

Domainkeys (DKIM) mit exim

DKIM: Zertifikat erstellen Werden die folgenden beiden Befehle ausgeführt

```
openssl genrsa -out dkim.private.key 2048
openssl rsa -in dkim.private.key -out dkim.public.key -pubout -outform PEM
```

werden zwei Dateien erstellt. Der private RSA Schlüssel in der Datei dkim.private.key und der öffentlich RSA Schlüssel in der Datei dkim.public.key.

DKIM: exim Konfiguration Im Abschnitt Transport-Konfiguration in der Datei configure sollte remote_smtp definiert sein. Unter driver = smtp wird die DKIM-Konfiguration erstellt:

```
remote_smtp:
    driver = smtp
    dkim_domain = example.com
    dkim_selector = x
    dkim_private_key = dkim.private.key
    dkim_canon = relaxed
```

Die dkim-Optionen müssen unter der driver-Option stehen.

Der DKIM Selector x wird im nächsten Schritt für die Nameserver Konfiguration verwendet. Für dkim_canon siehe Abschnitt 3.4 Canonicalization in RFC 4871

DKIM: DNS Konfiguration Für die bisher beschriebene Konfiguration werden zwei Zeilen im Zonefile ergänzt:

```
_domainkey.example.com.      IN TXT "t=y; o=~;"
x._domainkey.example.com.    IN TXT "v=DKIM1; t=y; k=rsa; p=<public key>"
```

<public key> ist ein Platzhalter für den Inhalt der Datei dkim.public.key. Aus dem kompletten Inhalt, der z.B. so aussehen kann

```
-----BEGIN PUBLIC KEY-----
MHwwDQYJKoZIhvcNAQEBBQADAwAwaAJhAK7uSvR8LJZX2cV8hBfaPIbWKDji3u04
cUT+0r9vipXD9F0sviSoI/sjGQ9bhxG/Usb/CgJFF9NZMkJ6C0Htugr8iXBhXDV0
9mZEQKTp7zIKP4bEio8bMeeaNMzlkij/hwIDAQAB
-----END PUBLIC KEY-----
```

werden nur die drei Zeilen zwischen ---BEGIN PUBLIC KEY--- und ---END PUBLIC KEY--- benötigt. Außerdem sollten die Zeilenumbrüche entfernt werden.

Nach laden der neuen Konfigurationen von BIND und exim sollten ausgehende E-Mails für die Domain example.com automatisch signiert werden.

DKIM: Testen Z.B. eine E-Mail zu der eigenen gmail Adresse senden und sich den Quelltext der Datei ansehen. Folgende Zeilen sollten zu finden sein:

Received-SPF: pass (google.com: best guess record for domain of mail@example.com designates 192.168.0.2 as permitted sender) client-ip=192.168.0.2;

Authentication-Results: mx.google.com; spf=pass (google.com: best guess record for domain of mail@example.com designates 192.168.0.2 as permitted sender) smtp.mail=mail@example.com; dkim=neutral header.i=@example.com

DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; d=example.com; s=x;

From:

<http://wiki.richter-ch.de/> - **Wiki.Richter-Ch.de**

Permanent link:

<http://wiki.richter-ch.de/doku.php?id=wiki:computer:linux:eisfair:dkim>

Last update: **2024/02/21 11:05**

