishingmails in hun postvak terechtkomen. Dit betekent minder risico, minder overbodige berichten en een betere algehele gebruikerservaring.

Vereisten voor validatie

Om een VMC te krijgen moeten organisaties een reeks validatieprocedures doorlopen die lijken op die voor het verkrijgen van een EV SSL. Tijdens het proces moet de identiteit van de betreffende persoon worden gevalideerd en in een persoonlijke ontmoeting door een notaris of advocaat worden bevestigd. Het validatieteam van DigiCert heeft bovendien een videogesprek met de aanvrager, die zijn of haar identiteitsbewijs voor de camera moet laten zien. Ten slotte valideert DigiCert dat uw logo wettelijk geregistreerd is en het juiste bestandsformaat heeft.

[Een logo maken in het juiste bestandsformaat \(.svg\)](#)

Een VMC aanschaffen

VMC-certificaten kunt via CertCentral worden aangeschaft.

Opmerking: voor de aanschaf hebt u een actieve account nodig.

[Nu kopen](#)

Installatie

1. Nadat u uw .svg-logo naar DigiCert hebt verzonden, ontvangt u een bestand met een PEM-gecodeerde certificaatketen
2. Het .svg- én het certificaatketenbestand moeten op een openbaar toegankelijke server worden geplaatst en toegankelijk zijn via https (met http mislukt dit)
3. Vervolgens moet u uw BIMi-record updaten met de juiste URL en bestandslocatie

Veelgestelde vragen

Hoeveel VMC's heb ik nodig?

Dit is afhankelijk van het aantal logo's dat uw organisatie in gebruik heeft.
[Raadpleeg ons blogbericht voor meer informatie.](#)

Mag ik in plaats van een logo een woordmerk gebruiken?

Ja. U kunt in plaats van een logo een woordmerk gebruiken, maar ook dit moet bij een deelnemend merkenbureau zijn geregistreerd.

Hoe weet ik of mijn organisatie aan DMARC voldoet?

[U kunt hier controleren of u aan DMARC voldoet.](#)

Hoe controleer ik of mijn merk officieel geregistreerd is en zo niet, hoe kan ik het dan registreren?

Uw logo moet bij een goedgekeurde merkeninstantie zijn geregistreerd.

[Raadpleeg ons blogbericht voor meer informatie over het vastleggen van merken.](#)

Welke e-mailclients geven VMC's weer?

Gmail, Yahoo, FastMail, Verizon en andere.

VMC's zijn nieuw, dus de lijst met ondersteunende e-mailclients groeit nog steeds. Raadpleeg onze website voor de meest recente lijst.

Wat gebeurt er als ik na het aanschaffen van een VMC stop met de naleving van DMARC?

Uw certificaat blijft geldig, maar uw logo wordt niet langer afgebeeld. Om te zorgen dat uw logo zichtbaar blijft, dient u DMARC actief na te leven, zoals aangegeven in uw BIMl-record.

Hoe vaak moet ik hernieuwen en opnieuw valideren?

Klanten moeten hun certificaat jaarlijks verlengen. Wanneer een klant zijn organisatie eenmaal heeft gevalideerd, hoeft hij niet opnieuw het notariële proces te doorlopen. Het volstaat dan om het certificaat iedere 398 dagen opnieuw te valideren, net als bij een standaard EV-TLS/SSL-certificaat. Ook moet de klant opnieuw inloggen bij CertCentral om het certificaat te verlengen.

Wij zijn een officiële organisatie maar ons logo is geen officieel merk. Kunnen wij gebruik maken van VMC's?

Op dit moment helaas niet. Alleen officieel als merk geregistreerde logo's worden getoond.

Hebt u nog vragen?

Meer (contact)informatie vindt u op
<https://www.digicert.com/tls-ssl/verified-mark-certificates>