

DKIM record

WHAT IS THE DKIM RECORD?

DKIM is the abbreviation for DomainKeys Identified Mail. DKIM is not really a spam protection technology, it's a cryptographic signature that our mail server (that is, not our own machine) digitally signs on sending, protecting it against unauthorized modifications. Spam protection will take effect if you enter a rule in the domain TXT record so that the host server will dismiss all unsigned mails to protect the (as all unsigned emails are, as a rule, fake). This is useful if few users only email through 1-2 servers.

Signatures with the DKIM key are executed by the sender server.

DKIM signature is usually invisible to average users.

QUERYING DKIM RECORD

For example, you can use the nslookup command in Windows to access record DKIM, while under Linux the host command.

Example of a Windows-based nslookup query:

```
nslookup -q=TXT staff._domainkey.dotroll.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
staff._domainkey.dotroll.com  text =

    "k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDMGy34jPh1A9JPiDN+fHGuLPf0Kb0U752RW8UZti9F4/6BHZ
Vm1aYCNG+QZfy4RAdYTW2uyajuQKigzNemNgAmm6FOEerc+pUFI3CFI3+KzkFcjErSPL6oeZYp1Gs43j3nYb0MJWJt
tFJZkKKLpIPAKq4HccE52Uk3fs+qo4c9UQIDAQAB"
```

Example of Linux based host query:

```
host -t TXT staff._domainkey.dotroll.com
staff._domainkey.dotroll.com descriptive text "k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDMGy34jPh1A9JPiDN+fHGuLPf0Kb0U752RW8UZti9F4/6BHZ
Vm1aYCNG+QZfy4RAAdYTW2uyajuQKigzNemNgAmm6FOEerc+pUFI3CFI3+KzkFcjErSPL6oeZYp1Gs43j3nYb0MJWJt
tFJZkKKLpIPAKq4HccE52Uk3fs+qo4c9UQIDAQAB"
```

DKIM RECORD FORMAT

Fields name	Description
v=	set to the record type, the value will typically be <code>DKIM1</code> . Required element.
k=	specifies the type of generated key, which can be <code>dsa</code> or <code>rsa</code> . Required element.
g=	you can enter the detail of the key. Not required element.
h=	an authorized HASH algorithm that can be any <code>SHA1</code> or <code>SHA256</code> . Not required element.
n=	can be added a comment. Not required element.
s=	define the service type. Not required element.
t=	the given key can be assigned to a single subdomain name. Not required element.
p=	you can enter the public key part of the generated key pair. Required element.

Some service providers limit the length of the TXT record in 255 characters. If the received DKIM key is longer than 255 characters, the key can be truncated.

For example, the following DKIM key length is 411 characters:

```
v=DKIM1; k=rsa;
p=MIIBIjANBgqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAIv2kr5/XYymYzy1ynCe25/2AYsLaQtZMvKoXsa1W1qgF
fKFKmMw6vhcuLkII8FA8gJG18p9ww0XoP5wNZZOC02u9rrgoZt8FsuQmO6b/QJKNSuHEECr6hVD+H9C9zS9ThuQk2
qa3RtVO6apHCcw/DLpQ1DN14kNd7URNQIGZLKFgblGI1NwaCOLvUgqpFP/hOzk5veqG2qh50krPLrg6Lzjvd4pLx/5+
n87yvLXian3ZAjcVZ1lqT9O7UQtPu1mwPbjBH+odpc6xF3ZUFUoHLDpgxYmwW3z7ID7vTLERGkhxpzeI1+xQwYKG8I
M/ryO85cZ4ADRX7fqj/QUi1mzGwIDAQAB;
```

In this case, the key must be divided into two sections where the first part will be 254 characters long while the second part will contain the remaining 156 characters:

```
"v=DKIM1; k=rsa;
p=MIIBIjANBgqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAIv2kr5/XYymYzy1ynCe25/2AYsLaQtZMvKoXsa1W1qgF
```

```
fKFKmMw6vhcuLkII8FA8gJG18p9wwXoP5wNZZOC02u9rrgoZt8FsuQmO6b/QJKNSuHEECr6hVD+H9C9zS9ThuQk2
qa3RtVO6apHCcw/DLpQ1DN14kNd7URNQIGZLKFgblGI1NwaCOLvUgqpFP/"
```

```
"hOzk5veqG2qh50krPLrg6Lzjvd4pLx/5+n87yvLXian3ZAjcVZ1IqT9O7UQtPu1mwPbjBH+odpc6xF3ZUFUoHLDpgxY
mwW3z7ID7vTLERGhxpzeI1+xQwYKG8IM/ryO85cZ4ADRX7fqj/QUI1mzGwIDAQAB"
```

The DNS management interface can then be added, so that the subdomain name is given in the domain / subdomain box:

```
default._domainkey 14400 IN TXT "v=DKIM1; k=rsa; p=..."
default._domainkey 14400 IN TXT "hOzk5ve..."
```

ADDING DKIM RECORD

1. Sign in with <https://admin.dotroll.com> with your username and password
2. In the top menu bar, click the **Domains / My Domains** menu.
3. Select the domain name for which you want to make the change and then click on it.
4. In the **Manage** box on the left, select **Manage DNS**.
5. At the bottom of the page, click **Add**.
 - In the first field, you can enter a subdomain name, or leave blank
 - the TTL value can be selected in the second field, but typically the default is 1 hour
 - select **DKIM** from the next drop-down list.
 - set the desired values
6. Then click **Save Changes**.

Revision #1

Created 20 October 2023 09:39:55 by Judit Pásztor

Updated 20 October 2023 09:41:08 by Judit Pásztor