DKIM

- DKIM Setup
- DKIM Short

DKIM Setup

DomainKeys Identified Mail (DKIM) is a protocol that contributes to DMARC compliancy and allows a company to take responsibility for sent messages that can be verified by mailbox providers. Essentially, it enables the outbound domain to digitally sign email to provide legitimacy for the recipient. In conjunction with SPF, DKIM will significantly increase your email delivery rates, and setting it up for your domain is a requirement to become DMARK compliant. Although a somewhat involved task, implementing DKIM on your own is doable. To that point, MxToolbox is here to help you set up DKIM for your business email.

How DKIM Works

As a brief overview of the set up process, DKIM relies on asynchronous encryption, so it works with any tool developed for this type of use. The first step in setting up DKIM for your business is to generate a private/public key pair. Next, the public component of the key needs to be a TXT record assigned to the domain used as the sender address. Then, the private key is utilized to create a DKIM-Signature for each outbound email. Basically, the signature is a hash code computed by combining the content of the email with the private key using a security algorithm. The applied DKIM-Signature is then saved as the header of the email.

As soon as a receiving SMTP server detects this type of header, it looks up the public portion of the key by inquiring the domain name system (DNS) for the specific TXT record. A definite perk of asynchronous encryption is that the keys, in a sense, share data DNA. The public key allows anyone to confirm if the email was sent by the domain owner, which provides legitimacy to the received message. If this check fails or the header/signature does not exist, most email service providers will flag the message. Moreover, depending on the volume of email sent, the provider might decide to classify the email as spam or even block the sender's IP address. Needless to say, these measures should be avoided by your company email to ensure delivery, which also increases your brand's reputation.

How to Set Up DKIM

For a quick rundown of the main steps to set up DKIM, see the following:

1. Configure DKIM to Generate the Key Pair

The applicable tool depends on your operating system. Contact MxToolbox for the ideal scenario for your situation.

2. Create the Public Key as a TXT Record in the DNS Settings

After your DNS provider is selected, update its settings as needed. Note: Some DNS providers are more difficult to set up/navigate than others. MxToolbox will gladly assist you along the way.

3. Generate and Save the DKIM-Signature

Ensure email delivery by applying a unique signature to your messages.

If your company sends messages from third-party providers, DKIM set up is required for each, so be sure to verify that all of your outbound domains apply this protocol. To help you gain DKIM for your business, MxToolbox provides the easiest path for implementation. Let us know how we can help your business achieve 100% DKIM (as well as SPF and DMARC) compliancy.

From <https://mxtoolbox.com/dmarc/dkim/setup/how-to-setup-dkim>

DKIM Short

DKIM short:

Setup an encryption key

Outbound email get a value added that identifies it

Inbound email server uses public key to check encyption and validate

Forwarded messages keep DKIM key when situations would have SPF fail