Einleitung:

(1) gunicron installieren:

    sudo apt install gunicorn3 // Für Python3

(2) Generierung von Certificate und Primary Key (Self-Certificate)

openssl req -x509 -newkey rsa:4096 -nodes -out cert.pem -keyout key.pem -days 365
- (req) PKCS#10 X.509 Certificate Signing Request
- (rsa) RSA key management
- (nodes) If this option is specified then if a private key is created it will not be encrypted.

(3) 1.Variante (certificate direkt mit Gunicorn aufrufen)

gunicorn3 --certfile cert.pem --keyfile key.pem -b 0.0.0.0:5000 app:app
- certfile:
- keyfíle:
- b:

(4) 2.Variante: apache2 konfigurieren

cd /etc/apache2/sites-enabled
sudo vim default-ssl.conf

ServerName localhost
SSLEngine on
ProxyPass / http://localhost:5000
ProxyPassReverse / http://localhost:5000
SSLCertificate /etc/ssl/certs/cert.pem
SSLCertificateKeyFile /etc/ssl/private/key.pem