



ВЕБ-РАЗРАБОТКА | ДАТА-ЦЕНТР
ТЕХНИЧЕСКАЯ ПОДДЕРЖКА | ФАРМ-СТУДИЯ
itsoft.ru

CSR - что это и как его сгенерировать

Что такое CSR?

Certificate Signing Request (CSR) - это данные, представляющие собой запрос на выдачу цифрового сертификата для защиты веб-сайта или приложения. CSR создается и отправляется центру сертификации, чтобы получить подписанный сертификат, который подтверждает подлинность и безопасность сервера.

Как выглядит CSR?

Сам CSR создается в формате base64-encoded PEM.

Файл CSR можно открыть с помощью простого текстового редактора.

```
sirkliy@Vladimirs-MacBook-Air-2 ~ % cat itsoft.csr | head -n 3 && ec
-----BEGIN CERTIFICATE REQUEST-----
MIICijCCAIXICAQAwRTELMAkGA1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3RhdGUx
ITAfBgNVBAoMGE1udGVybmV0IFdpZGdpdHMgUHR5IEEx0ZDCCASIwDQYJKoZIhvcN
...
l+sS49kfWXUie+FH4CrW1DVdMkt1bB13REcmFKSjoZrTmzC7ZgmsYSKWRcA+6YZE
I3RgaMCvJAu6rPV48FTMc7XHdoxiXBWajiC2xTW4
-----END CERTIFICATE REQUEST-----
```

Как создать запрос на подписание сертификата (CSR)?

Существует два способа создания запроса:

1. Используя командную строку MacOS / Linux

В терминале выполняем команду:

```
openssl req -nodes -newkey rsa:2048 -sha256 -keyout itsoft.key
-out itsoft.csr
```

```
mc [sirkliiv@Vladimirs-MacBook-Pro.local]:~/Downloads/cert
sirkliiv@Vladimirs-MacBook-Pro cert % openssl req -nodes -newkey rsa:2048 -sha256 -keyout itsoft.key -out itsoft.csr 1
-----
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 2
State or Province Name (full name) [Some-State]:Moscow 3
Locality Name (eg, city) []:Moscow 4
Organization Name (eg, company) [Internet Widgits Pty Ltd]:itsoft 5
Organizational Unit Name (eg, section) []:support 6
Common Name (e.g. server FQDN or YOUR name) []:*.itsoft.ru 7
Email Address []:support@itsoft.ru 8

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []: 9
An optional company name []:
sirkliiv@Vladimirs-MacBook-Pro cert % ls
itsoft.csr      itsoft.key
sirkliiv@Vladimirs-MacBook-Pro cert %
```

В данной команде

itsoft.key и itsoft.csr имена генерируемых ключа и csr

rsa:2048 - тип шифрования (rsa) и желаемая длина ключа (2048)

Далее вводим запрашиваемую информацию, отвечая на вопросы:

- Country Name (2 letter code) [AU]: обычно RU (Россия), либо другая, в которой находится ваша организация. Коды стран можно найти в [справочнике](#)
- State or Province Name (full name) [Some-State]: регион или штат, в котором находится ваша организация. Не следует использовать сокращения при заполнении данного поля.
- Locality Name (eg, city) []: город, в котором находится организация. Не следует сокращать это название.
- Organization Name (eg, company) [Internet Widgits Pty Ltd]: - юридическое название вашей организации. Не сокращайте наименование организации и указывайте суффиксы, такие как Inc., Corp. или LLC. Для физического лица нужно указать Private Person.
- Organizational Unit Name (eg, section) []: - подразделение вашей организации, в котором будет находиться сертификат.
- Common Name (e.g. server FQDN or YOUR name) []: полное доменное имя (Fully Qualified Domain Name или FQDN) вашего сервера.
- Email Address []: адрес электронной почты, используемый для связи с вашей организацией.

Следующие поля не используем, поэтому заполнять не нужно (просто нажать 2 раза enter):

A challenge password []:

An optional company name []:

После будут созданы 2 файла, один из которых содержит приватный ключ (.key), второй - запрос (.csr).
Файл с ключом остаётся у вас, а файл с CSR необходимо передать менеджеру itsoft для выпуска сертификата.

Обращаем внимание, что при утере ключа процедуру генерации ключа и запроса, а затем и выпуска сертификата нужно будет произвести заново.

Важно: при выпуске сертификата OV и EV данные для генерации CSR должны совпадать с данными в каталогах организаций, используемых УЦ для проверки ([Infobel](#) или [Kompass](#)).

пример записи в Infobel:

<https://www.infobel.com/en/russia/itsoftware/moskva/RU103166120/businessdetails.aspx>

Для ускорения процедуры создания CSR или, например, если различных сертификатов очень много, чтобы не запоминать информацию по каждому домену можно создать файлы конфигурации:

req_itsoft.txt:

```
[req]
default_bits = 2048
prompt = no
default_md = sha256
req_extensions = req_ext
distinguished_name = dn

[ dn ]
C=RU
ST=Moscow
L=Moscow
O=itsoft
OU=support
emailAddress=support@itsoft.ru
CN=*.itsoft.ru

[ req_ext ]
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = itsoft.ru
DNS.2 = www.itsoft.ru
DNS.3 = mail.itsoft.ru
```

Генерируем csr используя файл конфигурации:

```
openssl req -new -sha256 -nodes -out itsoft.csr -newkey rsa:2048
-keyout itsoft.key -config req_itsoft.txt
```

Важно! В условиях санкций против РФ, для доменов ru, su, moscow, рф сертификаты выпускает только GlobalSign (AlphaSSL, GlobalSign)

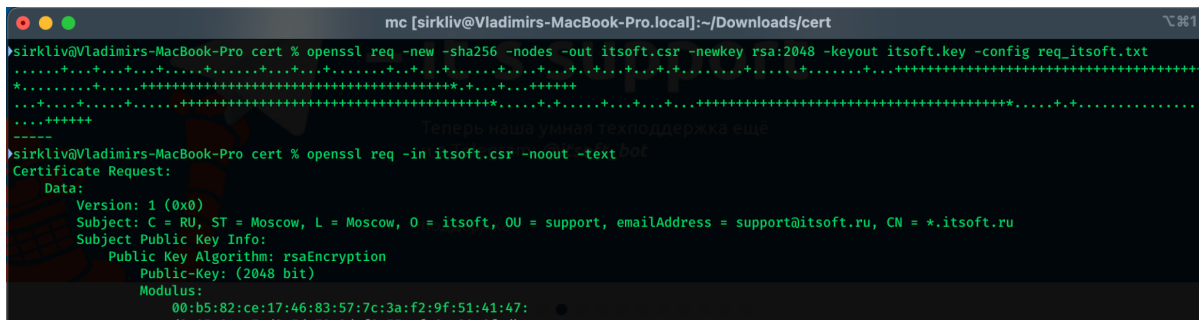
У данного УЦ при выпуске AlphaSSL DV не поддерживается SAN (Subject Alternative Name), поэтому необходимо из файла конфигурации убрать строку

```
req_extensions = req_ext
```

`u секции [req_ext] u [alt_names]`

Проконтролировать правильность сгенерированного CSR можно командой:

```
openssl req -in itsoft.csr -noout -text
```



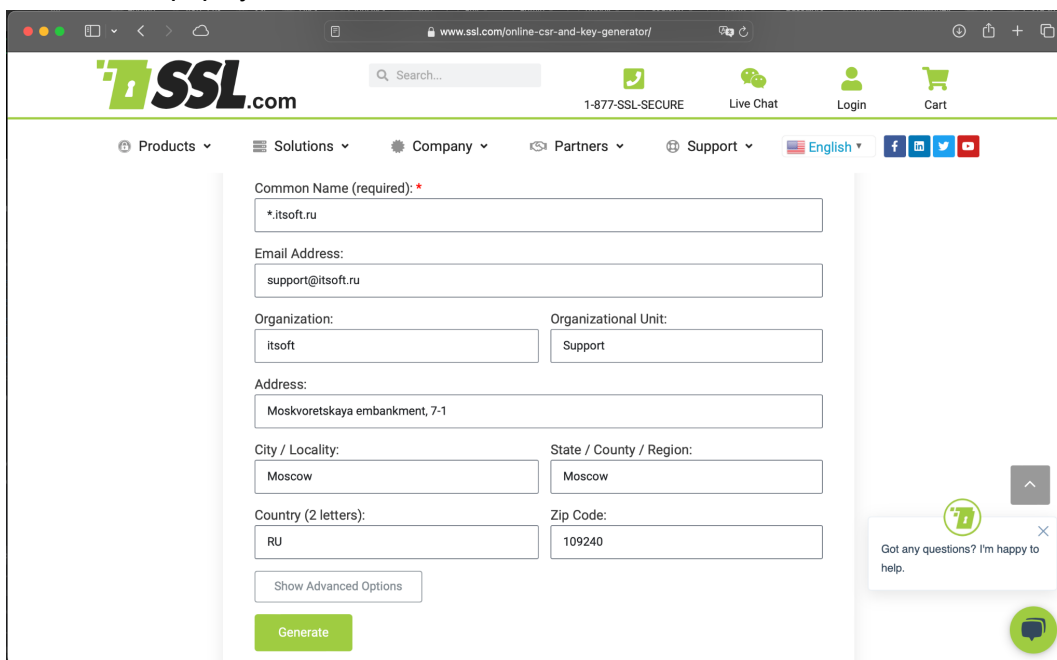
```
mc [sirkliv@Vladimirs-MacBook-Pro.local]:~/Downloads/cert
>sirkliv@Vladimirs-MacBook-Pro cert % openssl req -new -sha256 -nodes -out itsoft.csr -newkey rsa:2048 -keyout itsoft.key -config req_itsoft.txt
.....
*.....
.....
-----
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = RU, ST = Moscow, L = Moscow, O = itsoft, OU = support, emailAddress = support@itsoft.ru, CN = *.itsoft.ru
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:b5:82:ce:17:46:83:57:7c:3a:f2:9f:51:41:47:
      d2:05:04:e2:d2:5d:72:7d:09:55:ef:6c:30:6f:d8:
```

2. При помощи различных веб-сервисов (данный способ может быть небезопасен, так как вы доверяете создание закрытого ключа сторонним сервисам и передаете его через интернет).

Поля для заполнения примерно аналогичны из п1, могут быть и дополнительные поля, например выбор шифрования или почтовый индекс.

Пример такого сервиса <https://www.ssl.com/online-csr-and-key-generator/>

Заполняем форму на сайте, нажимаем Generate



После успешной генерации запроса и ключа их необходимо сохранить

www.ssl.com/online-csr-and-key-generator/

SSL.com

Search

Login Cart

English

Products

Solutions

Common

*.itsoft

Email Address

support

Organization

itssoft

Address

Mosk

City / Loc

Mosco

Country

RU

Show

Generated CSR and Private Key

Certificate Signing Request (CSR):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDKTCANMCAQAwgblUxgbIwEgYDVQDDAsqLm10c29mdC5ydTAeBgkqhkiG9w0B
CQETEXN1cHBvcnRAAXRzb2Z0LnJ1MA4GA1UECzMHU3VvcG9ydDANBgNVBAoTBM10
c29mdDA1BgNVBAkTHk1vc2t2b3JldHNhYXN1c29mdC5ydTAeBgkqhkiG9w0B
BACjBk1vc29mdzANBgNVBAgTBk1vc29mdzANBgNVBBETBjEwOTI0MDAJBgNVBAYT
ALJVMiIiBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1RxfZR/4TTAM1Iw
D3ph5ILMj/IHNeseZ0awFxb9/bByPvKY8cEF2f4Vj+XHHSshLX8qAz4jDRGsiH9L
AdQXleMmpaw09ULi+yRBjM8ddXEitnCWz4/c3b9H0RKRmDyBk3e9PP+A7FXWz5z
vXq5fk0bg0Zeh8P9R5j17XB72xB0WxNjNbasfBZuXkV660Uv1hx6GZY5ouz5fv
zJNEz0blFF5aVj6pBAWojqrpbfRWvgRkyx59GuVnvoKwm9LWqRCKA0RmC+2xkE
+QA8wFyw82KUMt9m/479t14TM786PxdqZ6haxQ56BLStLvjeEpbP0MVECV03JA
-----
```

Private Key:

```
-----BEGIN PRIVATE KEY-----
MIIEVAIBADANBgkqhkiG9w0BAQEFAASCbKYYggS1AgEAAoIBAQCvHF9LH/HMMWY
0hYpEmHkiLWm8gc16x5K5rAXH39vzI+8pJxwQZJ/hwP5ccfmyGVfyODPPJmNEayI
f2UB1AxeV4yaLrAP15wL7JEEmbx11c5K2cLDPj9zd0fFRGEX3IGtd708/4DsVdb
NL09epJ+05uBChmaHq/1HkMLtcFPbEHRbE2M1tqx8Fm5eRrrRBS/MHFzZnJKL7P
1+/Mk07NBuUUXlpUnqEBa10quL9Fa+BTGLHn28ShWe+grCb0vJapEioDRGVL7b
G0T5ADzAXLDzYp0y2f2b/v22Lhmzvo/F2pnaGFrFBL0Evm2W+N4ISLs/QxUQK8
4k8cSmubAgMBAAECggEACxgmKuPYOYSTk6zHR7G342jpxMEYJW6rbQ8/tjGRm4
ehyo80CWb1fuLSqM6T7deCnyL+PwLHvcz99/UcaJUEYr05Fq1qRusRPVUfjthrC
xGqFet66hrngMePFE+ooUdhSK69Eh1IQmd+VJLiwnPDKlqjF0M60YnX7XsG6jB
C+Qf0BTcGN0P4eH65sFABDgZuETA4m5/SYk0pvZgbcSj9YJkkqyto7VYseweeRAM
-----
```

Copy CSR Download Private Key

Got any questions? I'm happy to help.