E-mail anti-spam

Technical guide to setup SPF, DKIM, and DMARC to secure optimal email deliverability from webCRM, using Mailjet

To secure the optimal delivery rate of emails sent from webCRM using Mailjet and to avoid getting caught in spam filters, we have made a guide of technical tasks that can be performed to improve the delivery rate. The guide is mainly focussed on e-mails sent using Mailjet, but you can also send from your own email server, see **4. Sending from your own e-mail server** on page 5.

To be able to send mass e-mails from webCRM, such as newsletters, invitations and reminder to events etc. you must complete at least step 1 about SPF-records. We strongly suggest that you also complete step 2 about DKIM. Once this step is completed, you will send from an IP-address with a better rating than only when SPF-records are set up, thus increasing the deliverability.

If you wish to improve your setup further, you can complete step 3 and implement DMARC authentication. It will require changes your side and should only be done by experts.

1. SPF-records

Sender Policy Framework (SPF) is an email validation system designed to prevent e-mail spam by detecting e-mail spoofing, a common vulnerability, by verifying sender IP-addresses. SPF allows administrators to specify which hosts/servers are allowed to send mail from by creating a specific SPF-record in a domains Domain Name System (DNS) zone. Mail-servers use DNS to check that mail from a given domain is being sent by a host sanctioned by that domain's administrators.

This requires that you have your own domain. If your e-mail is a public domain provider for example an @hotmail or @gmail e-mail address you should not send mass e-mails from webCRM.

1.1 Technical setup

To publish that you permit sending e-mails from your webCRM system you need to create or modify the SPF-record to include **“include:spf.webcrm.com”**. The SPF-record should be setup as a TXT-record. Some DNS providers allow you to do it yourself, but otherwise you must contact your DNS provider and have them do it.

SPF-record formats do vary, and you should consult your IT staff or DNS Provider for the exact format to use.

Example text for SPF-record permitting webCRM and Mailjet SMTP server as well as your own e-mail server:

"v=spf1 ip4:111.222.333.444 include:spf.webcrm.com -all", where 111.222.333.444 is the IP for your own smtp server if you have one.

If you have Office 365, the record would look like this:

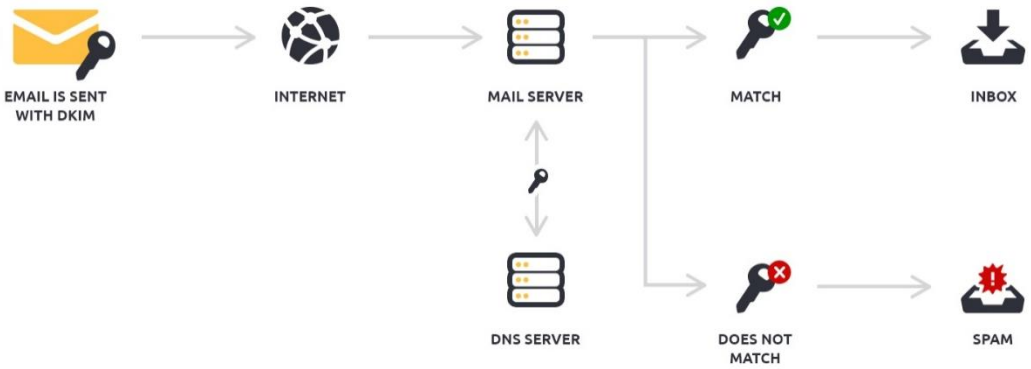
v=spf1 include:spf.protection.outlook.com include:spf.webcrm.com +a +mx ~all

2. DKIM

The acronym DKIM stands for "Domain Keys Identified Mail". It is an encryption authentication method that is used by mail servers to establish if the e-mail originated from an authorized system and prevents spammers from stealing the identity of legitimate entities.

DKIM allows for a unique signature to be added to the message header for each e-mail you send. This signature is specific for your domain and is generated by a private key. The corresponding public key is added to a DNS record for your domain.

When an e-mail server receives your e-mail, it checks the public key to determine if your private key was used to generate the e-mail signature. If your private key was not used, the e-mail is considered to be a phishing or spam attempt.



2.1 Technical setup

To setup DKIM for your domain, you need to confirm the ownership of your domain either by creating a DNS record or by placing an empty text file with a name provided by webCRM in the root of your web-server. After that you must create a TXT-record in your DNS with a DKIM value provided by webCRM. It is important that both these steps (2.2 and 2.3 in this document) are implemented correct for webCRM to validate the DKIM setup.

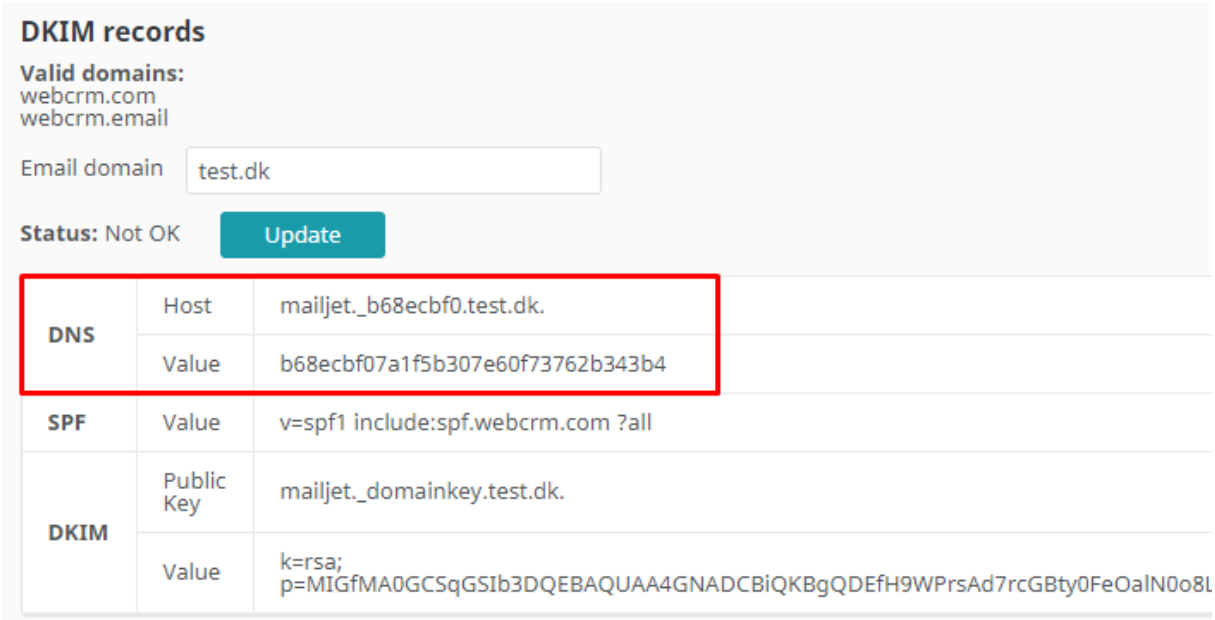
You must be able to create and insert these values yourself or get your DNS Provider to do it, as we cannot help with these steps. If we could do it on your behalf, the validation would not mean anything as all spammers could do the same.

2.2 Validating domain

To validate your domain, we offer two methods

1) Create a DNS record with hostname and value provided in webCRM
2) Host a temporary file on your website with a filename provided in webCRM

You can get the hostname and value in webCRM, under Configuration -> Main settings -> E-mail, by inserting your domain and clicking Validate.

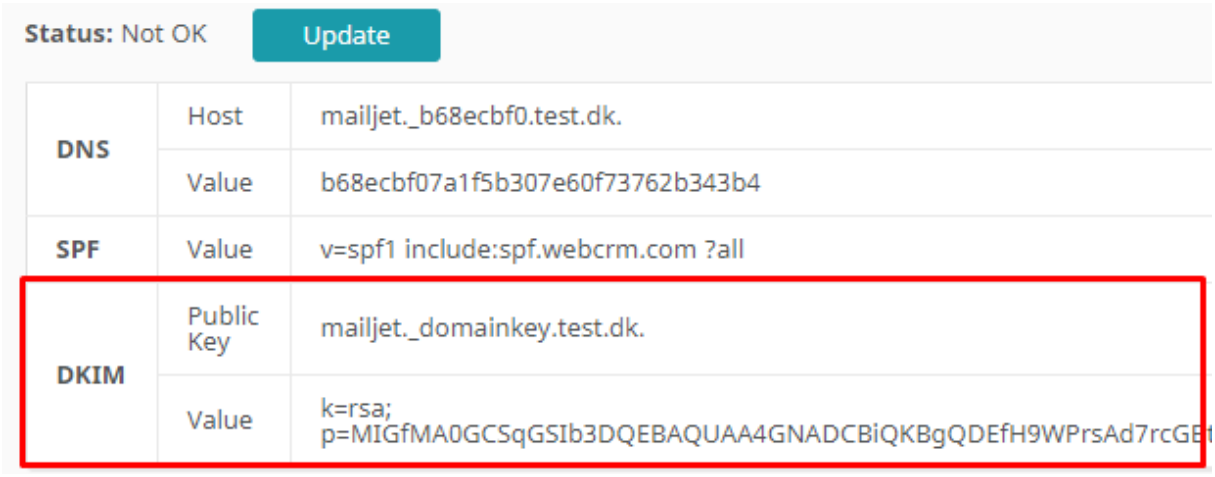


If you use method 2, the filename should be the value followed by .txt. In this case it will be: "*b68ecbf07a1f5b307e60f73762b343b4.txt*".

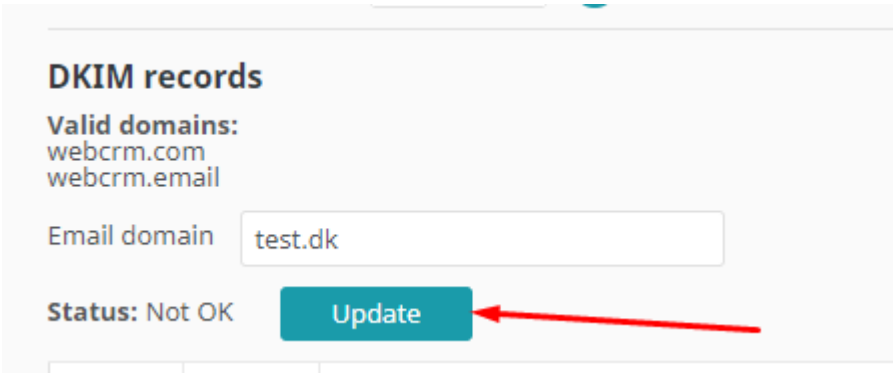
2.3 DKIM authentication

To validate your DKIM setup, you must first setup SPF-records, as described in **1. SPF-records**. Then you must create a DKIM record.

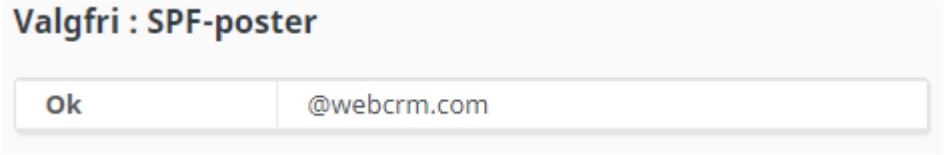
When validating your domain in webCRM, you will also receive a Public Key and Value for the DKIM authentication. Please make sure that the DKIM value is in one line when you add it, no matter how your browser has divided the value when it is shown.



When you have added the values, you can Update status to check that Domain validation and DKIM are correct and thereafter your deliverability should be increased.



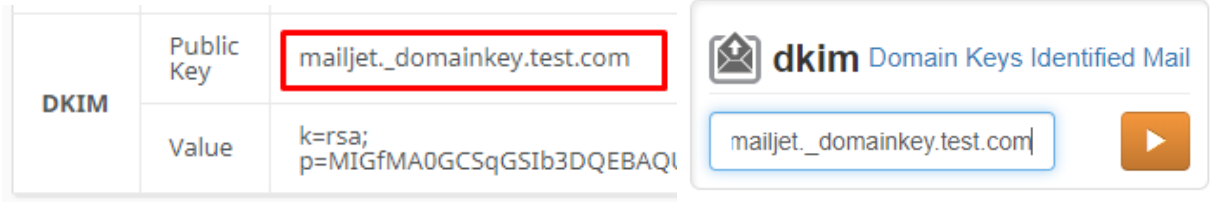
Remember to also Verify your SPF records, which can be done on the same page.



2.4 Validation errors

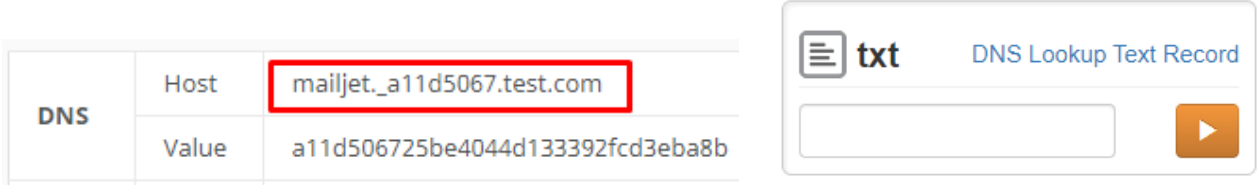
If the DKIm validation in webCRM fails, even though you have tried to setup both step 2.2 and 2.3, you can check the validation using this link: https://mxtoolbox.com/NetworkTools.aspx

The DKIM record is checked by inserting the Public key in the DKIM box:



The value from webCRM should be shown in a green box.

Validation of the domain (step 2.2) is validated by inserting the Host value in the txt box:



A DNS record with the value from webCRM should be shown, otherwise the DNS record is not made or published correct.

If you chose to validate your domain ownership by placing a file on your website, your should go to an URL consisting of your domain/DNS-value, e.g. https://www.test.com/a11d506725be4044d133392fcd3eba8b.txt This must show a page with a file and not just an error page such as 404 Page not found.

3. DMARC authentication

DMARC stands for "Domain-based Message Authentication, Reporting & Conformance". It allows you to indicate to the recipient servers which behavior to adopt should the SPF and DKIM authentications fail (NB: Certain recipient servers do not take into consideration the DMARC policy in the context of delivering e-mails).

It is important that this additional authentication procedure is put in place only after the SPF and DKIM authentication are set and validated.

In order to apply a DMARC policy to a sender domain, it is enough to add a TXT-record in the DNS zone of your sender domain, such as for example:
Host: *dmarc.yourdomain.com.*
Txt: *v=DMARC1; p=none; pct=100; rua=mailto:yourmail@yourdomain.com; sp=none; aspf=r;*

It is important that the DMARC setup is done by someone who knows how this setup should be done. It is possible to get recipient servers to delete all e-mails coming from your domain if everything is not set up correctly. webCRM cannot guide you on this setup and if you are in doubt it is better to avoid setting up DMARC than setting it up incorrectly.

If you wish to setup DMARC authentication with your webCRM solution, you should read and follow Mailjet's technical documentation. This includes multiple steps, that should be completed before the validation works as intended.

4. Sending from your own e-mail server

An alternative to setting up these steps is to relay e-mails sent from within webCRM through your own e-mail server. This way you will be responsible for the spam-rating of your domain and should maintain a good reputation yourself. Another disadvantage is that you cannot use Mailjet in webCRM, meaning that click and open-rates will not be monitored and you cannot gather and use data about this.

If you wish to send from your own server, you must verify that the webCRM system can access your SMTP server by checking your server's authentication method. webCRM can be allowed to send by either providing us the username and password for the SMTP server or by whitelisting the IP address **40.119.151.106**, which the webCRM system sends e-mails from. If you do not use authentication on your SMTP server you can skip this step, but this is not recommended, as everybody can then send e-mails as you.

When this is done, please provide us the following information:

- E-mail domain or IP address to relay by
- The port to relay by
- If you want to apply encryption (TLS)
- (Username and password, if you chose this authentication)

We will then make the required setup on our side and your own e-mail server will be used.

5. Special settings for internal e-mails

Some customers have a setup where e-mails send and received internally in the organization are protected in a special way. This is implemented to secure that people from outside the company cannot identify as an employee and send e-mails from the domain from elsewhere than your own servers.

However, this will also limit webCRM from sending e-mails to your internal e-mail addresses and you should allow e-mails from the following IP addresses to be received from internal e-mail addresses:

- 31.31.83.10
- 87.253.233.38
- 87.253.233.39
- 87.253.233.40
- 87.253.233.41