**Domain Keys Identified Mail, or DKIM,** is a standard that prevents email senders and recipients from spam, spoofing, and phishing. This form of email authentication allows an organization to add digital signature to the emails that can be validated by the recipient to check if the email belongs to the legitimate Sender. To verify the authorization of email Server, it uses approach called “public key cryptography”. It supplements SMTP, the basic protocol used to send email, because it does not itself include any authentication mechanisms.

**How it works**

It works by adding a digital signature to the headers of an email message. That signature can be validated against a public cryptographic key in the organization’s Domain Name System (DNS) records. A domain owner publishes a cryptographic public key as a specially-formatted TXT record in the domain’s overall DNS records. When a mail message is sent by an outbound mail server, the server generates and attaches a unique DKIM signature header to the message. This header includes two cryptographic hashes, one of specified headers, and one of the message body (or part of it). The header contains information about how the signature was generated.

When an inbound mail server receives an incoming email, it looks up the sender’s public DKIM key in DNS. The inbound server uses this key to decrypt the signature and compare it against a freshly computed version. If the two values match, the message can be proved to authentic and unaltered in transit.

**How is it related to SPF, DMARC, or other standards?**

- SPF allows senders to define which IP addresses are allowed to send mail for a particular domain.
- DKIM provides an encryption key and digital signature that verifies that an email message was not faked or altered.
- DMARC (Domain-based Message Authentication, Reporting and Conformance) unifies the SPF and DKIM authentication mechanisms into a common framework and allows domain owners to declare how they would like email from that domain to be handled if it fails an authorization test. DMARC is still in its early age and unfortunately not used as much as hoped to make a huge difference. DMARC can (and will) break your mail flow if you don’t set up both SPF and DKIM before changing DMARC policy to anything above “none”
- Please work through the proper process carefully, otherwise your messages won’t be delivered to your users as potentially seen as fraudulent by a wrong SPF, DKIM or DMARC setup.

**Does Proofpoint Support DKIM And DMARC?**

Currently DKIM and DMARC integration is not supported on Proofpoint Essentials platform, but is on the product roadmap without any ETA. Proofpoint Essentials can pass DKIM and DMARC signed messages without impacting the
signature or doing any signing. The sender would need to set everything up and we could then pass the email. Proofpoint Essentials recommends to point domain SPF records as per their data center Information to implement DKIM on customer domain. For Proofpoint Essentials recommended SPF records, please refer the below knowledge-base:

Connection details - Proofpoint, Inc.