

# DKIM rekord

## MI AZ A DKIM REKORD?

A DKIM a DomainKeys Identified Mail rövidítése. A DKIM igazából nem egy spam védelmi technológia, hanem egy kriptográfiai aláírás, amelyet a levélküldő szerverünk (tehát nem a saját gépünk) a küldéskor digitálisan aláírja a levelet, így védve az illetéktelen módosítások ellen. Spamvédelem akkor lesz ebből, ha a domain TXT rekordjában olyan szabályt adunk meg, hogy a fogadó szerver minden aláíratlan levelet dobjon el, ezzel védekezve a nevükben írt e-mail-ek ellen (hiszen minden aláíratlan levél a szabály szerint hamisítvány). Ez akkor hasznos, ha kevés számú felhasználó kizárólag 1-2 szerveren keresztül levelezik.

A levelek DKIM kulccsal történő aláírását a levél küldő szerver végzi.

A DKIM aláírás általában az átlag felhasználók számára láthatatlan.

## A DKIM REKORD LEKÉRDEZÉSE

A DKIM rekord lekérdezéséhez használható Windows alatt például az nslookup parancs, míg Linux alatt a host parancs.

Példa egy Windows alapú nslookup lekérdezésre:

```
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"
```

Példa Linux alapú host lekérdezésre:

```
host -t TXT staff._domainkey.dotroll.com  
staff._domainkey.dotroll.com descriptive text "k=rsa\  
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDMGy34jPh1A9JPiDN+fHGuLPf0Kb0U752RW8UZti9F4/6BHZ  
Vm1aYCNG+QZfy4RAdYTW2uyajuQKigzNemNgAmm6FOEerc+pUFI3CFI3+KzkFcjErSPL6oeZYp1Gs43j3nYb0MJWJt  
tFJZkKKLpIPAKq4HccE52Uk3fs+qo4c9UQIDAQAB"
```

## A DKIM REKORD FORMÁTUMA

Használható elemek	Leírás
v=	ezzel állítjuk be a rekord típusát, értéke jellemzően <code>DKIM1</code> lesz, kötelező elem.
k=	a generált kulcs típusát adja meg, ami lehet <code>dsa</code> vagy <code>rsa</code> , kötelező elem.
g=	itt lehet megadni a kulcs részletességét, használata nem kötelező.
h=	engedélyezett HASH algoritmus, amely lehet minden, <code>SHA1</code> vagy <code>SHA256</code> , a használata nem kötelező.
n=	megjegyzést lehet hozzáfűzni, a használata nem kötelező.
s=	a szolgáltatás típust határozza meg, használata nem kötelező.
t=	az adott kulcsot hozzá lehet rendelni egyetlen aldomain névhez, használata nem kötelező.
p=	itt lehet megadni a generált kulcspár publikus kulcs részét, kötelező elem.

Egyes szolgáltatók 255 karakterben korlátozzák a TXT rekord hosszúságát. Ha a kapott DKIM kulcs hosszabb mint 255 karakter akkor a kulcsot fel lehet darabolni.

Például a következő DKIM kulcs hossza 411 karakter:

```
v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAI Dv2kr5/XYymYzy1ynCe25/2AYsLaQtZMvKoXsa1W1qgF
fKFKmMw6vhcuLkII8FA8gJG18p9ww0XoP5wNZZOC02u9rrgoZt8FsuQmO6b/QJKNSuHEECr6hVD+H9C9zS9ThuQk2
qa3RtVO6apHCcw/DLpQ1DN14kNd7URNQIGZLKFgblGI1NwaCOLvUgqpFP/hOzk5veqG2qh50krPLrg6Lzjvd4pLx/5+
n87yvLXian3ZAjcVZ1IqT9O7UQtPu1mwPbjBH+odpc6xF3ZUFUoHLDpgxYmwW3z7ID7vTLERgkxpxzEI1+xQwYKG8I
M/ryO85cZ4ADRX7fqj/QUi1mzGwIDAQAB;
```

Ebben az esetben a kulcsot fel kell osztani két részre, ahol az első rész 254 karakter hosszúságú lesz, míg a második rész fogja tartalmazni a maradék 156 karaktert:

```
"v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAI Dv2kr5/XYymYzy1ynCe25/2AYsLaQtZMvKoXsa1W1qgF
fKFKmMw6vhcuLkII8FA8gJG18p9ww0XoP5wNZZOC02u9rrgoZt8FsuQmO6b/QJKNSuHEECr6hVD+H9C9zS9ThuQk2
qa3RtVO6apHCcw/DLpQ1DN14kNd7URNQIGZLKFgblGI1NwaCOLvUgqpFP/"

"hOzk5veqG2qh50krPLrg6Lzjvd4pLx/5+n87yvLXian3ZAjcVZ1IqT9O7UQtPu1mwPbjBH+odpc6xF3ZUFUoHLDpgxY
mwW3z7ID7vTLERgkxpxzEI1+xQwYKG8IM/ryO85cZ4ADRX7fqj/QUi1mzGwIDAQAB"
```

A DNS kezelő felületen ezt követően már fel lehet venni, olyan módon, hogy a domain/aldomain mezőben ugyan az az aldomain név kerül megadásra:

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

## DKIM REKORD FELVÉTELE

1. Jelentkezzen be a <https://admin.dotroll.com> oldalon a felhasználói nevével és jelszavával
2. Kattintson a felső menüsorban a **Domainek / Domain neveim** menüpontra.
3. Válassza ki azt a domain nevet amelynél a módosítást szeretné elvégezni, majd kattintson rá.
4. A baloldali **Kezelés** dobozban válassza ki a **DNS kezelése** menüpontot.
5. Az oldal alján kattintson a **Hozzáad** gombra.
  - Az első mezőben megadhat szolgáltatás nevet, protokollt, aldomian nevet, vagy üresen is hagyhatja
  - a második mezőben kiválasztható a TTL érték, de jellemzően az alapértelmezett 1 óra megfelelő választás
  - a következő lehulló listából válassza ki az **DKIM** lehetőséget.
  - állítsa be a kívánt értékeket
6. Ezt követően kattintson a **Változások mentése** gombra.

