How to set up DKIM for Mautic

DKIM (DomainKeys Identified Mail) adds a digital signature to every email you send. The receiving server checks the signature against a public key published in your DNS, which proves the email really came from your domain and wasn't changed on the way. If I could get every Mautic user to do just one authentication job properly, it would be this one. It survives forwarding much better than SPF, DMARC relies on it, and one-click unsubscribe won't work without it.

DKIM is defined in RFC 6376 if you'd like the full technical detail.

Before you start

You'll need these.

- Access to the DNS settings for your sending domain
- Admin access to the email service Mautic sends through
- Admin access to Mautic, to send test emails

Step 1. Set up domain authentication at your email service

Mautic doesn't usually sign emails itself. The email service you've set up under **Settings > Configuration > Email Settings** does the signing. So log in to that service and look for **domain authentication**, **domain verification** or **sender authentication**, and add the domain you use as your From address in Mautic.

If you send from your own mail server (Postfix with OpenDKIM, for example), you'll generate the key yourself. Use a 2048-bit key.

Step 2. Publish the DNS records

Your email service will give you one or more DNS records to add. They usually look like one of these.

A CNAME record, where the service hosts the key for you.

```
s1._domainkey.yourdomain.com  CNAME  s1.domainkey.u12345.wl.sendgrid.net
```

A TXT record, where you publish the key yourself.

```
mautic2026._domainkey.yourdomain.com  TXT  "v=DKIM1; k=rsa; p=MIIBIjANBgkq..."
```

The bit before ._domainkey is called the **selector**. It lets you have several keys at once, which is handy when you use more than one service or want to change keys later.

Copy the records exactly. A missing character in a key breaks it.

Step 3. Verify at your email service

Go back to your email service and click verify (or wait for it to check automatically). Don't move on until it shows the domain as verified.

Step 4. Check it worked

1. Send a test email from Mautic to a Gmail address.
2. Open it, choose **Show original** from the three-dot menu, and check DKIM shows **PASS**.

3. Look at the line that says DKIM: 'PASS' with domain .... That domain should be **your** domain (or a subdomain of it), not your email service's domain.

That last check matters. An email signed by yourprovider.net passes DKIM but does nothing for DMARC on your own domain.

Get the settings right

Most services handle these for you, but if you run your own server or your service lets you choose, aim for these.

Setting	Use	Why
Key size	2048-bit	1024 is the minimum, 2048 is the sensible default today
Algorithm	rsa-sha256	Avoid rsa-sha1
Canonicalisation	relaxed/relaxed	Copes with small changes to spacing in transit
Body length (l=)	Don't use it	It lets someone add content to the end of your email without breaking the signature

DKIM (DomainKeys Identified Mail) adds a digital signature to every email you send. The receiving server checks the signature against a public key published in your DNS, which proves the email really came from your domain and wasn't changed on the way. If I could get every Mautic user to do just one authentication job properly, it would be this one. It survives forwarding much better than SPF, DMARC relies on it, and one-click unsubscribe won't work without it.

DKIM is defined in RFC 6376 if you'd like the full technical detail.

Before you start

You'll need these.

- Access to the DNS settings for your sending domain
- Admin access to the email service Mautic sends through
- Admin access to Mautic, to send test emails

Step 1. Set up domain authentication at your email service

Mautic doesn't usually sign emails itself. The email service you've set up under **Settings > Configuration > Email Settings** does the signing. So log in to that service and look for **domain authentication**, **domain verification** or **sender authentication**, and add the domain you use as your From address in Mautic.

If you send from your own mail server (Postfix with OpenDKIM, for example), you'll generate the key yourself. Use a 2048-bit key.

Step 2. Publish the DNS records

Your email service will give you one or more DNS records to add. They

usually look like one of these.

A CNAME record, where the service hosts the key for you.

```
s1._domainkey.yourdomain.com  CNAME  s1.domainkey.u12345.wl.sendgrid.net
```

A TXT record, where you publish the key yourself.

```
mautic2026._domainkey.yourdomain.com  TXT  "v=DKIM1; k=rsa; p=MIIBIjANBgkq..."
```

The bit before ._domainkey is called the **selector**. It lets you have several keys at once, which is handy when you use more than one service or want to change keys later.

Copy the records exactly. A missing character in a key breaks it.

Step 3. Verify at your email service

Go back to your email service and click verify (or wait for it to check automatically). Don't move on until it shows the domain as verified.

Step 4. Check it worked

1. Send a test email from Mautic to a Gmail address.
2. Open it, choose **Show original** from the three-dot menu, and check DKIM shows **PASS**.
3. Look at the line that says DKIM: 'PASS' with domain .... That domain should be **your** domain (or a subdomain of it), not your email service's domain.

That last check matters. An email signed by yourprovider.net passes DKIM but does nothing for DMARC on your own domain.

Get the settings right

Most services handle these for you, but if you run your own server or your service lets you choose, aim for these.

Setting	Use	Why
Key size	2048-bit	1024 is the minimum, 2048 is the sensible default today
Algorithm	rsa-sha256	Avoid rsa-sha1
Canonicalisation	relaxed/relaxed	Copes with small changes to spacing in transit
Body length (l=)	Don't use it	It lets someone add content to the end of your email without breaking the signature
Testing flag (t=y)	Remove when done	Receivers treat test-mode signatures as unsigned

Make sure the right headers are signed

When you look at the DKIM-Signature header in the message source, you'll see h= followed by a list of the headers included in the signature. Check these are in the list.

- from (required)
- subject, date, to, reply-to
- list-unsubscribe and list-unsubscribe-post

The last two are essential for one-click unsubscribe. In our community forum, one Mautic user traced their failing one-click unsubscribe to exactly this, with the two headers missing from the signature when sending through Amazon

SES. See *How to set up one-click unsubscribe in Mautic.*

Changing keys

To change a key without breaking anything, publish the new key under a **new** selector name, switch signing to it, and leave the old key in DNS for a week or so before removing it. Date-based selectors like mautic2026 and mautic2027 make this easy to keep track of. If your service uses CNAME records, they usually rotate keys for you.

Common problems

DKIM passes but with your provider's domain. Domain authentication isn't finished for your domain at the email service. Go back to Step 1.

"Body hash did not verify". Something changed the email after it was signed, such as a gateway adding a footer or a disclaimer. Sign after any changes are made.

DKIM fails even though the DNS record is there. Check the selector. The s= value in the DKIM-Signature header must match the start of your DNS record name, the part before ._domainkey. A typo in either, or a record added under the wrong name, means the key can't be found.

No DKIM at all. The From address in this email doesn't match the domain you authenticated. Check the From address on the email's **Advanced** tab in Mautic, as well as the default in Email Settings.

Quick checklist

- Domain authenticated at your email service
- DNS records published and verified
- Gmail test shows DKIM PASS with **your** domain

- 2048-bit key, rsa-sha256, no l=, no leftover t=y
- list-unsubscribe and list-unsubscribe-post included in the signed headers

Over to you

How often do you change your DKIM keys, if at all? I'm curious how integrators handle this across lots of client domains.

References

Crocker, D., Hansen, T. and Kucherawy, M. (eds.) (2011) *DomainKeys Identified Mail (DKIM) signatures*. RFC 6376. Internet Engineering Task Force. Available at https://www.rfc-editor.org/rfc/rfc6376.html (Accessed 26 October 2026).

Mautic Community Forum *Unsubscription test fails*. Available at https://forum.mautic.org/t/unsubscription-test-fails/30648 (Accessed 26 October 2026).

Online URL:
https://kb.mautic.org/article/how-to-set-up-dkim-for-mautic.html