Todo:

- Wie aktualisiert man `/var/spool/postfix/etc/ssl/certs/ca-certificates.crt`? Wird das bei Debian genutzt?
- DH-Parameter einbinden [1)]

Vorraussetzungen

- Einfache postfix Installation
- ssl Zertifikat erzeugt
- Korrektes DNS
- Korrekte Uhrzeiten auf allen Rechnern

SSL / TLS für Postfix

Server-Zertifikat für verschlüsselte Verbindungen

Wie in ssl beschrieben Server-Zertifikat bauen

```
cd /etc/ssl
cp /root/server-ssl/servercert.pem certs/
cp /root/server-ssl/serverkey.pem  private/
cp /home/ca/ca.*/cacert.pem  certs/
```

```
chmod 640 private/serverkey.pem
chgrp ssl private/serverkey.pem
```

openSuSE 12.1

postfix Benutzer Zugriff auf ssl-Verzeichnis erlauben

```
gpasswd -a postfix ssl
```

Postfix konfigurieren

```
postconf -e "smtpd_use_tls = yes"
postconf -e "smtpd_tls_cert_file = /etc/ssl/certs/servercert.pem"
postconf -e "smtpd_tls_key_file  = /etc/ssl/private/serverkey.pem"
postconf -e "smtpd_tls_CAfile    = /etc/ssl/certs/cacert.pem"
```

oder besser wie von Mozilla vorgeschlagen [2)]

testen

```
netcat localhost smtp
EHLO asdf
```

..

```
250-STARTTLS
```

```
openssl s_client -starttls smtp -CApath /etc/ssl/certs -connect localhost:25
```

```
swaks -f me.example.com -t you.example.com -tls -s 127.0.0.1
```

DANE

DNS Resource Record erzeugen:

```
postfix tls output-server-tlsa
```

oder

```
postfix tls output-server-tlsa
/var/lib/dehydrated/certs/brahma.kramskrims.de/privkey.pem
```

Den TLSA Resource Record muss man immer neu erzeugen, wenn der öffentliche Schlüssel des Zertifikats sich ändert. TODO: certbot oder dehydrated so aufrufen, dass der bisherige Schlüssel wieder verwendet wird.

... und im DNS hinterlegen.

Dokus & Links

- http://www.state-of-mind.de/vortraege/
- http://www.postfix.org/TLS_README.html
- http://sys4.de/de/blog/2013/08/14/postfix-tls-forward-secrecy/
- https://blog.tausys.de/2016/07/13/letsencrypt-zertifikate-fuer-dovecot-und-postfix/

1)
`smtpd_tls_dh1024_param_file = ${config_directory}/dhparams.pem` in /etc/postfix/main.cf
2)

main.cf

```
# generated 2022-09-23, Mozilla Guideline v5.6, Postfix 3.5.13, OpenSSL
1.1.1n, intermediate configuration
```

```
#
https://ssl-config.mozilla.org/#server=postfix&version=3.5.13&config=in
termediate&openssl=1.1.1n&guideline=5.6
smtpd_tls_security_level = may
smtpd_tls_auth_only = yes
smtpd_tls_cert_file = /path/to/signed_cert_plus_intermediates
smtpd_tls_key_file = /path/to/private_key
smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1
smtpd_tls_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1
smtpd_tls_mandatory_ciphers = medium

# curl https://ssl-config.mozilla.org/ffdhe2048.txt > /path/to/dhparam
# not actually 1024 bits, this applies to all DHE >= 1024 bits
smtpd_tls_dh1024_param_file = /path/to/dhparam

tls_medium_cipherlist = ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-
GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-
RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384
tls_preempt_cipherlist = no
```