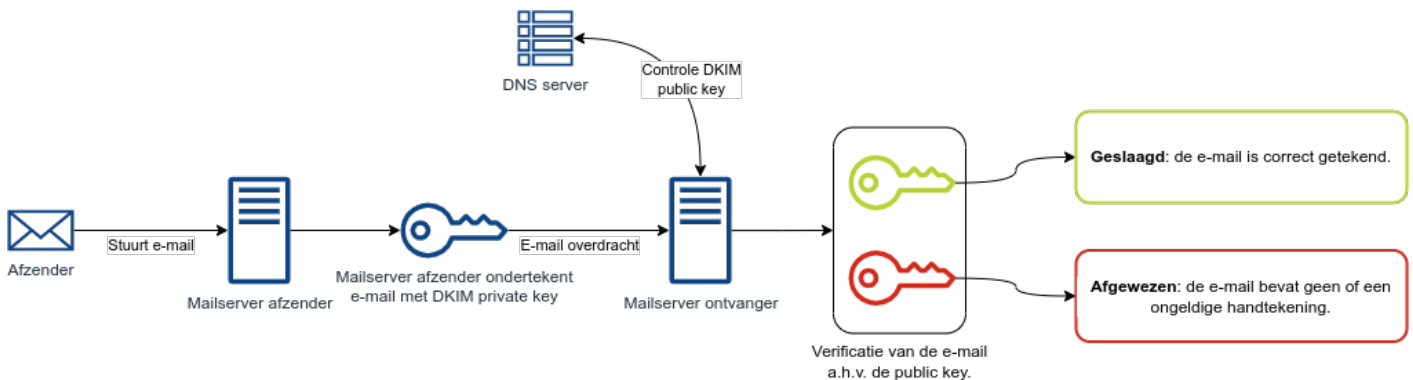


Een DKIM record instellen

Wat is DKIM?

DKIM staat voor Domain Keys Identified Mail. DKIM wordt op zowel het niveau van een DNS record op je domeinnaam geregistreerd alsook op je e-mailserver. DKIM 'ondertekent' digitaal iedere e-mail wat je verzendt en stuurt die digitale handtekening mee in de 'headers' van iedere verzonden e-mail. De ontvanger controleert of de digitale handtekening in de e-mail overeenkomt met het publieke DNS record. Komt de digitale handtekening overeen? Dan is het zeker dat de e-mail en de bijlagen niet gewijzigd zijn.



DKIM werkt op basis van een private en een public key. Op je mailserver staat een private key geconfigureerd. Wanneer je mailserver een e-mail verzendt, dan wordt dat bericht automatisch ondertekend met de private key. De ontvangende e-mailserver controleert deze handtekening aan de hand van de public key wat in het DNS record staat.

In zeven stappen ziet het technische DKIM teken- en validatieproces er als volgt uit:

1. Op je e-mailserver is een DKIM public key gegenereerd.
2. Een eindgebruiker stuurt een e-mail.
3. Deze e-mail komt terecht op je e-mailserver. Je e-mailserver tekent met de private key de e-mail en plaatst de handtekening in de headers van het e-mailbericht en verzendt de e-mail naar de ontvanger.
4. Het bericht komt aan op de e-mailserver van de ontvanger.
5. De ontvangende e-mailserver vraagt de DNS records op van het domein wat achter het @-teken van het 'From' adres staat.
6. De ontvangende e-mailserver ziet in het DNS record dat er een public DKIM key opgegeven is.

7. Met behulp van deze public key valideert de ontvangende e-mailserver de handtekening in de headers van het e-mailbericht.

Stap 1: DKIM activeren door een private en public key te genereren

Om je berichten digitaal te ondertekenen, moet op je e-mailserver een public en private DKIM RSA keypair gegenereerd worden. Hoe je dat precies moet doen, is volledig afhankelijk van het type mailserver of de mailprovider wat je gebruikt.

Wanneer je DKIM geactiveerd hebt, dan krijg je van je mailprovider de '**public**' key te zien. Deze public key heb je straks nodig om in je DNS record te configureren.

Daarnaast krijg je ook een '**selector**'. Deze selector is uniek per e-mailserver. De selector van Google Workspace is bijvoorbeeld `google` en de selector van Plesk is `default`. Ook deze 'selectors' heb je straks nodig om je DNS record te configureren.

Een DKIM private/public key genereren in Google Workspace

Gebruik je Google Workspace als mailserver, dan kan je een DKIM private key genereren in het admin paneel onder 'Apps > Google Workspace > Settings for Gmail > Authenticate email'. Zodra je dat gedaan hebt, krijg je je public key te zien (deze heb je straks nodig).

Authenticate email

DKIM authentication

The domains you select will use the DKIM (DomainKeys Identified Mail) protocol for authenticating outgoing emails. [Learn more](#)

Selected domain

nexxwave.be ▼

Status: Authenticating email

You must update the DNS records for this domain.
To start authenticating email for the domain selected above, enter the following DNS TXT record into your domain provider's DNS settings page. Then click "Start authentication."

DNS Host name (TXT record name):
google._domainkey

DNS record value:
v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAh0CBz2grteSLM+tBTPcyaLV2TRsVnhTN3G72BUFOI35WS9fTuLHmtiu8jahjONVhvTtWKsu2Cx9gmzi2cVjFxp1+p13tbHNepJpr7tFdOxZyG9FupBv6VV4QnFtLY6tSx7Xw+RZJBty49vISl/iSysyaxztfnX3fRGodsfinvZnEc8uK3E1c9Y4PyotOeiXVitmYGFKG+ejn01iF8eS0T+5NLVdpCQkiVGJf73NN0Yjt2qSOD+6jGzMeXbkN9w0i/SNZYp/KyDoOrdmyXBIJfTjAP6XC0KtjCy4wC8BTj0al/IRlhywGJltKtIDxyipkQwOROGGPro4QU/mooEX70QIDAQAB

GENERATE NEW RECORD

It may take up to 48 hours for DNS changes to fully propagate.

STOP AUTHENTICATION

Most changes take effect in a few minutes. [Learn more](#)
You can view prior changes in the [Audit log](#)

CANCEL

SAVE

Een DKIM private/public key genereren in Plesk

Gebruik je het Plesk controlepaneel, dan kan je een private key generen in je 'Mail Settings'. Klik op 'How to configure external DNS' om je public key te zien.

Mail Settings for nexxwave-demo4.eu ▾

Email Addresses **Mail Settings** Outgoing Mail Control

This is where you can change the mail service settings for this domain.

☒ Activate mail service on this domain

Webmail Roundcube (1.4.13) ▾

SSL/TLS certificate for webmail Lets Encrypt nexxwave-demo4.eu ▾

SSL/TLS certificate for mail Lets Encrypt nexxwave-demo4.eu ▾

☒ Use DKIM spam protection system to sign outgoing email messages [? How to configure external DNS](#)

☒ Switch on greylisting spam protection for all mail accounts under this domain

* Required fields

OK

Apply

Cancel

Stap 2: de public key in je DNS opnemen

Kopieer de public key wat je verkregen hebt bij het aanmaken van je private key. Deze key plaats je in de DNS instellingen van je domeinnaam. Dit doe je door in te loggen op het DNS beheerpaneel van je DNS provider.

- Voeg een record van het type '**TXT**' toe.
- Afhankelijk van je domein provider, geef je als '**domeinnaam**' twee zaken op: je 'selector' gevolgd door `._domainkey`. Voor Google Workspace is dat bijvoorbeeld: `google._domainkey`.
- Als je het record ingeeft voor een subdomein, dan noteer je hier ook het subdomein. Bijvoorbeeld voor subdomein 'voorbeeld.nexxwave-demo4.eu' zou het record zijn: `google._domainkey.voorbeeld.nexxwave-demo4.eu`.
- Als **TTL** raden we aan om te starten met een lage waarde zodat wijzigingen wat je doet vlgug opgepikt kunnen worden. Neem bijvoorbeeld een TTL van 5 minuten: 300.
- Als **TXT-record** noteer je de public key wat je gekregen hebt. Afhankelijk van je domein provider, moet dit tussen "aanhalingstekens" getypt worden.

Record type	<div>TXT ▼</div>
Domain name	<div>default_domainkey</div> .nexxwave-demo4.eu.
TTL	<div></div> <div>Default value: 21600 seconds</div>
TXT record	<div>v=DKIM1; p=MIGfMA0GCSqGSib3DQEBAQUAA4GNADCBiQKBgQDhW8463YmgcuWHWCJOXraC</div>
* Required fields	<div>OK</div> <div>Apply</div> <div>Cancel</div>

Stap 3: validatie van je DNS record

Wanneer je TXT record online staat, controleer dan of het goed reageert op aanvragen. Dat kan vanaf je computer of via een online tool zoals deze van [MXToolbox](#):

Geef hiervoor het volledige adres van je TXT record op, met de 'selector'. Zoals in onderstaand voorbeeld: `google._domainkey.nexxwave.be`.


```
klowet@rackpc: ~  
[klowet@rackpc]~  
$dig txt google._domainkey.nexxwave.be  
  
; <<>> DiG 9.16.27-Debian <<>> txt google._domainkey.nexxwave.be  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64491  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
;; EDNS: version: 0, flags:; udp: 4096  
;; QUESTION SECTION:  
;google._domainkey.nexxwave.be. IN      TXT  
  
;; ANSWER SECTION:  
google._domainkey.nexxwave.be. 3588 IN  TXT      "v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ  
8AMIIBCgKCAQEAh0CBz2grteSLM+tBTPcyaLV2TRsVnhTN3G72BUF0l35WS9fTuLHmtiu8jahjONVhvTtWKsu2Cx9gmzi2cVj  
Fxp1+p13tbHNepJpr7tFd0xZyG9FupBv6VV4QnFtLY6tSx7Xw+RZJBty49vLSl/iSysyaxztfnX3fRGodsfinvZnEc8uK3E1c  
9Y4Pyot0eIXVi" "tmYGFKG+ejn0liF8eS0T+5NLVdpCQkIVGJf73NN0Yjt2qS0D+6jGzMeXbkN9w0i/SNZYp/KyDo0rdmyXB  
lJfTjAP6XC0KtjCy4wC8BTj0al/IRlhywGJIItKtIDxyipkQw0ROGGPro4QU/mooEX70QIDAQAB"  
  
;; Query time: 0 msec  
;; SERVER: 10.55.10.254#53(10.55.10.254)  
;; WHEN: Wed Jul 20 14:21:10 CEST 2022  
;; MSG SIZE rcvd: 482  
  
[klowet@rackpc]~  
$
```

Je kan ook een validatie van je DKIM record doen door vanaf al je e-mailservers een e-mail te sturen naar een (best extern) e-mailadres. In de headers van deze e-mail vind je terug of de DKIM validatie geslaagd al dan niet geslaagd is:

Message ID	<43d5b6d6ef15af4b13496b3b65288699@docs.nexxwave.be>
Created at:	Tue, Jul 19, 2022 at 4:07 PM (Delivered after 1 second)
From:	BookStack <bookstack@docs.nexxwave.be>
To:	kris.lowet@nexxwave.be
Subject:	Test Email
SPF:	PASS with IP 2a01:4f8:c17:2520:0:0:0:1 Learn more
DKIM:	'PASS' with domain docs.nexxwave.be Learn more
DMARC:	'PASS' Learn more

Wil je dieper in de headers duiken, dan zal je in je headers `DKIM-Signature` tegenkomen. Zie dit voorbeeld:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=docs.nexxwave.be; s=nexx; t=1658239666;  
bh=RbX1G9ID6lVhuqtj1C/P7MzkydOmr82ZR1lFtfu+pP8=; h=Date:Subject:From:To:From;  
b=hHW80WA8zh/pRKZ+smWDxmlLVQ21tdEb0rumXOhxyGig94uyGXGMleTOjvQFcmw0H  
[] VXH+m/L/pieUSroXb4xDD6DhTWkSuhes/FTDM951fmVcwu3ViaGGD0AUDXhHxcMpUP
```

```
□ bJzl+vy7AEwN0q03pCoFsR6lyfhydfq/grGORRCqb+LgAKRNpaX8tyg5728XhRmMmM
□ ybgElQ5rUUo4VaTSUF2F1wRd3R+EC9iRKv4Odg/dim/RifTxql2r0J24Z9D+mYpdHU
□ WmxbdVbZfupQC5KAsGwjhqTXZvqUyLV3lrwSDAfk9S9OLRCwHBrDx1WUHyuLREwJ0Q
□ 2yd5/eZ82Mbdg==
```

Hier vind je:

- `d=docs.nexxwave.be` = het domein van de afzender. De ontvangende e-mailserver gaat in de DNS records van dit domein de public DKIM key opzoeken.
- `s=nexx` = de selector wat in de e-mailserver geconfigureerd staat. Dus de ontvangende e-mailserver weet zo dat de public DKIM key te vinden is op adres `nexx._domainkey.docs.nexxwave.be`
- Vervolgens zie je de digitale handtekening achter `b=`.

Revisie #2

Gemaakt: 20 juli 2022 11:24:29 door Kris Lowet

Bijgewerkt: 20 juli 2022 12:37:02 door Kris Lowet