appgate

APPGATE EMAIL PROTECTION

What is DMARC?

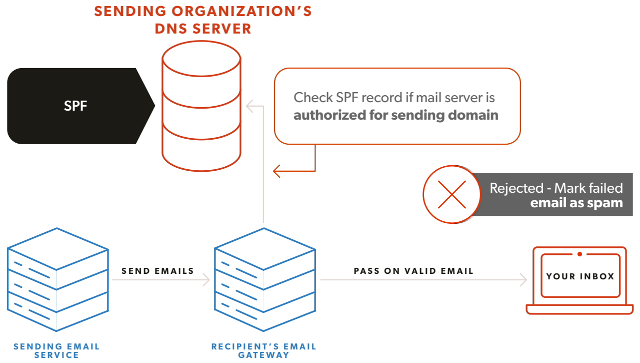
DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication system that protects your organization's domains from spoofing, phishing and other cyber attacks. It builds on the widely deployed email verification techniques: SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail).

What kind of threats does it protect against?

DMARC protects against exact-domain attacks that spoof the header From: address, which is the one you see in the From: field. Without DMARC, emails that appear to originate from your domain can be used to steal personally identifiable information (PII).

What is SPF?

SPF (Sender Policy Framework) specifies the servers that are allowed to send emails on your domain's behalf.


SENDING ORGANIZATION'S DNS SERVER
SPF
Check SPF record if mail server is **authorized for sending domain**
Rejected - Mark failed **email as spam**
SEND EMAILS
PASS ON VALID EMAIL
YOUR INBOX
SENDING EMAIL SERVICE
RECIPIENT'S EMAIL GATEWAY

What is DKIM?

DKIM, or Domain Keys Identified Mail, creates a digital signature, allowing senders to claim responsibility formessages and guarantee content has not been modified.

How does it work?

DKIM relies on cryptography, allowing senders to generate a pair of keys which are used to "sign" emails.

The **PUBLIC KEY** is published for internet service providers to access.

The **PRIVATE KEY** is kept on the outgoing mail server.

How are the keys used?

1. The PRIVATE KEY is used to create a signature for message content and key headers.
2. When the message is delivered, the destination server asks for a public key to verify the signature is right.
3. A matching signature means successful validation

Think of it this way: when you pay for something by credit card, the merchant checks your signature on both the RECEIPT and the CARD to confirm identity. DKIM operates on the same principle!

SO, HOW DOES DMARC BUILD ON SPF AND DKIM?

Unfortunately, SPF and DKIM cannot authenticate the header From: domain name on their own. DMARC addresses that by introducing the 'alignment' feature. This ties together either the 'Mail From/Return-Path' domain or the domain in the 'd=' DKIM signature field to that displayed in the header From:, hence authenticating the email.

DMARC also introduces a reporting feature that allows you to gain insight on your email traffic and boost your deliverability. However, these DMARC reports are generated in a not so easy to read XML format. Not to worry, PowerDMARC takes care of that for you by fetching the data from these reports and displaying them in easy to read charts.

Go the Extra Mile For Your Brand, Go BIMI

Your brand is the single most important part of your business that your customers associate with. It's not enough to have great products and services — people need to recognise and trust your brand. It's your personal seal of assurance, your business identity. The stronger your brand image, the better your chances are of getting through to potential customers.

BIMI Will TakeYour Brand Recall to the Next Level

Brand Indicators for Message Identification, or BIMI, is a standard that uses your brand presence to give your email more credibility. By affixing the logo of your brand on the emails you send, it acts as a second level of verification to let your customers know it's genuine. But with so many email authentication standards already being used today, you might be wondering:

Why Do You Need BIMI?

So glad you asked. These are the best things about BIMI:

Brand Recall: Every time you send an email, your customers will see your logo in their inbox, reinforcing your brand image.

Customer Confidence: A familiar logo will be recognisable to customers as a brand they have a relationship with.

Email Deliverability: An email that's immediately identified as trust-worthy is much more likely to reach inboxes and get clicks.

Visual Confirmation: Your logo is verified along with your email, so it's an easy way to indicate your message has been authenticated.

DMARC-Based: BIMI builds on a foundation of DMARC, giving you more security with your existing DMARC deployment.

DO YOU NEED DMARC?

Yes! Your domain needs to have DMARC deployed with a policy of p = quarantine or reject, with both SPF and DKIM enabled.

You have to develop a good reputation as a sender for email receiving servers to see you as a trusted source. This means following email best practices and deliverability guidelines. Your track record determines whether or not the email receiver will display your BIMI-based logo. There's no time to waste, you better get started!

Free Hosted BIMI

When you sign up for a DMARC deployment with PowerDMARC, you're also getting BIMI implementation on the house. Building your brand literally couldn't get easier.

One-Click Implementation

With PowerDMARC, getting your very own BIMI-based logo isn't just easy, it's fast. Just upload your logo image, click one button and boom. You're done. You can leave the rest to us.

BIMI is one of the newest email verification standards out there. The quicker you act, the easier it will be to build your brand image. ***Contact us now and get your own BIMI solution set up!***

Appgate Email Authentication is powered by Power DMARC

About Appgate

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Appgate helps organizations and government agencies worldwide start where they are, accelerate their Zero Trust journey and plan for their future. Learn more at appgate.com

appgate