PKCS#12

, , PKCS#12.

hpd

```
#       10         .rt,  -  .key,       .pem
openssl req  -newkey rsa:2048 -x509 -nodes -days 3650 -subj "/C=RU/ST=Moscow/L=Zelenograd/O=Latera Software LLC
/OU=Development section/CN=Latera Software development section/emailAddress=info@latera.ru" -keyout server.key -
out server.crt
cat server.crt server.key > server.pem

#
#     nginx
openssl req  -new -key server.key -out client.csr -config /usr/lib/ssl/openssl.cnf -subj "/C=RU/ST=Moscow
/L=Zelenograd/O=Latera Software LLC/OU=Development section/CN=Latera Software development section
/emailAddress=info@latera.ru"
openssl x509 -req -days 3650 -in client.csr   -signkey server.key -CA server.crt -CAkey server.key -
CAcreateserial -out ssl.crt && cat ssl.crt server.key > ssl.pem

# cyberplat   ssl-      ,   csr-  Cyberplat
#cyberplat.key -   ,       .      server.key,          ( )
#       cyberplat- private_key,      cyberplat.crt   Cyberplat
#   public_key   ,    Cyberplat
openssl rsa  -in server.key -out cyberplat.key
openssl x509 -req -days 365 -in Cyberplat.csr -signkey server.key -CA server.crt -CAkey server.key -
CAcreateserial -out cyberplat.crt -sha256
```

, .

RSA (RSA private key)

:

```
openssl genrsa -out <Key Filename> <Key Size>
```

:

- <Key Filename> — ;
- <Key Size> — . : 1024, 2048, 4096.

:

```
openssl genrsa -out private_key.key 4096
```

(Certificate Signing Request)

SSL- (Certificate Signing Request) . CSR , .

CSR : (Country), (State/Province), (Locality/City), (Organization), (Organizational Unit) (Common Name). :

1. "" .
2. "" "" .
3. "" — , .
4. "" — , , "IT".
5. " " — , .

:

```
openssl req -new -key <Key Filename> -out <Request Filename> -config /usr/lib/ssl/openssl.cnf
```

:

- <Key Filename> — RSA;
- <Request Filename> — .

, , . , .

:

```
user@server:~$ openssl req -new -key private_key.key -out request.csr -config /usr/lib/ssl/openssl.cnf

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----
Country Name (2 letter code) [AU]: RU

State or Province Name (full name) [Some-State]: Moscow

Locality Name (eg, city) []: Zelenograd

Organization Name (eg, company) [Internet Widgits Pty Ltd]: Latera Software LLC

Organizational Unit Name (eg, section) []: Development section

Common Name (e.g. server FQDN or YOUR name) []: Latera Software development section

Email Address []: info@latera.ru
```

(Self-signed public certificate)

:

```
user@server:~$ openssl x509 -req -days <Amount days> -in <Request Filename> -signkey <Key Filename> -out
<Certificate Filename>
```

:

- <Amount days> — , ;
- <Request Filename> — (**Certificate Signing Request**);
- <Key Filename> — , RSA;
- <Certificate Filename> — (**Self-signed public certificate**).

:

```
user@server:~$ openssl x509 -req -days 3650 -in request.csr -signkey private_key.key -out pub_cert.crt
```

PKCS#12

:

```
user@server:~$ openssl pkcs12 -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES -export -in <Public Certificate Filename> -inkey <Private Key Filename> -out <PKCS#12 Filename> -name "<Display Name>"
```

:

- <Public Certificate Filename> — (S**elf-signed public certificate**) PEM-;
- <Private Key Filename> — , RSA;
- <PKCS#12 Filename> — **PKCS#12** ( );
- <Display Name> — , .

:

```
user@server:~$ openssl pkcs12 -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES -export -in pub_cert.crt -inkey private_key.key -out my_pkcs12.pfx -name "TEST"
```

PEM- :

```
user@server:~$ openssl pkcs12 -in <PKCS#12 Filename> -out <PEM File> -nodes
```

:

- <PKCS#12 Filename> — **PKCS#12** ( );
- <PEM File> — PEM-

:

```
user@server:~$ openssl pkcs12 -in my_pkcs12.pfx -out my_pem.pem
```

HPD

RSA (**Self-signed public certificate**) PEM-, hpd.conf HTTPS- .

:

```
user@server:~$ cat <Public Certificate Filename> <Key Filename> > <PEM File>
```

:

- <Public Certificate Filename> — (**Self-signed public certificate**) PEM-;
- <Private Key Filename> — RSA;
- <PEM File> — PEM-

:

```
user@server:~$ cat pub_cert.crt private_key.key > cv-ssl.pem
```

PEM- **/etc/hpd/cert** (**/etc/hydra/hpd/cert**), **hpd.conf**, HTTPS- .

:

```
...

cv-ssl server status = on
cv-ssl server ip = 0.0.0.0
cv-ssl server port = 9444

#   PEM-  HTTPS-
cv-ssl server pem path = /etc/hpd/cert/cv-ssl.pem

cv-ssl server plugins list = osmp

...
```