R|R|Z|N|

Server-Zertifikate

R|R|Z|N

Anleitung suchen: ->www.rrzn->uh-ca-server->anleitung

Der Rest dieser Bemerkungen ist nur zu verstehen, wenn man gleichzeitig die Anleitung vor sich hat.

Schlüsselpaar erstellen (rsa 2048, Format pem) ->server.key,server.req

Aus Anleitung abschreiben, -nodes nicht vergessen (wg autostart ohne Passphrase)

Beantragung: server.req->Zum Zertifizieren schicken

Teilnahmeerklärung ausfüllen, in CA abgeben

Auf E-Mail warten,->2 E-Mails->1 Nummer

R|R|Z|N

Download: Schlüssel mit Zertifikat ->server.crt
drei Ober-CA-Zertifikate holen, zusammenkopieren:
cat dfn... top... cacert... .pem >ca_bundle.crt

Umkopieren nach /etc/ssl/certs und /etc/ssl/private
private key schützen (chmod, chgrp)

Sicherheitskopie verschlüsselt aufbewahren

gpg --gen-key mit User froriep # passphrase
gpg -e datei mit User froriep # encrypt
gpg -d datei mit Passphrase # decrypt

Reste entfernen
Ablauftermin z.B. in Kalender eintragen

R|R|Z|N

Beispiel Apache2:

server.key->.../ssl.key/
server.crt->.../ssl.crt/
ca_bundle.crt->.../ssl.crt/
make in .../ssl.crt/
httpd.conf: SSLCA-zertifikatdatei=..ca-bundle.crt
Apache restart
Testen

Hinweis: Passphrase entfernen: openssl rsa -in server.key -out server.key