bluehornet®
Digital River™

DKIM? SENDER ID? SPF?

EMAIL AUTHENTICATION: AN INFORMATIONAL PRIMER AND HOW-TO

WHAT IS EMAIL AUTHENTICATION?

The term "email authentication" refers to multiple methods that ISPs use to confirm whether an email sender is who they say they are and that the message source is the correct source associated with that sender.

ISPs rely on email authentication to reduce email fraud including:

- "Spoofing," where a sender with bad intentions attempts to impersonate a trusted sender to in an attempt to get the email recipient to take an action; and
- "Phishing," where a sender may use spoofing techniques to get the email recipient to provide sensitive information.

WHY AUTHENTICATE?

If you don't authenticate your emails, ISPs may block your messages because they can't verify your identity. You can't be confident that your deliverability is optimized if your emails aren't authenticated.

However, email authentication is not a golden ticket to the inbox. Even if your emails are authenticated and ISPs can verify your identity, they also consider your sending reputation when determining how to handle your messages. In other words, email authentication, while important, will not cover up or compensate for other reasons ISPs may choose to block or route your messages to the bulk folder.

EMAIL AUTHENTICATION METHODS

DKIM and Domain Keys

DKIM stands for Domain Keys Identified Mail. It is the successor to Domain Keys. When you authenticate with DKIM, you're adding a "key" or digital signature to your message headers that ISPs use to perform a DNS search and verify your identity.

DKIM allows you to prove that your email isn't forged, and can help receiving servers like ISPs and corporate email servers control inbound spam. It can help improve deliverability and establish (or maintain) a reputation for your sending domain.

SPF and SenderID

SPF stands for Sender Policy Framework. The Sender ID authentication method relies on SPF records to verify sender identity at the IP level. Sender ID looks to see that the IP address of the server sending the email match the SPF record's authorized list of domains.

Failure to maintain Sender ID compliance will result in your emails being flagged as potentially fraudulent to MSN and Hotmail users, and it may result in your emails being blocked from your MSN and Hotmail subscribers altogether.

Since you're using BlueHornet to send your emails, DKIM and Sender ID authentication will ensure that your email headers and your SPF record let ISPs know that your company is who they say they are and that we're authorized to send emails on your behalf. Plus, a first-party DKIM signature can speed up mail processing times and it may give you a slightly higher complaint threshold. Additionally, Microsoft autoloads images for authenticated senders.

So it is important to authenticate using both methods—DKIM and Sender ID.

HOW TO AUTHENTICATE YOUR EMAIL WITH DKIM AND SENDER ID

Setting up DKIM

BlueHornet will set up DKIM for you, but before we can complete the process, we'll need to work with you to configure your Domain Name Server (DNS).

Here's how we'll configure your DNS:

You: Identify the domain(s) you intend to send mail with. Example of sending domains include: emails.yourdomain.com or newsletter.yourdomain.com. (Note: Identified domain(s) cannot be the same as the CNAME used with BlueHornet).

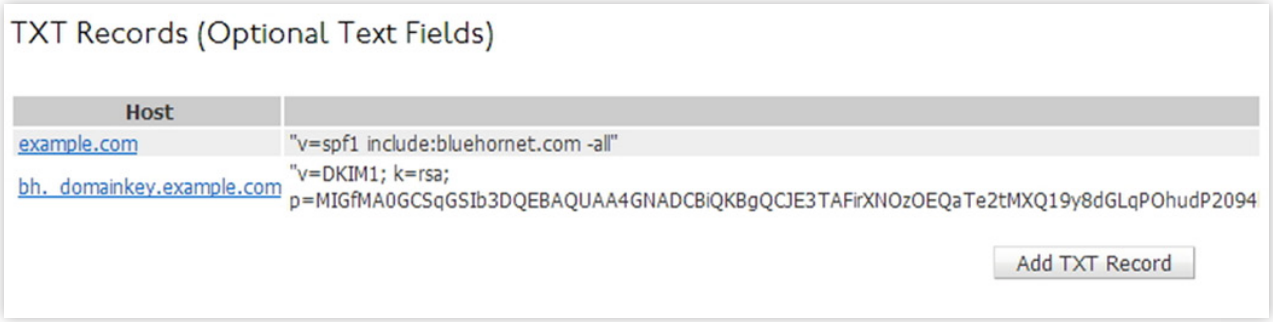
You: Send the domain(s) and the BlueHornet Username of the associated account to your Deliverability Management Services (DMS) or Account Management representative.

Example:
Domain: emails.yourdomain.com
Username: user123

BlueHornet: Once you send us your domain(s) and user name, we will generate the key parts and pass them back to you.

You: Input the key parts we send you into your zone file.

Every host has a different UI so client side implementation will vary from client to client but the setup should look something like this:



✓Congratulations! Your DNS should now be successfully configured

You: Notify your BlueHornet contact that DNS is configures, and we will complete the DKIM setup. The process will take us 3 business days.

SETTING UP SENDER ID

Setting up Sender ID requires you to update your DNS records with SPF:

In your host's DNS records, include:

v=spf1 include:bluehornet.com ~all

If you already have an SPF record in place (because you send from multiple ESPs or send from ESP(s) plus your own platform) you only need to add the following to your SPF record:

include:bluehornet.com

It can take 2-24 hours for your DNS record to show the updated SPF. Here is a validation tool that we recommend for checking:

http://www.kitterman.com/spf/validate.html

If you have any questions or concerns please let your Deliverability Management Services (DMS) or Account Management representative know.