

Генерация запроса на сертификат (CSR) на хостинге R01

Для создания запроса на сертификат (CSR) необходимо использовать криптографический пакет с открытым исходным кодом OpenSSL. Он доступен для большинства UNIX-подобных операционных систем и доступен на нашем хостинге.

1. Подключение к хостингу по SSH

Все необходимые операции по созданию CSR выполняются на хостинге при подключении по SSH. Вам потребуется получить параметры для подключения в панели управления хостингом и [настроить подключение](#) с помощью SSH-клиента, например PuTTY.

2. Создание закрытого (приватного) ключа

Перед созданием CSR необходимо сгенерировать закрытый ключ длиной не менее 2048 бит. Закрытый ключ должен создаваться и храниться на сервере, для которого выпускается сертификат.

После подключения к хостингу по SSH выполните в командной строке следующие команды.

1. Перейдите в каталог для временных файлов `/home/идентификатор/tmp`. В этом каталоге будут сохранены созданные вами файлы

```
cd ~/tmp
```

2. Создайте закрытый ключ командой:

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

3. В ответ на запрос **Enter pass phrase for private.key** введите пароль для защиты закрытого ключа.

4. После запроса **Verifying — Enter pass phrase for private.key** — повторите ввод пароля.

```
[localuser@~/]$ openssl genrsa -des3 -out private.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
Enter pass phrase for private.key:
Verifying - Enter pass phrase for private.key:
```

Ваш закрытый ключ будет создан и сохранен в файле `private.key`. Просмотреть его можно, выполнив команду:

```
less private.key
```

Для выхода нажмите **Q**.

При утрате пароля или компрометации закрытого ключа сертификат необходимо перевыпустить. Обязательно сохраните копию закрытого ключа на своем компьютере.

3. Создание запроса на сертификат (CSR)

При создании CSR все данные вводятся латинскими символами.

1. В командной строке выполните команду:

```
openssl req -new -key private.key -out domain-name.csr
```

2. Введите пароль закрытого ключа в ответ на запрос **Enter pass phrase for private.key**.

3. Следующие поля заполняются латинскими символами:

- **Country Name** — двухсимвольный код страны согласно ISO-3166. **«RU»** для России.
- **State or Province Name**: название области или региона без сокращений;
- **Locality Name**: название города или населенного пункта;
- **Organization Name**: название организации в латинском эквиваленте;
- **Organizational Unit Name**: название подразделения, для которого заказывается сертификат (необязательное поле);
- **Common Name**: полностью определенное (FQDN) доменное имя;
- **Email Address**: контактный e-mail адрес (необязательное поле);
- **A challenge password**: не заполняется;
- **An optional company name**: альтернативное имя компании (не заполняется).

```
[localuser@~/]$ openssl req -new -key private.key -out domain-name.csr
Enter pass phrase for private.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Moscow
Locality Name (eg, city) []:Moscow
Organization Name (eg, company) [Internet Widgits Pty Ltd]: MyCompanyName Ltd
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:mydomain.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[localuser@~/]$ █
```

Запрос на сертификат будет сохранен в файле domain-name.csr в виде закодированного текста. Проверьте корректность введенных данных, выполнив следующую команду:

```
openssl req -noout -text -in domain-name.csr
```

При создании заказа на SSL-сертификат в личном кабинете на сайте www.r01.ru вам потребуется указать CSR. Для этого выполните просмотр полученного CSR-файла командой **less** и скопируйте его содержимое в форму заказа.

```
[localuser@~/]$ less domain-name.csr
-----BEGIN CERTIFICATE REQUEST-----
MIICqDCCAZAQAwYzELMAkGA1UEBhMCU1UxDzANBgNVBAgTBk1vc2NvdzEPMAOG
A1UEBxMGTW9zY293MRswGQYDVQQKEsIgTX1Db21wYW55TmFtZSBMdGQxFTATBgNV
BAMTDG15ZG9tYWluLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ALJWQaMH3Vo9FPD34bibjRH9pVUx8etkBBgg9t4kqR5u+nMyfq+AF3bD0s1VrimS
v8zBikGVarDIjkE+GTlsgSokCR9uTP1BC6IOULqXc/rgLqCQYoS6h0/rA9P5/SwA
RjSc8r4u8tZ1W3rejBYQaA6NMy3YCdTSOKOPNXFUaBQx+KE/86U1i5ksN16Kuh2R
svQL3936m0dkuKdZYSrTHkGBAkRXQp9QEt+WJ52Ogg61SdoECMc5BqKuPbrigWUX
LO56zyhyS4mBK31UaFPUS+SFex1N+2BcRtMt5ZjOXXYWsthNhV1FLBB6wH8krLFs
L4DhJmnce2qC7kVayKrn7qUCAwEAaAAMAOGCSqGSIb3DQEBBQUAA4IBAQCIOfl9
XeIM8GPYZtyd1JBW3h/PVH1+JBx6OR4z5YHYpDf6yIEA4ZYCwlngD35ueRLrmwxN
v9MB3+t4UCDtMuJWW2tG5VKKenLObAvmP/szOD81iYTAKtA5C2MqcGkiKWywlu4S
9ZtgEs4e+LzgsjPe8ytLyJDukOt6n7ijEGCWDQfqy16XGSFNBJEntaO6Dr+Q18qN
Dk3p5mAC2YWWdhLmRtgteK3if5TglsnQMmf1OGOYCpGH3/OOs1ru6ndiQg/eaOKm
EdI8Nhd/zeNOFVpnKwCRaxIbcwgZ8EYnCV17h5PqWduood5aqzaYamRDf1RGYprH
HLBvMFX4I4OUYXOO
-----END CERTIFICATE REQUEST-----
domain-name.csr (END)
```