HOW TO SIGN WITH DKIM

WHAT IS DKIM?

DKIM (DomainKeys Identified Mail) is a protocol that allows an organization to take responsibility for transmitting a message in a way that can be verified by mailbox providers. This verification is made possible through cryptographic authentication.

A sender decides which elements of the email they want to include in the signing process. They can decide to include the whole message (header and body) or just focus on one or more fields of the email header. The elements they decide to include in their DKIM signing process must remain unchanged in transit, or the DKIM signature will fail authentication.

HOW TO SIGN WITH DKIM

STEP 1: Identify all of your sending domains

Make a list of all of your sending domains, and be sure to consider whether any of the following are used to send email:

- Web server
- In-office mail server (such as Microsoft Exchange)
- Your ISP's mail server
- Mail server of your end-users' mailbox provider
- Any other mail server used to send email on behalf of your brand

STEP 2: Install and configure DKIM on your email server

Because all outgoing email is required to be signed with DKIM, you will need to install a DKIM package specifically for your email server. To find out whether or not your platform has available DKIM software, you can check DKIM.org or check with your vendor. If you're using an email service provider, you will need to work with them on setting up your DKIM record.

STEP 3: Create a public and private key pair

Use an online wizard or your mail server's own key generator to create the DKIM public/private key pairing and the policy record. The public key will be placed in your public-facing DNS record. The private key is installed on the MTA/Email sending system(s). You can also generate your own using openssl:

- Enter the From: domain that you are authenticating
- Enter the selector name. Make this name descriptive of the type of email you are sending, like *marketing*, or *newsletter*.
- Also, ensure your key is 1024-bit or higher. Most providers don't have an option for anything lower, but if you are using your own tools, 1024 is required.

STEP 4: Publish your public key

The DKIM wizard should now have given you a selector record. This record includes the DKIM subdomain that will store the public key which is a combination of the domain and selector name.

For example, domain.com with a selector of marketing will have the public key stored in marketing._domainkey.domain.com. You will store your public key in the TXT portion of that domain. Most people will need to work with their system administrator to publish this. If you're using a hosted solution, you can set this up within their interface.

STEP 5: Store your private key

Your private key will also be generated by the wizard and will need to be stored where your DKIM package specifies. It is absolutely critical that this private key is never shared or exposed. If it is, your security will be compromised.

STEP 6: Configure your email server

You will need to configure your system appropriately. Consult your server's installation instructions or contact your vendor.

STEP 7: Test!

If you've successfully configured everything on your system, the next step is testing.

You should consider rotating your keys for maximum protection in case a key or set of keys becomes compromised. We recommend 6 monthly key rotations. To ensure you're continuing to authentication properly, contact Proofpoint and we'll help you manage your DKIM signatures