УЦ ГАЗИНФОРМ СЕРВИС

Инструкция.

Генерация запроса и установка SSL сертификата на веб-сервер Apache 2

Санкт-Петербург, 2019

1 Генерация CSR: Apache + Mod SSL + OpenSSL

Для формирования CSR-запроса для Вашего сайта используйте данную пошаговую инструкцию. В результате вы получите CSR-запрос, который потребуется для получения SSL-сертификата.

1. Установите OpenSSL, если данная программа отсутствует на вашем сервере.
2. Создайте RSA-ключ для веб-сервера Apache:

```
cd /apacheserverroot/conf/ssl.key

(ssl.key - директория по умолчанию для ключей).
```

Если вы используете другой путь, то перейдите в директорию веб-сервера Apache для закрытых ключей.

3. Введите следующую команду для генерации кодированного приватного ключа. Вам будет предложено ввести пароль для доступа к файлу. Данный пароль также необходимо будет вводить каждый раз при запуске веб-сервера.

Предупреждение: в случае утери пароля необходимо будет заказывать новый сертификат.

```
openssl genrsa -des3 -out domainname.key 2048
```

Вы можете создать приватный ключ и без использования кодирования, если Вы не желаете вводить пароль при каждом запуске веб-сервера:

```
openssl genrsa -out domainname.key 2048
```

Примечание: Мы рекомендуем использовать для наименования приватного ключа доменное имя, для которого заказывается сертификат, например ***domainname.key***.

4. Введите следующую команду для создания CSR с приватным ключом RSA (на выходе будет получен PEM-формат):

```
openssl req -new -key domainname.key -out domainname.csr
```

Примечание: Если на шаге 3 вы использовали ключ "-des3", то будет запрошен пароль для PEM-формата.

5. При создании CSR необходимо придерживаться следующих правил. Введите информацию, которая будет отображаться в сертификате. Нельзя использовать следующие символы: < > ~ ! @ # $ % ^ * / \ ( ) ? . , &

Описание полей запроса на сертификат приведено в таблице 1.

Таблица 1 – Описание полей запроса на сертификат

DN - поле	Пояснение	Пример
Common Name	Полное доменное имя для вашего веб-сервера. Оно должно в точности совпадать.	Если вы предполагаете использовать следующий URL: https://www.yourdomain.com, то "Common Name" должно быть www.yourdomain.com
Organization	Точное наименование организации в соответствии с Уставом организации на английском языке. Не используйте сокращенное наименование организации.	RapidSSL Ltd.
Organization Unit	Наименование отдела, подразделения (на английском языке).	Marketing
City or Locality	Город, где официально зарегистрирована организация (на английском языке).	Moscow
State or Province	Область, в которой официально зарегистрирована организация (на английском языке).	Moscow
Country	Страна, в виде двухсимвольного ISO-кода. Для России: RU.	RU

6. Не вводите дополнительные атрибуты.

Предупреждение: Оставьте пароль пустым (нажмите Enter).

Примечание: для проверки содержимого CSR используйте следующую команду:

```
openssl req -noout -text -in domainname.csr
```

7. Введите Ваш CSR в форме заказа.

Не забудьте сохранить копию приватного ключа в надежном месте! В случае утери данного файла, Вам необходимо будет заказать новый сертификат.

Приватный ключ должен начинаться -----BEGIN RSA PRIVATE KEY----- и заканчиваться -----END RSA PRIVATE KEY-----. Для просмотра содержимого приватного ключа используйте следующую команду:

```
openssl rsa -noout -text -in domainname.key
```

2 Установка SSL-сертификата: Apache + Mod SSL + OpenSSL

В письме с уведомлением о выпуске SSL-сертификата содержится zip-архив. В архиве содержатся 2 файла "domainname.cer" и "domainname.ca-bundle". Первый является сертификатом для вашего домена, а второй содержит корневой и промежуточные сертификаты.

Шаг 1. Скопируйте файлы domainname.cer и domainname.ca-bundle на сервер в ту же директорию, в которой содержится Private Key (приватный ключ).

В данном примере мы используем **'/etc/ssl/cer/'** . The private key (приватный ключ), используемый в примере, помечен как **'private.key'** , a public key будет называться **'yourDOMAINNAME.cer'** .

Примечание: Рекомендуем Вам создавать директорию, содержащую файл private key (приватный ключ), видимой только корневым каталогом.

Совет: рекомендуется выставить права доступа на чтение для директории, содержащей приватный ключ только для пользователя root.

Шаг 2. Установите на сервере корневой и промежуточный сертификаты.

2.1. Откройте в текстовом редакторе конфигурационный файл сервера Apache 2.x httpd.conf. Найдите раздел VirtualHost, относящийся к вашему SSL-сертификату. Убедитесь, что в нем содержатся три следующие строки. Если их нет - их необходимо добавить:

```
SSLCertificateChainFile /etc/ssl/cer/domainname.ca-bundle

SSLCertificateFile /etc/ssl/cer/domainname.cer

SSLCertificateKeyFile /etc/ssl/cer/private.key
```

Для Apache 1.x используйте вместо SSLCertificateChainFile директиву SSLCACertificateFile:

```
SSLCACertificateFile /etc/ssl/cer/domainname.ca-bundle
```

Примечание: в ряде конфигураций Virtual Host размещается в файле ssl.conf. Если в файле httpd.conf не содержится раздел Virtual Host, тогда поищите его в файле ssl.conf как было сказано выше.

2.2. Сохраните изменения и закройте текстовый редактор.

2.3. Запустите (или перезапустите) ваш веб-сервер Apache.

Дополнительная информация

Файл httpd.conf должен содержать несколько или все следующие строки (для IP-based сайта). Строки, относящиеся к настройкам SSL выделены жирным шрифтом. Строки, выделенные курсивом используются только для отладки (для выявления проблем при настройке SSL).

```
<VirtualHost 192.168.1.1:443>
DocumentRoot /var/www/html
ServerName 192.168.1.98
ServerAdmin someone@your.domain
ErrorLog /etc/httpd/logs/ssl_error_log
TransferLog /etc/httpd/logs/ssl_access_log
SSLEngine On
SSLCertificateFile /etc/ssl/cer/domainname.cer
SSLCertificateKeyFile /etc/ssl/cer/domainname.key
SSLCertificateChainFile /etc/ssl/cer/domainname.ca-bundle
SSLSessionCache dbm:/var/cache/httpd/ssl_cache
</VirtualHost>
```

Проверить настройки можно используя веб-браузер. Используйте https-протокол (например, https://ваш сервер/) для просмотра кодированных страниц. Иконка браузера с изображением навесного замка отображается в виде закрытого замка, если ваш сертификат установлен корректно и сервер правильно настроен.