How do I create a DKIM DNS record?

This article introduces the *DomainKeys Identified Mail* or *DKIM* record to you - a type of DNS record that allows for digitally signing of (parts of) an e-mail. It is a useful e-mail security tool to identify the sender of the e-mail and authenticate the contents of the message.

Together with SPF and DMARC, DKIM is a crucial element of e-mail security.

This article contains the following sections:

Introduction: the purpose of DKIM

The DKIM technology uses a very common protocol to verify that an e-mail was sent from an authorised server: it uses "public key cryptography", a standard that everybody knows from SSL certificates.

If DKIM is enabled, the sending mail server will digitally sign (a part of) the e-mail before it's transmitted to the recipient. The receiving mail server uses publicly available DNS records to verify the signature. If the verification succeeds, the recipient knows for sure that the e-mail was untampered with.

> *The idea behind public key cryptography is, that the signing key consists of two elements: a private key that nobody knows except the owner, and a public key that is available to everybody. Those two keys are related to each other: only a text encrypted with the private key can be decrypted with the public key; and a text encrypted with the public key can be decrypted with the private key only. In other words: if you can decrypt the message with the public key, you are sure it was signed with the private key that only the owner knows. And if you encrypt a message with the public key, you are sure that nobody except the owner of the private key can decrypt it.*

The signature that the sending mail server adds, is included as a header to the e-mail. The receiving mail server can read in this header which parts of the e-mail it should verify, and where it can find the public key for verification.

Important note: if you want to use DKIM, your mail server must be capable of it. Check with your hosting provider or system engineer for details on activating DKIM on your mail server. A useful read is the blog of registry SIDN, who has published how-tos for Exim and Postfix that you might want to refer to. This article only describes the DNS records involved in DKIM validation.

Note on e-mail forwarding: e-mail forwarding and DKIM is a tricky combination. E-mail forwarding often changes parts of the e-mail: the sender changes, the body can change (for example because a virus scanner adds a note), and so on. If your DKIM implementation signs parts of the e-mail that change during the forwarding, the DKIM signature check can no longer be performed. Keep this in mind when configuring DKIM.

DKIM records in Openprovider

The Openprovider DNS management supports the TXT type for DNS records, that can be used to store DKIM information. The contents of the DKIM record depends on the sending mail server; your provider or system engineer is able to provide you with the correct record.

The name of the record is also important: DKIM information is not stored at the highest level, but as a subdomain which includes _domainkey:

```
default._domainkey
```

or, more general,

```
something._domainkey
```

The DKIM record now is available through *default._domainkey.yourdomain.com* or *something._domainkey.yourdomain.com*.

DKIM record syntax

Note that in most cases, your outgoing mail server provider will send you the exact contents to put in the DNS record. For understanding the syntax of this record, these are the most important elements of a DKIM record:

- **v=** is the version number; at the moment of writing this is always DKIM1
- **k=** is the key type; in most cases this is *rsa*
- **p=** is the public key used for verifying the signatures
- **t=** can tell the receiving mail server that the sending server is just testing, and signatures should be ignored even if they are invalid

Putting all this together, a valid DKIM record in the DNS may look like this:

```
default._domainkey.yourdomain.com    TXT    "v=DKIM1; t=y; k=rsa; p=MIGfMA0GCSqGS[...]A2CA;"
```

DKIM for domains without e-mail

DKIM is useful as well if a domain is not intended to send e-mail. In that case, declare the following DKIM record in your DNS:

```
*._domainkey TXT "v=DKIM1; p="
```

Useful documentation

- The website dkim.org contains full syntax documentation and references to a lot of other documentation and information.

Revision #2
Created 2026-08-07 14:31:48 UTC by Sarath
Updated 2026-08-07 15:48:36 UTC by Sarath