

# Table of Contents

- Cert Identity Search** ..... 1
- OpenSSL conf** ..... 1
- PGP Keyserver** ..... 1
  - Hardware Acceleration** ..... 1
  - Check OpenSSL throughput** ..... 1
  - Performance remarks** ..... 1
  - OpenSSL Cipher list** ..... 2
  - OpenSSL Performance test** ..... 2
  - My preferred string for now** ..... 2
  - Test StartTLS** ..... 2
  - Encrypt tar with password** ..... 2
  - Install additional CA in CentOS / Redhat** ..... 3
  - Self signed certificate + altname** ..... 3

# Cert Identity Search

<https://crt.sh/>

## OpenSSL conf

CentOS location

```
/etc/pki/tls/openssl.conf
```

## PGP Keyserver

<https://keyserver.pgp.com/vkd/GetWelcomeScreen.event>

## Hardware Acceleration

Check if AES-NI is enabled

```
grep -ml -o aes /proc/cpuinfo
```

Check speed

```
openssl speed aes-128-cbc  
openssl speed -evp aes-128-cbc  
openssl speed -evp chacha20
```

## Check OpenSSL throughput

```
dd if=/dev/zero count=100 bs=1M | ssh -c aes128-cbc localhost "cat  
>/dev/null"
```

## Performance remarks

<b>Decrypting a 1MB file on the Galaxy Nexus (OMAP 4460 chip)</b>	
AES-128-GCM	41.6ms
ChaCha20-Poly1305	13.2ms

AES128 vs AES256 1.38x faster

AES128 faster on desktop due to AES-NI HW Acceleration AES-NI is between 4-8x the performance of AES

ChaCha20-Poly1305 faster on mobile phones or slower HW

## OpenSSL Cipher list

```
# openssl ciphers | sed 's/\:/\n/gi'
```

## OpenSSL Performance test

```
# openssl speed md5 sha1 sha256 sha512 des des-ede3 aes-128-cbc aes-192-cbc  
aes-256-cbc rsa2048 dsa2048
```

## My preferred string for now

Functional with HTTP/2 protocol

```
ssl_session_timeout 4h;  
ssl_session_cache shared:SSL:40M;  
ssl_protocols TLSv1.2 TLSv1.3;  
ssl_prefer_server_ciphers on;  
ssl_ciphers !aNULL:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-  
SHA256;  
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains;"
```

## Test StartTLS

```
openssl s_client -connect ip:21 -starttls ftp -showcerts  
openssl s_client -connect ip:25 -starttls smtp -showcerts
```

## Encrypt tar with password

Compress and encrypt

```
tar cvfz - * | openssl enc -e -aes128 -out secured.tar.gz
```

Decrypt and decompress

```
openssl enc -d -aes128 -in secured.tar.gz | tar xvz -C test
```

## Install additional CA in CentOS / Redhat

```
place CA here -> /etc/pki/tls/certs/cert.pem
yum install /usr/bin/c_rehash
c_rehash
```

## Self signed certificate + altname

```
set -e

if [ -z "$1" ]; then
    hostname="$HOSTNAME"
else
    hostname="$1"
fi

local_openssl_config="
[ req ]
prompt = no
distinguished_name = req_distinguished_name
x509_extensions = san_self_signed
[ req_distinguished_name ]
CN=$hostname
[ san_self_signed ]
subjectAltName = DNS:$hostname, DNS:localhost
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = CA:true
keyUsage = nonRepudiation, digitalSignature, keyEncipherment,
dataEncipherment, keyCertSign, cRLSign
extendedKeyUsage = serverAuth, clientAuth, timeStamping
"

openssl req \
    -newkey rsa:2048 -nodes \
    -keyout "$hostname.key.pem" \
    -x509 -sha256 -days 3650 \
    -config <(echo "$local_openssl_config") \
    -out "$hostname.cert.pem"
openssl x509 -noout -text -in "$hostname.cert.pem"
```

From:  
<https://wiki.janforman.com/> - [wiki.janforman.com](https://wiki.janforman.com/)

Permanent link:  
<https://wiki.janforman.com/cryptography>

Last update: **2019/11/11 12:38**



