**Создание самоподписанных SSL сертификатов**

Чт, 2009/04/09 - 12:30 | [*Константин Бояндин*](http://boyandin.info/users/3)

Иногда возникает необходимость создания самоподписанного SSL-сертификата (для обеспечения надёжного доступа к сервисам интранета и т.п.). Делается это таким образом:

В дальнейшем 'server' — условная строка, используйте любую, рекомендуется делать её мнемонической, чтобы она сообщала о том, где и для чего будет использоваться сертификат — например, 'example.com-smtp').

1. Создаём ключ (потребуется ввод пароля, введите любой):

openssl genrsa -des3 -out server-tmp.key

2. Если не хочется вводить пароль при запуске сервиса, пароль нужно убрать (примите меры после этого, чтобы доступ к ключу был только у суперпользователя):

openssl rsa -in server-tmp.key -out server.key

3. Создаём файл запроса о подписи (certificate signing request, CSR):

openssl req -new -key server.key -out server.csr

Программа запросит ряд параметров для сертификата, отвечайте примерно таким образом:

Country Name (2 letter code) [GB]:RU  
State or Province Name (full name) [Berkshire]:Tmutarakan region  
Locality Name (eg, city) [Newbury]:Tmutarakan  
Organization Name (eg, company) [My Company Ltd]:FooBar Tmutarakanian  
Organizational Unit Name (eg, section) []:Bystronet  
Common Name (eg, your name or your server's hostname) []:example.com  
Email Address []:[admin@example.com](mailto:admin%40example.com)

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

В случае 'Common Name'(указывал localhost и запускал в фидлере https://localhost:443 и на <https://localhost:55555> а в браузере <https://localhost:55555> смотри код ssl\_server\_3.py) необходимо указать доменное имя сервера. Внимание: при настройке сервиса доменное имя должно быть в точности таким же, иначе будет как минимум выдаваться предупреждение о том, что сертификат выдан на другой сервер.

Дополнительные ('extra') параметры можно не вводить (просто нажмите Enter).

4. На этом этапе можно получить сертификат от доверенного источника (платный). Если достаточно самоподписанного (достаточно для нужд интранета), то генерируем сертификат сами:

openssl x509 -req -days 3650 -in server.csr -signkey server.key -out server.crt

Параметр после '-days' - время годности сертификата в днях, считая от текущего момента. В примере выше мы создаём сертификат, годный в течение примерно 10 лет.

Всё готово. Файл server.key - ключ, файл server.crt - собственно сертификат.

openssl x509 –noout –text –in server.crt

openssl req –new –x509 –days 30 –nodes –out timecert.pem –keyout timecert.pem

http://pro-ldap.ru/tr/zytrax/tech/ssl.html