

**СИСТЕМА «PETROL PLUS»  
ПОДСИСТЕМА «PERSONAL WEB SUITE  
(PWS)»**

***Методика настройки SSL для Resin Profes-  
sional 4.x.xx  
Версия 1.00***

**ВЕДОМОСТЬ ИЗМЕНЕНИЙ**

| <b>ИЗМЕНЁННАЯ ЧАСТЬ</b><br><b>(раздел, страница)</b> | <b>ИЗМЕНЕНИЯ</b><br><b>тип (дополнения, удаления) и конкретное описание</b> |                     |
|------------------------------------------------------|-----------------------------------------------------------------------------|---------------------|
|                                                      | <b>Дата: 27.07.2011</b>                                                     | <b>Версия: 1.00</b> |
| Публикация документа                                 |                                                                             |                     |

|                       |                                       |              |     |
|-----------------------|---------------------------------------|--------------|-----|
| Система «Petrol Plus» | Подсистема «Personal Web Suite (PWS)» | Версия: 1.00 | 2/5 |
|-----------------------|---------------------------------------|--------------|-----|

Все исключительные авторские права принадлежат ООО «НКТ Софтвэр».  
Передача данного документа или прав на него третьим лицам, его распространение, равно и использование  
иным образом без письменного согласия правообладателя ООО «НКТ Софтвэр» запрещены

## СОДЕРЖАНИЕ

|          |                                                                                    |          |
|----------|------------------------------------------------------------------------------------|----------|
| <b>1</b> | <b>НАСТРОЙКА RESIN PROFESSIONAL ВЕРСИИ 4.X.XX ДЛЯ РАБОТЫ ПО ПРОТОКОЛУ SSL.....</b> | <b>4</b> |
| 1.1      | СОЗДАНИЕ КЛЮЧЕЙ.....                                                               | 4        |
| 1.2      | НАСТРОЙКА ЗАШИФРОВАННОГО СОЕДИНЕНИЯ.....                                           | 5        |

# 1 НАСТРОЙКА RESIN PROFESSIONAL ВЕРСИИ 4.X.XX ДЛЯ РАБОТЫ ПО ПРОТОКОЛУ SSL

## 1.1 Создание ключей

Для создания ключей выполните следующие действия:

1. Установите программу Microsoft Visual C++ 2005 — файл `vcredist_x86.exe`, следуя указаниям мастера установки.
2. Установите программу Open SSL Light (32-bit) — файл `Win32OpenSSL_Light-1_0_0d.exe`, следуя указаниям мастера установки.
3. Скопируйте файлы `ssleay32.dll` и `libeay32.dll` в каталог `$RESIN_HOME\win32`.
4. В каталоге `$RESIN_HOME\keys` создайте конфигурационный файл с именем `openssl.cnf`.

Например:

```
[ req ]
default_bits           = 1024
distinguished_name     = req_distinguished_name

[ req_distinguished_name ]
C                     = 2 letter Country Code
C_default             = RU
ST                   = State or Province
ST_default           = Moscow
L                   = City
L_default            = Moscow
O                   = Organization Name
O_default            = NCT
OU                  = Organizational Unit Name
OU_default           = Marketing
CN                  = your domain name
CN_default           = www.smartcard.ru
emailAddress         = an email address
emailAddress_default = info@smartcard.ru
```

5. Создайте секретный ключ.

Для этого в командной строке Windows перейдите в каталог `$RESIN_HOME\keys`, после чего выполните команду:

```
c:\OpenSSL-Win32\bin\openssl.exe genrsa -des3 -out gryffindor.key 1024.
```

6. Создайте сертификат.

Существует два способа получения сертификата: самостоятельное его создание, либо получение сертификата в специальной организации — центре сертификации (ЦС).

### Примечание.

При использовании сертификата, созданного самостоятельно, браузер не сможет распознать его подпись и будет выдавать предупреждение. За исключением этого предупреждения, такие сертификаты работают правильно.

Браузер не может подтвердить, что сервер — тот, за кого себя выдаёт, но данные, передаваемые между браузером и сервером, будут зашифрованы.

Для самостоятельного создания сертификата в командной строке Windows выполните команду:

```
c:\OpenSSL-Win32\bin\openssl.exe req -config ./openssl.cnf -new -key gryffindor.key -x509 -out gryffindor.crt
```

Вам будет предложено предоставить некоторую информацию о сервере (например, название вашей организации). Общее имя (CN) — это имя вашего домена (например, `www.smartcard.ru`).

Для получения сертификата из ЦС создайте запрос на подпись сертификата (CSR), для чего выполните команду:

```
C:\Program Files\GnuWin32\bin\openssl.exe" req -new -config ./openssl.cnf -key gryffindor.key -out gryffindor.csr
```

Вам будет предложено предоставить некоторую информацию о сервере (например, название вашей организации). Общее имя (CN) — это имя вашего домена (например, `www.smartcard.ru`).

Далее следует отправить csr-файл в ЦС (например, VeriSign или Thawte). В ответ вы получите файл `gryffindor.crt`.

**Примечание.**

При использовании сертификата, полученного из ЦС, предупреждение в браузерах не появляется.

## 1.2 Настройка зашифрованного соединения

Для настройки зашифрованного соединения выполните следующие действия:

1. Поместите сертификат в каталог `$RESIN_HOME\keys`.
2. Откройте файл конфигурации `resin.xml` и в узле `<!-- SSL port configuration: -->` добавьте (измените) раздел:

```
<http address="*" port="8443">
  <openssl>
    <certificate-file>keys/gryffindor.crt</certificate-file>
    <certificate-key-file>keys/gryffindor.key</certificate-key-file>
    <password>пароль, указанный при создании ключа</password>
  </openssl>
</http>
```

3. Зашифрованное соединение будет организовано через порт 8443. Например: `https://localhost:8443/pws`.