

# What is DKIM and how to manage it with EasyDMARC

## DKIM Lookup

### Why does DKIM lookup matter?

DKIM record lookup tool checks if your DKIM record is published for domain selector (as a subdomain) and deployed correctly. It also informs whether you need to take action regarding the DKIM record validation result. To run a DKIM check, enter your domain in the Domain section, input your selector name and click on the DKIM Lookup button.

### What does DKIM lookup do?

- Check if the DKIM TXT record is published in DNS for the domain
- Check the published DKIM TXT record syntax
- Validate DKIM public key associated with selector

## DKIM - How does it work?

The domain owner generates a public/private key pair to be used for signing outgoing messages. Private keys are stored on the email server, while public keys are implemented in the domain's DNS server. Upon sending emails, the server uses the stored private key to generate a digital signature of the message, which will be inserted in the message header. The receiving server, on the other hand, will retrieve the sender's Public Key from DNS to verify that the signature was generated by the matching private key. A match effectively proves that the email was truly sent from, and with the permission of, the claimed domain and that the message headers and content have not been altered during transit.

## How to analyze DKIM selector from DMARC Aggregate Reports

DMARC Aggregate reports contain a specific tag with "selector name", which helps you easily identify your DKIM signature Selector name. We also convert this data into an easy-to-read format where you can identify your DKIM Selector name under the "DKIM Auth. Results" tab of your dashboard.

## How to check DKIM record in your DNS

To check your DKIM Record in your DNS, you need to find a TXT or CNAME type record with the Host / Name similar to [selector].\_domainkey.yourdomain.com.

## How to analyze DKIM selector from Email Headers

DKIM selector is inserted into the DKIM-Signature email header as an s= tag when the email is sent.

E.g: DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=easydmarc.com; h=content-type:from:mime-version:subject:reply-to:x-feedback-id:to: list-unsubscribe; s=s1;

## How many DKIM records can I have?

There are no limitations. You can have multiple DKIM Records, since technically speaking each DKIM record can be associated with a unique selector. In fact, if your domain uses multiple email services to send emails (Marketing, Transactional, etc.), multiple DKIM selectors and private/public key pairs must be used to separate these services.

## Investigating DKIM Issues

Use EasyDMARC's DKIM Lookup tool to verify if your DKIM record and Public Key are properly implemented without any syntax or other issues

Analyze DMARC Aggregate Reports that contains all the relevant information of your DKIM Signatures (If they're passing or failing)

Investigate Email Headers to retrieve DKIM-Signature, and analyze the underlying results

If you're using third-party ESPs and obtained DKIM Public key from them, make sure you have "Activated" DKIM Signing process from their portal

# Is DKIM part of the DMARC protection?

Yes. DKIM is one of the authentication protocols (along with SPF) DMARC relies on to provide a set of instructions to receiving email servers on how to handle unauthenticated mail.

## If I have an SPF do I have to implement DKIM?

Absolutely. Both SPF and DKIM play a major role in the email authentication world. In fact, unlike SPF, DKIM tends to survive the Forwarding cases.

## How to generate a DKIM record?

How to generate a DKIM record? DKIM adds an encrypted signature to the header of all outgoing messages. Email servers that get signed messages use DKIM public key to decrypt the message header and verify the message was not changed after it was sent. Generally, DKIM detects forged header fields and content in emails. As DKIM works with Private and Public keys, there are multiple use-cases for DKIM implementation:

- If you are using Third-Party ESPs (Google, Microsoft365, Mailchimp, etc.) DKIM Public keys are obtained from their portals. ESPs won't share their Private Keys for privacy and security concerns.
- For dedicated servers, EasyDMARC's DKIM Generator tool is particularly made to make the process easy and fast. You will securely store the Private key in your own server while implementing the Public key in your DNS.

## How does DKIM work?

DKIM uses a pair of keys, one private and one public, to verify messages. A private domain key adds an encrypted signature header to all outgoing messages sent from your email domain. A matching public key is added to the Domain Name System (DNS) record for your email domain. Email servers that get messages from your domain use the public key to decrypt the message signature and verify the signed message sources.

## How to use a DKIM Record Generator?

In order to use the DKIM Record Generator, you need to specify the “selector” name, your domain name, and the Key length.

- A selector can be any given name. Use a name to clearly identify the DKIM Signature in future.
- Enter your domain name, this should match the visible “From” address domain.
- Specify the Key length. We support 1024, 2048, and 4096-bit size keys.
- Once DKIM Record is generated, store the Private Key in your mail server configurations (with .pem file), and implement the Public Key in your DNS Zone.

## Do I need to generate a DKIM Record if I’m using a third-party ESP?

No. This is a common misconception. You only need to generate a DKIM Record only for your dedicated mail servers. For Third-Party ESPs such as Google Workspace, Microsoft, Mailchimp, etc. they already store the Private Key in their own mail server configurations and provide only Public Signatures for their users. The only action you need to take is to get the Public Signature from the given ESP portal and implement it in your DNS, and later turn on the “Activation” for DKIM within the ESP portal.

---

Revision #2

Created 2026-08-07 14:59:00 UTC by Sarath

Updated 2026-08-07 16:05:08 UTC by Sarath