|  |
| --- |
| **Самостоятельная генерация сертификата** |
| 1. Скачиваем инсталлятор *openssl* с сайта [openssl.org](http://slproweb.com/products/Win32OpenSSL.html)(для Windows). Устанавливаем openssl, если при установке openssl на Windows он потребует Microsoft Redistributables Package, то предварительно, скачиваем и устанавливаем соответствующий пакет.   Например, на данный момент доступна версия openssl v1.0.1c и соответствующий ему Visual C++ 2008 Redistributables (x86/x64) по следующим ссылкам: [openssl](http://slproweb.com/download/Win32OpenSSL-1_0_1c.exe) и [Redistributables](http://www.microsoft.com/downloads/details.aspx?familyid=9B2DA534-3E03-4391-8A4D-074B9F2BC1BF)   1. После установки openssl запускаем командную строку cmd и выполняем следующие команды, предварительно перейдя в каталог **bin** установленного openssl (по умолчанию **c:\OpenSSL-Win32\bin**):    * Указываем путь к конфигурации openssl: set OPENSSL\_CONF=C:\OpenSSL-Win32\bin\openssl.cfg ;    * Генерируем приватный ключ (в процессе генерации приватного ключа необходимо задать пароль): openssl genrsa -des3 -out c:\certificate\private.key 2048 ;    * Генерируем запрос на сертификат: openssl req -new -key c:\certificate\private.key -out c:\certificate\csr.csr В процессе генерации запроса будут запрошены параметры для сертификата, которые необходимо вводить в латинской раскладке. Достаточными являются: - **Country Name (2 letter code) [AU]** - страна регистрации организации, для которой готовим сертификат (для Росcии - RU) - **State or Province Name (full name) [Some-State]** - область, регион регистрации организации (Москва - Moscow) - **Locality Name (eg, city) []** - город регистрации организации (Москва - Moscow) - **Organization Name (eg, company) [Internet Widgits Pty Ltd]** - наименование организации - **Common Name (e.g. server FQDN or YOUR name) []** - доменное имя, для которого генерируется сертификат (в данном случае может не совпадать с действительным доменным именем) (localhost, companyname.com)    * Генерируем сам сертификат сроком на 365 дней (можно больше или меньше): openssl x509 -req -days 365 -in c:\certificate\csr.csr -signkey c:\certificate\private.key -out c:\certificate\certificate.pem   В результате в каталоге c:\certificate будет создан приватный ключ (private.key) и сертификат (certificate.pem), который, в случае самостоятельно генерируемого сертификата, будет являться и сертификатом центра сертификации.   1. Для того чтобы браузер не выдавал предупреждения по поводу недостоверности сертификата, можно установить сертификат (certificate.pem) в систему (предварительно поменяв его расширение на.crt) или в браузер, если он использует собственное хранилище сертификатов. |