DMARC Shield

A power booster to improve your email service channels

An email authentication system that helps organizanization to understand and improve their email communication

Netcore

DMARC Domain-based Message Authentication, Reporting and Conformance

DMARC stands for Domain-based Message Authentication, Reporting, and Conformance. It is an email authentication protocol that allows email domain owners to protect their domain from unauthorized use in email messages, commonly known as email spoofing.

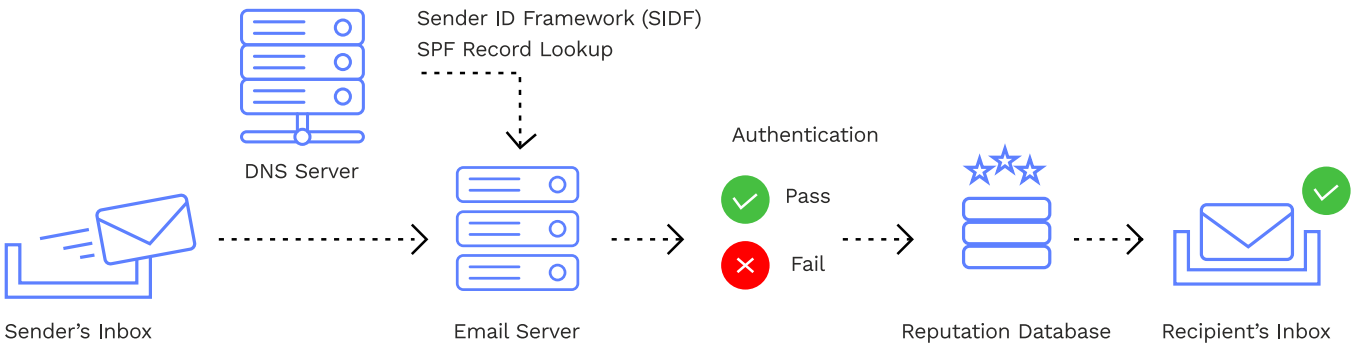
DMARC is built on top of two existing email authentication protocols: Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). It provides a way for email receivers to determine if an incoming message is legitimate based on the alignment of the domain name used in the "From" field of the message header with the domains specified in SPF and DKIM records.

DMARC also provides a mechanism for email domain owners to receive feedback on their email authentication practices, allowing them to monitor and improve their email deliverability and reputation. In addition, DMARC allows domain owners to specify how to handle messages that fail authentication, such as rejecting them outright or sending them to the spam folder.

Overall, DMARC provides an important layer of protection against email fraud and phishing attacks, helping to ensure that email messages are delivered securely and reliably.

SPF Sender Policy Framework

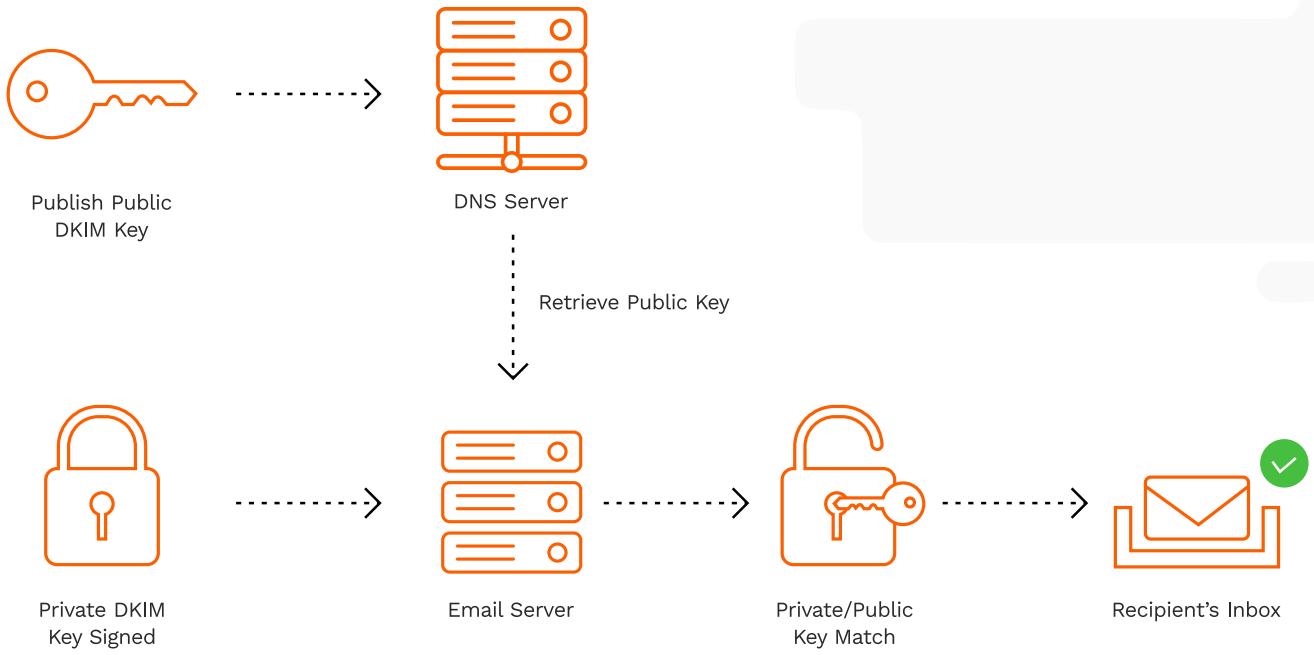
It is an email authentication protocol that allows email domain owners to specify which IP addresses are authorized to send email on behalf of their domain.



SPF works by creating a DNS record that lists the authorized IP addresses for a given domain. When an email is received, the receiving mail server checks the SPF record for the sender's domain to see if the IP address of the sending server is authorized to send email on behalf of that domain. If the sending IP address is not listed in the SPF record, the receiving server can consider the email suspicious and may take actions such as marking it as spam or rejecting it outright.

DKIM DomainKeys Identified Mail

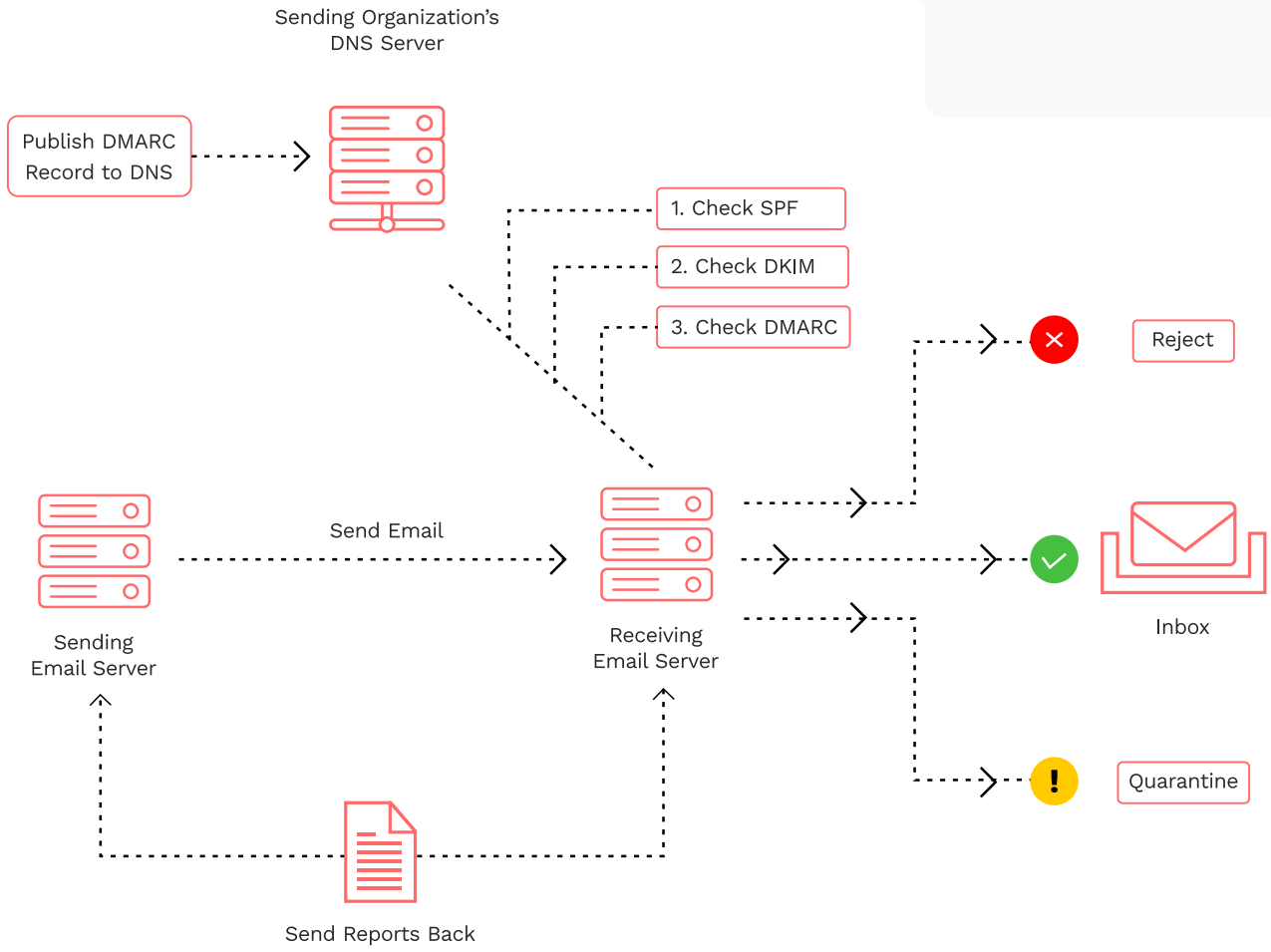
DKIM stands for DomainKeys Identified Mail. It is an email authentication protocol that allows email domain owners to associate their domain name with an email message, providing a digital signature that can be verified by email receivers.



DKIM works by adding a digital signature to the header of the email message. The signature is generated using a private key that is associated with the domain. When an email is received, the receiving mail server can retrieve the public key from the DNS record for the sender's domain and use it to verify the signature. If the signature is valid, the receiver can be confident that the message was sent by the domain owner and that it has not been modified during transit.

DMARC provide reports know has aggregate and forensic reports and has depending on receiver domain. It is the perfect solution for any size of organization looking to protect their email domain from malicious attacks such as domain spoofing, phishing, and other related cyber threats. Our SaaS Offering utilizes industry leading XML parsing and reporting techniques to provide a comprehensive overview of DMARC Shield your email security status.

How DMARC works?



With our easy to understand and user-friendly dashboard, Organization can easily monitor and enforce DMARC policies none to reject, as well as addon module can detect domain lookalikes that may be used to perform malicious activities. DMARC Shield provides the ultimate protection against these potentially dangerous attacks.

Domain Look alike

Protect your domain with DMARC Shield- Domain Look alike module the ultimate solution to prevent email fraud and protect your brand's reputation. Don't let cybercriminals fool your clients with look-alike domains, take control of your domain security today with DMARC Shield!

Verified Mark Certificate BIMI

Netcore

VMC BIMI

Verified Mark Certificate BIMI

(Brand Indicators for Message Identification)

Key Benefits

- Elevate email strategy
- Create a more personalized brand experience for email
- Increase brand impressions
- Cultivate immediate brand recognition
- Stand out in a crowded inbox
- Control the displayed logo
- Reduce email spoofing with DMARC technology

Requirements

- Logo with a confirmed registered trademark
- DMARC, SPF, and DKIM technology with quarantine or reject policy
- High Assurance Verification

Supported Mailbox Provider

- Gmail

Show your registered logo on your emails.

VMC is a new technology that enables you to verify your brand to display your registered logo alongside your outgoing emails. Recipients can see your brand logo assuring them that it's really from you, cultivating a more immersive email experience.

Control logo from sending domains

Gmail will start displaying your logo once the authenticated emails pass all of their other anti-abuse checks. A certification authority will confirm that the logo submitted by the organization is a registered trademark. We confirm that the logo that will be displayed in the email is a registered trademark* of the organization.

Request and manage VMCs in Certificate Services

Customers can request verification for VMCs and manage their associated brand logos our robust certificate management platform, making it easier to manage the end-to-end experience for multiple brands from a central platform.

BIMI Support by Mailbox Provider - BIMI Group

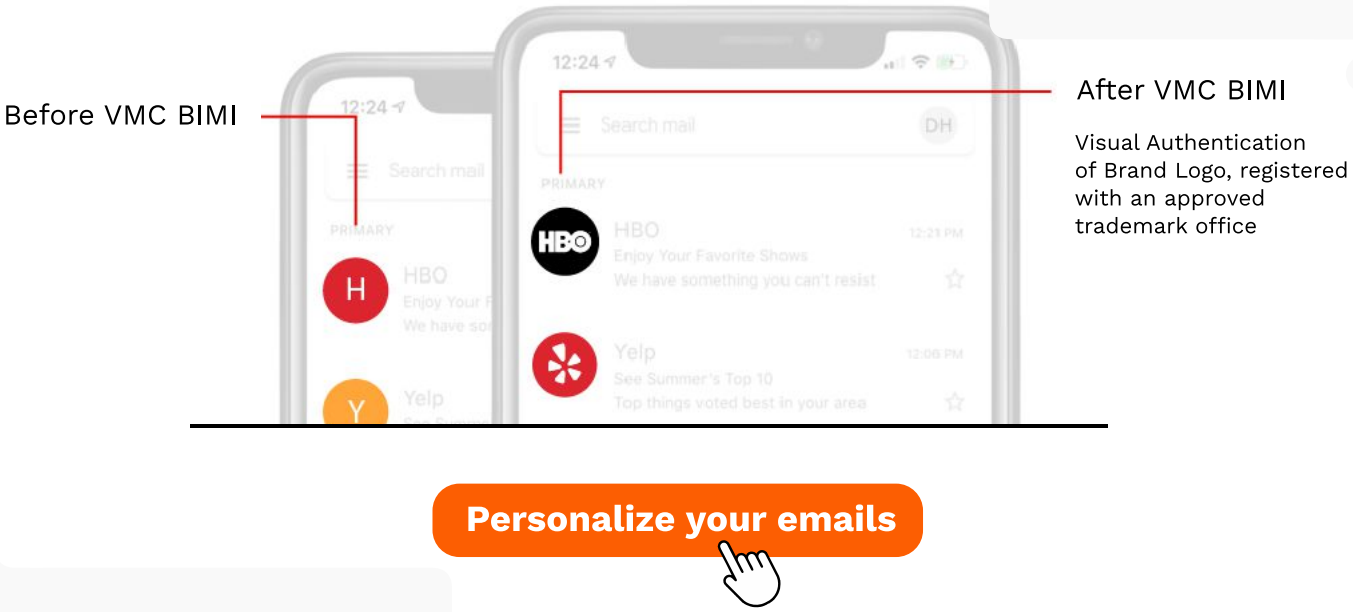
VMC BIMI

Verified Mark Certificate BIMI

(Brand Indicators for Message Identification)

How it works

VMCs only work with email applications that support it and brands that use DMARC (Domain-based Message Authentication, Reporting, and Conformance) with Quarantine or Reject policy, which is used to prevent email spoofing from the sending and receiving servers. BIMI is a set of standards that controls the visual representation in the email. By adding BIMI instructions to your DNS record, your organization's logo is displayed on email communications that originate from your domain.



Netcore

Netcore Cloud Pvt. Ltd.

8th Floor, Peninsula Towers, Peninsula Corporate Park, Lower Parel (W), Mumbai- 400013

infraist@netcorecloud.com I +91 22 6662 8000 I netcorecloud.com

INDIA | US | EU | APAC | SEA | MENA