

DKIM Einrichtung - Mail Gateway

Allgemeine Infos:

Dieser Artikel beschreibt, wie Sie DKIM für unser ausgehendes Mailgateway erstellen können.

DKIM ist eine E-Mail-Authentifizierungsmethode zur Erkennung gefälschter Absenderadressen in E-Mails. Beim Signieren ausgehender Nachrichten mit DKIM können Empfänger überprüfen, ob eine entsprechende Nachricht von dem Absender stammt, von dem sie angeblich stammt, und dass der Inhalt der Nachricht nicht geändert wurde.

Dieser Artikel gilt nur in Verbindung mit dem Produkt: **profi Spamschutz AUSGEHEND** oder **profi Spamschutz KOMPLETT**

1. Login

Loggen Sie sich am Mail Gateway ein.

2. Gehen Sie zum Menüpunkt **Ausgehend - DKIM**

Wir empfehlen Ihnen die Schlüssellänge 2048 Bits, bitte Überprüfen Sie ob Ihr DNS Anbieter diese Schlüssellänge unterstützt.

DKIM ()

Here you can generate a DKIM certificate for your domain. Please fill the form below with the desired selector you've chosen earlier. As a result you will get a value for public key which should be available in your DNS. After successful DKIM generation you should enable the resulting DKIM certificate for each outgoing user using your selector.

DKIM key length: ☒ DKIM length 2048 bits (Recommended)
☐ DKIM length 1024 bits (Only can be used if unable to use a 2048 bit key DNS provider)

DKIM selector:

✓ Generate and save new private/public pair

Wählen Sie anschließend einen DKIM Selector, wir empfehlen Ihnen **mmg**, dieser kann frei gewählt werden.

Klicken Sie auf den generieren Button, ihnen wird nun der DNS Eintrag angezeigt.

DKIM ()

Here you can generate a DKIM certificate for your domain. Please fill the form below with the desired selector you've chosen earlier. As a result you will get a value for public key which should be available in your DNS. After successful DKIM generation you should enable the resulting DKIM certificate for each outgoing user using your selector.

Generation successful!

DKIM public key (for DNS record):

```
v=DKIM1; k=rsa;  
p=MlIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1e3ik86SejEPnU5Q27B1r1RzDDcqo8bs5hLiVqaraXopOAxV+1RAD5PolF4r7u1UPMmEn  
  
/typvOn3BCsgSr5L2UmJmZnzSEhyiFGcwCT8owIDAQAB;
```

Associated DKIM private key has been stored internally

DKIM key length: ☒ DKIM length 2048 bits (Recommended)
☐ DKIM length 1024 bits (Only can be used if unable to use a 2048 bit key DNS provider)

DKIM selector:

3. DKIM aktivieren

Navigieren Sie nun zu Ausgehend - Ausgehende Benutzer und wählen Sie Ihren Benutzer. Tragen Sie anschließend im Feld DKIM Selector Ihren vorher gewählten Wert ein, z. B. **mmg**.

Nach dem Klick auf Speichern werden Ihre ausgehenden Mails signiert.

Outgoing user settings

Underneath you can manage the outgoing user settings.

Username:

Password:

Confirm password:

Domain:

Identification method: ⓘ

Automatic lock:

Lock identities automatically:

User and identity lock timeout:
(in minutes)

Maximum unlocks by timeout:

Enable outgoing connection limits: ☒ ⓘ

Limit per month:

Limit per week:

Limit per day:

Limit per hour:

Limit per minute:

DKIM selector:

Maximum number of recipients per day:
(0 is unlimited)

Quarantine response:

Message archiving for senders: ☐ ⓘ

4. Erstellen Sie den notwendigen DNS Eintrag

Fügen Sie einen neuen DNS Eintrag bei Ihrer Domain hinzu.

Name: selector._domainkey.example.tld --> Beispiel: mmg._domainkey.testdomain.de

Typ: TXT

Wert: Ihr angezeigter Key

Prio: 0
TTL: 3600

Hinweis: Das DNS System von FISINGER.de kürzt den **Namen** um die Domain. Somit sieht der Eintrag wie folgt aus: **mmg._domainkey**

DNS Record bearbeiten

(ID: 1674978890)

Name:

mmg._domainkey

Typ:

TXT

Wert:

v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMXXXXXcqp8bs5hLiVt

Prio:

0

TTL:

300

✓ Speichern

🌐 DynDNS anlegen

🗑️ Löschen

✕ Schließen

Revision #3

Created 29 November 2024 06:37:27 by Thomas Fisinger

Updated 29 November 2024 07:13:37 by Thomas Fisinger