

Установка SSL-сертификата для локального сайта (веб-сервер)

Данная инструкция описывает процесс обновления SSL-сертификата для сайта, работающего на локальном или корпоративном сервере. Инструкция составлена на основе реального кейса: замена сертификата для сайта в папке C:/RIT_WEB/html/ssl с использованием файлов, полученных из программы Sert.xdb (конвертация PFX в CRT и KEY).

Необходимые файлы

Перед началом работы у вас должны быть два файла:

`sert.crt` — публичный сертификат (выдается сервером).

`sert.key` — приватный ключ (секретная часть, хранится на сервере).

Если у вас есть только файл `.pfx` (например, `sert.pfx`), его необходимо сконвертировать. Для этого используется программа Sert.xdb или OpenSSL.

Преобразование сертификата pfx в crt

Преобразование с помощью openssl

Открываем командную строку переходим в папку с бинарником и выполняем последовательно команды

Получаем открытую часть сертификата

```
.\openssl.exe pkcs12 -in C:\TEMP\cert.pfx -clcerts -nokeys -out  
C:\TEMP\mms.crt
```

Получаем закрытую часть сертификата

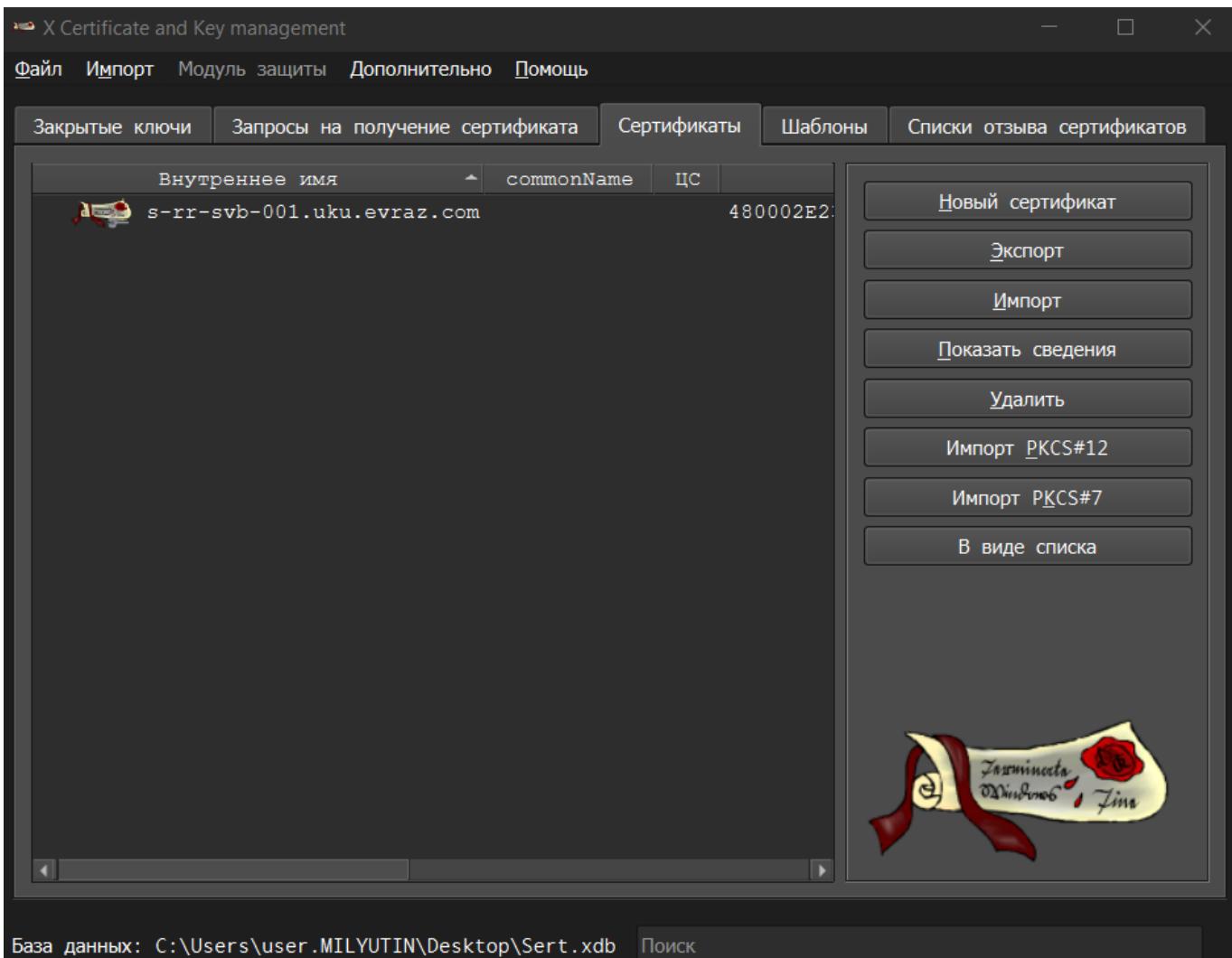
```
.\openssl.exe pkcs12 -in C:\TEMP\cert.pfx -nocerts -out C:\TEMP\mms.key
```

Сбрасываем пароль у закрытой части.

```
.\openssl.exe rsa -in C:\TEMP\mms.key -out C:\TEMP\test\mms.key
```

Преобразование с помощью Sert.xdb

Запустите программу Sert.xdb и укажите путь к вашему `.pfx`-файлу. В большинстве программ такого типа потребуется ввести пароль от PFX-контейнера (если он был установлен при создании).



База данных: C:\Users\user.MILYUTIN\Desktop\Sert.xdb Поиск

Выбор формата выходных файлов В настройках экспорта (или конвертации) необходимо указать, что на выходе вы хотите получить файлы в формате CRT/KEY.

Выполнение конвертации Запустите процесс. В результате программа создаст два файла:

`sert.crt` — публичный сертификат.

`sert.pem` — приватный ключ.

Переименование ключа (опционально)

Веб-сервер «ожидает» файл ключа с расширением '`.key`', а не `.pem`. В этом случае файл `sert.pem` можно безопасно переименовать в `sert.key`. Содержимое файла от этого не изменится, так как PEM — это текстовый формат, и расширение не влияет на его работу

Путь к сертификатам на сервере

В рассматриваемом примере сертификаты расположены по следующему пути:

`C:/RIT_WEB/html/ssl/`

В этой папке должны лежать два файла:

Процесс установки

Процесс обновления состоит из четырёх шагов.

Шаг 1. Остановка веб-сервера Для избежания ошибок во время замены файлов рекомендуется остановить службу веб-сервера.

Шаг 2. Замена файлов Скопируйте новые файлы crt и key в папку C:/RIT_WEB/html/ssl/.

Шаг 3. Запуск веб-сервера Запустите веб-сервер, чтобы он загрузил новые сертификаты.

Шаг 4. Очистка кэша браузера Если после замены сертификата в браузере отображается старый сертификат или возникает ошибка, необходимо очистить кэш браузера или зайти на сайт в режиме «Инкогнито»

Проверка результата

Чтобы убедиться, что новый сертификат установлен корректно:

Откройте ваш локальный сайт в браузере

Нажмите на значок замка слева от адресной строки.

Выберите пункт «Подключение безопасно», затем нажмите «Действительный сертификат»

From:
<https://wiki.rit-it.com/> - RIT Automation



Permanent link:
https://wiki.rit-it.com/doku.php/share:manuals:ssl_install

Last update: 2026/02/16 06:36