Генерация запроса на сертификат (CSR) на Apache

Для работы необходимо использовать криптографический пакет с открытым исходным кодом – OpenSSL. Он доступен для большинства UNIX-like операционных систем и, как правило, включен в базовую версию операционной системы. Официальный сайт проекта расположен по адресу www.openssl.org.

Перед созданием CSR необходимо сгенерировать закрытый ключ длиной не менее 2048 bit. Закрытый ключ должен создаваться и храниться на сервере, для которого выпускается сертификат.

Создание закрытого ключа

1. В командной строке выполните команду:
   `openssl genrsa -des3 -out private.key 2048`
2. В ответ на запрос «Enter pass phrase for private.key» введите пароль для защиты закрытого ключа;
3. После запроса «Verifying - Enter pass phrase for private.key» - повторите ввод пароля;

Ваш закрытый ключ будет создан и сохранен в файле private.key. Просмотреть его можно выполнив команду:

```
less private.key
```

Внимание: при утрате пароля или компрометации закрытого ключа сертификат необходимо перевыпустить.

Создание CSR.

Внимание: при создании CSR все данные вводятся латинскими символами.

1. В командной строке выполните команду:
   `openssl req -new -key private.key -out domain-name.csr`
2. Введите пароль закрытого ключа в ответ на запрос «Enter pass phrase for private.key».
3. Следующие поля заполняются латинскими символами:
   - Country Name - двухсимвольный код страны, согласно ISO-3166. «RU» для России.
   - State or Province Name: название области или региона без сокращений;
   - Locality Name: название города или населенного пункта;

- Organization Name: название организации в латинском эквиваленте;
- Organizational Unit Name: название подразделения, для которого заказывается сертификат (необязательное поле);
- Common Name: полностью определенное (FQDN) доменное имя;
- Email Address: контактный e-mail адрес (необязательное поле);
- A challenge password: не заполняется;
- An optional company name: альтернативное имя компании (не заполняется).

```
[localuser@~/]$ openssl req -new -key private.key -out domain-name.csr
Enter pass phrase for private.key:
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) []:Moscow
Organization Name (eg, company) [Internet Widgits Pty Ltd]: MyCompanyName Ltd
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:mydomain.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[localuser@~/]$
```

Запрос на сертификат будет сохранен в файле domain-name.csr в виде закодированного текста. Проверьте корректность введенных данных, выполнив следующую команду:

```
openssl req -noout -text -in domain-name.csr
```

При создании заказа вам потребуется указать CSR. Для этого выполните просмотр файла запроса на сертификат и скопируйте его содержимое в форму заказа: