Сертификаты SSL

Сертификаты могут лежать в нескольких местах

```
/etc/ssl/
```

```
/etc/letsencrypt/archive/доменное имя
```

```
/etc/letsencrypt/live/доменное имя
```

Создание Сертификата SSL через openssl

```
openssl req -new -x509 -days 1461 -nodes -out /etc/ssl/public.pem -keyout
/etc/ssl/private.key -subj "/C=RU/ST=SPb/L=SPb/O=Global Security/OU=IT
Department/CN=Ваше доменное имя"
```

> Где **/etc/ssl/** путь к сертификату

Создание сертификата SSL через certbot

Apache

```
certbot certonly --webroot --agree-tos --email service@fellk.ru --webroot-
path /var/www/html/ -d fellk.ru -d www.fellk.ru
```

TXT вашего хостера

```
certbot certonly --manual --agree-tos --email service@fellk.ru --preferred-
challenges=dns -d fellk.ru -d www.fellk.ru
```

На запрос отвечаем Y и получаем подобное сообщение

> Please deploy a DNS TXT record under the name _acme-challenge.fellk.ru with the following value:

VHFPbXt82j2oUjhxVgS7Bphpkf3Cv1Bq9KSA2dd

Once this is deployed,

Теперь идем к хостеру и создаем там TXT-запись _acme-challenge.fellk.ru с содержимым **VHFPbXt82j2oUjhxVgS7Bphpkf3Cv1Bq9KSA2dd**

Создание сертификата SSL через certbot на все поддомены

```
certbot certonly --manual --agree-tos --email service@fellk.ru --server https://acme-v02.api.letsencrypt.org/directory --preferred-challenges=dns -d fellk.ru -d *.fellk.ru
```

Как и в предыдущем случае система попросит создать TXT запись.

Собственный центр сертификации

- Создаем корневой закрытый ключ -

```
openssl genpkey -algorithm RSA -out rootCA.key -aes-128-cbc
```

- Создаем корневой закрытый сертификат -

```
openssl req -x509 -new -key rootCA.key -sha256 -days 3650 -out rootCA.crt
```

- Создаем файл для хранения порядковых номеров с содержимым **00** -

```
nano rootCA.srl
```

- Устанавливаем корневой сертификат на все нужные ПК любым способом в **Доверенные корневые центры сертификации**
- Создаем конфигурационный файл под каждое ваше доменное имя -

```
nano test.cnf
```

Содержимое конфига меняйте по своей структуре

```
[ req ]
default_bits = 2048
distinguished_name  = req_distinguished_name
req_extensions     = req_ext
[ req_distinguished_name ]
countryName                 = Country Name (2 letter code)
```

```
countryName_default             = RU
stateOrProvinceName               = State or Province Name (full
name)
stateOrProvinceName_default     = Spb
localityName                    = Locality Name (eg, city)
localityName_default            = Spb
organizationName                = Organization Name (eg, company)
organizationName_default        = Test
commonName                        = Common Name (eg, YOUR name or
FQDN)
commonName_max                  = 64
commonName_default              = test.test.ru
[ req_ext ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName          = DNS:test.test.ru
```

- Создаем закрытый ключ для своего домена -

```
openssl genpkey -algorithm RSA -out test.key
```

- Создаем файл запроса -

```
openssl req -new -key test.key -config test.cnf -reqexts req_ext -out
test.csr
```

- Создаем сам сертификат -

```
openssl x509 -req -days 730 -CA rootCA.crt -CAkey rootCA.key -extfile
test.cnf -extensions req_ext -in test.csr -out test.crt
```

- Подключаем созданный сертификат к вашему домену через ваш веб сервер
- Проверяем работу домена и не забываем обновлять сертификаты по истечении срока годности

From:
https://wiki.fellk.ru/dokuwiki/ - **Игорь FellK**

Permanent link:
https://wiki.fellk.ru/dokuwiki/doku.php/certification_ssl

Last update: **2023/12/25 09:21**