

DKIM/SPF/DMARC einrichten mit externen DNS Server

<https://nissel.it/index.php/2020/03/06/dkim-einrichten-mit-externen-dns-server/>

DKIM Plesk Konfiguration

In den Mail Settings der Domain sollte die Verschlüsselung und DKIM aktiviert sein.

Mail Settings for [redacted] ...

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

What to do with mail for non-existent users *

Bounce with message

This address no longer accepts mail.

Forward to address

[redacted]

The address should belong to the selected domain. Only the admin external address or one address for several domains.

Reject

None ▾

The webmail component was not installed.

Webmail

SSL/TLS certificate for webmail

Not selected ▾

SSL/TLS certificate for mail

Lets Encrypt [redacted] ▾

Use DKIM spam protection system to sign outgoing email messages

Enable mail autodiscover

* Required fields

OK

Apply

Cancel

DKIM DNS Eintrag erstellen

Skript zum Auslesen des dkim keys und direktes umwandeln in String für den DNS Eintrag:

```
#!/bin/bash

DOMAIN=$1

KEY=$(openssl rsa -in /etc/domainkeys/${DOMAIN}/default -pubout 2> /dev/null | tail -n 5 | head -n 4 | tr -d '\n')
echo "v=DKIM1;k=rsa; p=${KEY};"
```

Der eigentliche Befehl ist "openssl rsa -in /etc/domainkeys/\${DOMAIN}/default -pubout" danach wird mit "tail" und "head" der Anfang und das Ende abgeschnitten. Danach werden mit "tr" die Zeilenumbrüche entfernt. "2> /dev/null" unterdrückt die Ausgabe "writing RSA key" und alle Fehlerausgaben.

```
# dkim-print nissel.it
v=DKIM1;k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDzZmnbucDR9uEiT
EqW3oXUuFZ+2c+VcFp91vy5SGg+CqbvFaAzUTn008Ew4QK9TrZ+dvuGj2qMMXEjmZVhFK+
G8JRCxItQDQ2T6taHlrGpjom6+EBctpaD9hjUuart3Hqn1fSS8MyOTVxwG6jArWuLg95Uj
Ms1NRCyUkqjHjoGIwIDAQAB;
```

Damit kann dann ein DNS TXT Record mit dem Schlüssel default._domainkey erstellt werden.

```
default._domainkey TXT v=DKIM1;k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNAD  
CBiQKBgQDzZmnbucDR9uEiTEqW3oXUuFZ+2c+VcFp91vy5SGg+CqbvFaAzUTn008Ew4QK9  
TrZ+dvuGj2qMMXEjmZVhFK+G8JRCxItQDQ2T6taHlrGpjom6+EBctpaD9hjUuart3Hqn1f  
SS8MyOTVxwG6jArWuLg95UjMs1NRCyUkqjHjoGIwIDAQAB;
```

SPF

Versucht ein fremder Mailserver im Namen der eigenen Domain eine Email zu versenden, unterbindet dieser Eintrag dies. Es wird nur erlaubt, dass A und MX record Einträge eine Mail verschicken dürfen. Das -all verbietet alles andere.

```
TXT v=spf1 +a +mx -all
```

Mit ~all wird diese Regel nicht strickt angewandt.

DMARC

Zuletzt wird die DKIM uns SPF durch DMARC kombiniert. Falsch signierte und Mails die nicht den SPF Regeln entsprechen werden in Quarantäne gestellt.

```
_dmarc TXT v=DMARC1; p=quarantine; rf=afrrf; rua=mailto:admin@domain.de  
; ruf=mailto:admin@domain.de
```

Globale Einstellungen in Plesk

Server-Wide Mail Settings

Settings Black List White List Mail Queue

General options

Enable mail management functions in Plesk

Installed mail server Postfix
You can install and use another mail server if?

Install and use another IMAP/POP3 server Dovecot
You can install and use another IMAP/POP3 server if?

Maximum message size Kbytes

Maximum number of connections (IMAP, POP3, IMAP over SSL/TLS, or POP3 over SSL/TLS)
The maximum number of mail users that can be logged in at the same time.

Maximum number of connections for a user per IP address
The maximum number of connections (IMAP, POP3, IMAP over SSL/TLS, or POP3 over SSL/TLS) allowed for a user per IP address

Enable SMTP service on port 587 on all IP addresses

Outgoing mail mode

- Send from domain IP addresses
- Send from domain IP addresses and use domain names in SMTP greeting
- Send from the specified IP addresses

IPv4

IPv6

Enable mailbox quota warning
Send a notification to mail users when their mailbox quota usage exceeds 95%
[Customize the default mailbox quota warning](#)

Mail autodiscover

Enable mail autodiscover
Enabling this feature reconfigures all domains that have autodiscover turned on

Specify a custom domain name for mail autodiscover
Note: The domain name must be secured with a valid SSL/TLS certificate.

Relay options

Relaying

- closed
- authorization is required:
 - POP3 before SMTP lock time min
 - SMTP

Turn on limitations on outgoing email messages

The following limits are default. They can be overridden in each service plan and subscription. The limits do not work server-wide.

Default limit on outgoing messages from a mailbox (per hour) Unlimited

Default limit on outgoing messages from a domain (per hour) Unlimited

Default limit on outgoing messages from a subscription (per hour) Unlimited

Allow users and scripts to use Sendmail
Scripts and users will be able to send email messages (on behalf of the subscription's system user) by using it. It acts as a default setting for service plans and subscriptions.

Show reports based on statistics for the last
The reports are created and the alert is shown on the Home page about attempts to exceed limits on outgoing mail.

Send an email notification entry
The notifications provide statistics on attempts to exceed limits on outgoing mail during the specified period.

Antivirus settings

Used antivirus None Plesk Premium Antivirus

DMARC

Enable DMARC to check incoming mail
This option is available when DKIM and SPF are switched on for incoming mail.

DKIM spam protection

Allow signing outgoing mail

Verify incoming mail
This option cannot be switched off while DMARC is switched on for incoming mail.

SPF spam protection

Enable SPF spam protection to check incoming mail
This option cannot be switched off while DMARC is switched on for incoming mail.

SPF checking continues when there are DNS lookup problems
First, SPF performs a DNS lookup. Select this option to continue checking if the DNS lookup fails. This option

SPF checking mode
Then, SPF applies local and guess rules. The message can be rejected depending on the selected checking mode.

SPF local rules

SPF guess rules

SPF explanation text

Turn on spam protection based on DNS blackhole lists

DNS zones for DNSBL service
Separate entries with a semicolon, for example: 'zen.spamhaus.org:dbn1.example.net'

Linux: Ubuntu 18.04.4
Plesk: Obsidian 18.0.24