госуслуги

> Для создания запроса на выпуск tls-сертификата предварительно установите приложение openssl и откройте командную строку

Создание запроса на выпуск tls-сертификата с новым ключом

Linux

В командной строке введите:
«openssl req -out test.csr -new \
-subj "/C=RU/ST=Moscow/L=Moscow/O=The Ministry of Digital Development and Communications/CN=*.mydomain.ru" \
-addext "keyUsage = digitalSignature, keyEncipherment" \
-addext "subjectAltName = DNS:mydomain.ru, DNS:www.mydomain.ru, DNS:*.mydomain.ru \
-addext "extendedKeyUsage = serverAuth" \
-newkey rsa:2048 -nodes -keyout newKey.key»,

где:
- test.csr – наименование запроса, например, mydomain.csr
- C – двухбуквенный код страны, для России – RU
- ST – район, область, например, Moscow
- L – полное название города, например, Moscow
- официальное название организации, например, The Ministry of Digital Development and Communications
- CN – имя домена, на который оформляется TLS-сертификат. Например, *.mydomain.ru. Для доменных имён на русском языке следует указывать конвертированное с помощью метода punycode значение, например, xn--j1ail.xn--p1ai

При заполнении параметров ST/L/O/OU кириллицей в запросе **укажите** ключ «-utf8». Например: «openssl req -out test.csr -new -subj "/C=RU/ST=Москва/L=Москва/O=Тестовая Организация/OU=Тестовый департамент/CN=*.mydomain.ru" -addext "keyUsage = digitalSignature, keyEncipherment" -addext "subjectAltName = DNS:mydomain.ru, DNS:www.mydomain.ru, DNS:*.mydomain.ru" -addext "extendedKeyUsage = serverAuth" **-utf8** -newkey rsa:2048 -nodes -keyout newKey.key»

где:
- keyUsage – расширение, определяющее назначение ключа. В запросе **обязательно** должны присутствовать digitalSignature и keyEncipherment, иные – при необходимости
- subjectAltName – расширение, определяющее альтернативное имя субъекта (DNS-имя). **Обязательно** укажите хотя бы одно значение. Пример записи: subjectAltName = DNS:mydomain.ru.
- extendedKeyUsage – расширение, определяющее расширенное назначение ключа. В запросе **обязательно** должно присутствовать serverAuth, иные – при необходимост
- newKey.key – наименование нового ключа. Например, mydomain.key

```
ubuntu@ubuntu:~$ openssl req -out test.csr -new \
> -subj "/C=RU/ST=Moscow/L=Moscow/O=The Ministry of Digital Development and Communications/CN=*.mydomain.ru" \
> -addext "keyUsage = digitalSignature, keyEncipherment" \
> -addext "subjectAltName = DNS:mydomain.ru, DNS:www.mydomain.ru, DNS:*.mydomain.ru, IP:192.168.7.1, URI:http://my.example.ru/" \
> -addext "extendedKeyUsage = serverAuth" \
> -newkey rsa:2048 -nodes -keyout newKey.key
Generating a RSA private key
....+++++
.....................................................+++++
writing new private key to 'newKey.key'
-----
ubuntu@ubuntu:~$
```

Проверить созданный запрос можно с помощью следующей команды:
«openssl req -in test.csr -noout -text»
«openssl req -in test.csr -noout -text -nameopt utf8» — при заполнении параметров ST/L/O/OU кириллицей

где:

- test.csr – наименование созданного запроса

```
ubuntu@ubuntu:~$ openssl req -in test2.csr -noout -text
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = RU, ST = Moscow, L = Moscow, O = The Ministry of Digital Development and Communications, CN = *.mydomain.ru
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b3:c4:73:be:f2:a2:f6:7e:5b:6c:aa:80:31:60:
                    1b:8a:98:7d:81:3f:99:f1:c2:6b:21:bd:8f:c7:e8:
                    a7:40:3d:61:e9:3d:34:66:ab:1d:ef:d5:7b:94:aa:
                    79:d8:21:ec:7a:ab:96:da:95:08:39:1e:9b:fd:b3:
                    78:96:58:53:85:2b:3b:b1:4a:7d:46:35:75:ac:09:
                    84:20:5e:59:ad:b7:bf:67:b1:da:29:1e:b5:21:e4:
                    9e:f0:e7:61:34:ea:3e:e2:6b:20:a7:17:83:43:43:
                    1b:f4:f6:9e:34:28:cd:5a:c0:2c:1c:ce:a9:b1:98:
                    95:f9:da:9d:37:26:86:2a:09:2d:f6:af:97:a7:0b:
                    88:07:08:9b:39:4d:77:9a:bf:54:f9:a8:d1:5e:91:
                    fe:cc:05:d8:3b:3c:60:3d:b1:77:d6:88:eb:50:6c:
                    92:1f:5e:a9:b3:92:32:51:98:eb:4a:b1:e9:07:db:
                    5e:00:c0:af:07:cb:87:a3:de:81:71:5d:d5:41:90:
                    9d:03:8b:39:c5:6d:55:d3:f1:18:f0:e9:8e:33:2e:
                    b0:5c:87:13:70:6b:99:88:c5:81:f2:f6:09:72:14:
                    3b:70:b8:ff:5d:f2:3f:79:30:df:88:3d:24:3b:03:
                    22:ff:fb:63:ef:00:9f:5f:26:5d:5f:6a:f4:35:51:
                    af:11
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
            X509v3 Subject Alternative Name:
                DNS:mydomain.ru, DNS:www.mydomain.ru, DNS:*.mydomain.ru, IP Address:192.168.7.1, URI:http://my.example.ru/
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
    Signature Algorithm: sha256WithRSAEncryption
         59:00:0c:d2:db:84:a9:6c:0a:b2:94:b1:02:41:88:12:e2:c1:
         fc:d5:a7:72:80:bb:ed:04:85:6a:3c:86:01:94:c3:30:b6:23:
         d1:aa:b6:b9:35:31:51:a9:93:ce:32:80:d6:b3:1c:68:ef:63:
         dc:7c:53:e4:79:7f:e4:18:bc:2f:2e:a3:c6:ae:60:a2:7b:41:
         03:d6:9a:18:9b:04:c5:ed:8f:60:9f:2f:b3:cf:1e:da:1a:83:
         9f:96:2a:22:14:bc:50:18:44:0d:e8:0b:89:0b:9b:46:48:c1:
         2a:22:a6:c8:f8:62:ed:72:5b:08:08:c0:fa:3d:82:cc:65:6b:
         f5:02:71:65:32:06:67:3f:bd:ff:65:33:49:6c:e9:35:3c:47:
```

Windows

В командной строке введите:
«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -out test3.csr -new -subj "/C=RU/ST=Moscow/L=Moscow/O=The Ministry of Digital Development and Communications/CN=*.mydomain.ru" -addext "keyUsage = digitalSignature, keyEncipherment" -addext "subjectAltName = DNS:mydomain.ru, DNS:www.mydomain.ru, DNS:*.mydomain.ru" -addext "extendedKeyUsage = serverAuth" -newkey rsa:2048 -nodes -keyout newKey.key»,

где:

- test3.csr – наименование запроса, например, mydomain.csr
- C – двухбуквенный код страны, для России – RU
- ST – район, область, например, Moscow
- L – полное название города, например, Moscow
- официальное название организации, например, The Ministry of Digital Development and Communications
- CN – имя домена, на который оформляется TLS-сертификат. Например *.mydomain.ru. Для доменных имён на русском языке следует указывать конвертированное с помощью метода punycode значение. Например, xn--j1ail.xn--p1ai

При заполнении параметров ST/L/O/OU кириллицей **необходимо** создать в «C:\Program Files\OpenSSL-Win64\bin\cnf» конфигурационный файл mydomain.cnf, **заполнить его так:**

> «[req]
> prompt = no
> distinguished_name = dn
> [dn]
> C = RU
> ST = Москва
> L = Москва
> O = Тестовая Организация
> OU = Тестовый департамент
> CN = *.mydomain.ru»

и изменить команду перед выполнением:
«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -out test3.csr -new -addext "keyUsage = digitalSignature, keyEncipherment" -addext "subjectAltName = DNS:-mydomain.ru, DNS:www.mydomain.ru, DNS:*.mydomain.ru" -addext "extendedKeyUsage = serverAuth" **-utf8 -config "C:\Program Files\OpenSSL-Win64\bin\cnf\mydomain.cnf"** -newkey rsa:2048 -nodes -keyout newKey.key»

где:

- keyUsage – расширение, определяющее назначение ключа. В запросе **обязательно** должны присутствовать digitalSignature и keyEncipherment, иные – при необходимости
- subjectAltName – расширение, определяющее альтернативное имя субъекта (DNS-имя). **Обязательно** должно быть указано хотя бы одно значение. Пример записи: subjectAltName = DNS:mydomain.ru
- extendedKeyUsage – расширение, определяющее расширенное назначение ключа; в запросе **обязательно** должно присутствовать serverAuth, иные – при необходимости
- newKey.key – наименование нового ключа, например, mydomain.key

```
C:\Users\Natalia>"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -out test3.csr -new -subj "/C=RU/ST=Moscow/L=Mosco
w/O=The Ministry of Digital Development and Communications/CN=*.mydomain.ru" -addext "keyUsage = digitalSignature, keyEn
cipherment" -addext "subjectAltName = DNS:mydomain.ru, DNS:www.mydomain.ru, DNS:*.mydomain.ru, IP:192.168.7.1, URI:http:
//my.example.ru/" -addext "extendedKeyUsage = serverAuth" -newkey rsa:2048 -nodes -keyout newKey.key
..+....+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.........+..+...................+.....+.+..
....+..+.........+.....+.+..........+....+.........+..+...+.........+..+.+.....++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++*..+....+...........+........+.+......+........+.......+.....+...+...+....+.....+......+...+
.........+......+...........+...+.........+...+....++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.......+..+.+...........+.........+...+..+...+...+....+.........+.....+...........+.......+......+......+...+...+.....
+...+....+..+....+...........+.++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.........+.............
.........+..+...+....+.....+......+....+...+........++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*..
......+...+..++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
-----
```

Проверить созданный запрос можно с помощью следующей команды:
«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in "\path\to\test3.csr" -noout -text»,
«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in "\path\to\test3.csr" -noout -text -nameopt utf8» - при заполнении параметров ST/L/O/OU кириллицей,

где:

- test3.csr – наименование созданного запроса

```
C:\Users\Natalia>"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in "C:\Users\Natalia\test4.csr" -noout -text
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = RU, ST = Moscow, L = Moscow, O = The Ministry of Digital Development and Communications, CN = *.myd
omain.ru
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c1:81:2c:69:80:84:e5:16:fc:b7:06:17:14:42:
                    37:66:53:0b:76:1d:26:3d:21:02:4e:2e:c7:d9:b2:
                    6c:2b:4a:0a:f3:a1:f1:aa:bc:44:91:a6:c5:f8:be:
                    17:73:17:f1:7d:95:5f:5d:58:d0:ac:cc:cc:01:b8:
                    7a:20:24:d9:a3:85:31:a8:4e:3e:c3:44:31:ba:5b:
                    f0:e4:46:04:27:df:68:89:50:96:48:b2:db:d4:00:
                    11:14:a5:3f:43:fc:c2:98:9a:d6:51:c5:da:34:5c:
                    7d:b0:75:3d:5a:b8:cb:2c:1e:28:f2:44:d9:b8:11:
                    69:98:a7:89:0f:62:2e:d1:d6:ea:a7:f1:54:36:51:
                    2b:59:2f:55:c6:e1:91:f8:9b:4b:df:8f:02:fb:b6:
                    c8:b8:5b:78:96:65:16:f2:95:80:ad:c4:66:5e:17:
                    33:ff:23:85:5b:82:da:ed:30:ed:f4:37:0b:1e:d9:
                    1e:8c:0a:a1:ae:dc:e8:50:93:59:a5:74:6e:f2:96:
                    14:05:19:70:c2:18:37:ee:98:e8:2a:1f:e6:5c:37:
                    3b:43:28:65:2a:74:ac:d6:77:e7:13:d6:dd:4b:4b:
                    68:f2:09:bd:12:8b:ca:01:f9:ec:c6:8a:db:26:cd:
                    ef:ba:74:6f:16:b3:6f:c0:06:e9:e2:f2:5f:41:c8:
                    99:ef
                Exponent: 65537 (0x10001)
        Attributes:
            Requested Extensions:
                X509v3 Key Usage:
                    Digital Signature, Key Encipherment
                X509v3 Subject Alternative Name:
                    DNS:mydomain.ru, DNS:www.mydomain.ru, DNS:*.mydomain.ru, IP Address:192.168.7.1, URI:http://my.examp
le.ru/
                X509v3 Extended Key Usage:
                    TLS Web Server Authentication
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        12:f0:c1:7d:29:2b:c0:05:e1:d0:40:5b:98:e5:a3:40:5a:a0:
        a1:67:c2:19:8d:cd:3d:bf:83:21:c0:9f:3e:16:25:c2:a7:ad:
        07:f7:81:1b:2d:bf:33:f2:c5:ca:ba:38:be:c3:b9:a5:45:c7:
        b1:91:61:e3:39:9f:be:81:f2:95:35:99:38:66:de:71:ea:9e:
        22:63:e2:de:96:21:ab:8d:5e:72:52:32:f6:f4:de:82:f6:d5:
        ad:87:88:d3:2d:12:68:69:6d:a3:13:ee:bb:32:10:a0:c1:7d:
        81:ec:71:11:ee:d3:ae:06:9f:24:21:85:5a:28:6d:fe:43:70:
        6d:1b:ae:e4:ec:aa:2d:9e:dd:7a:47:6e:7e:82:f7:f9:e4:99:
```

госуслуги

Создание запроса на выпуск tls-сертификата с существующим ключом

Рекомендуется генерировать новый закрытый ключ всякий раз, когда вы генерируете CSR

Linux

В командной строке введите:
«openssl req -out test2.csr -new \
-subj "/C=RU/ST=Moscow/L=Moscow/O=The Ministry of Digital Development and Communications/CN=*.mydomain.ru" \
-addext "keyUsage = digitalSignature, keyEncipherment" \
-addext "subjectAltName = DNS:mydomain.ru, DNS:www.mydomain.ru, DNS:*.mydomain.ru"\
-addext "extendedKeyUsage = serverAuth" \
-key /path/to/existsKey.key»,

где:
- test2.csr – наименование запроса, например, mydomain.csr
- C – двухбуквенный код страны, для России – RU
- ST – район, область, например, Moscow
- L – полное название города, например, Moscow
- официальное название организации. Например, The Ministry of Digital Development and Communications
- CN – имя домена, на который оформляется TLS-сертификат. Например, mydomain.ru. Для доменных имён на русском языке следует указывать конвертированное с помощью метода punycode значение, например, xn--j1ail.xn--p1ai

При заполнении параметров ST/L/O/OU кириллицей **необходимо** в запросе указывать ключ «-utf8». Например: «openssl req -out test2.csr -new -subj "/C=RU/ST=Москва/L=Москва/O=Тестовая Организация/OU=Тестовый департамент/CN=*.mydomain.ru" -addext "keyUsage = digitalSignature, keyEncipherment" -addext "subjectAltName = DNS:mydomain.ru, DNS:www.mydomain.ru, DNS:*.mydomain.ru" -addext "extendedKeyUsage = serverAuth" **-utf8** -key /path/to/existsKey.key»

где:
- keyUsage – расширение, определяющее назначение ключа. В запросе **обязательно** должны присутствовать digitalSignature и keyEncipherment, иные – при необходимости
- subjectAltName – расширение, определяющее альтернативное имя субъекта (DNS-имя). **Обязательно** должно быть указано хотя бы одно значение. Пример записи: subjectAltName = DNS:mydomain.ru
- extendedKeyUsage – расширение, определяющее расширенное назначение ключа; в запросе **обязательно** должно присутствовать serverAuth, иные – при необходимости
- existsKey.key – наименование существующего ключа, например, mydomain.key

```
ubuntu@ubuntu:~$ openssl req -out test2.csr -new \
> -subj "/C=RU/ST=Moscow/L=Moscow/O=The Ministry of Digital Development and Communications/CN=*.mydomain.ru" \
> -addext "keyUsage = digitalSignature, keyEncipherment" \
> -addext "subjectAltName = DNS:mydomain.ru, DNS:www.mydomain.ru, DNS:*.mydomain.ru, IP:192.168.7.1, URI:http://my.example.ru/" \
> -addext "extendedKeyUsage = serverAuth" \
> -key ./existsKey.key
ubuntu@ubuntu:~$
```

Проверить созданный запрос можно с помощью следующей команды:
«openssl req -in test2.csr -noout -text»,
«openssl req -in test2.csr -noout -text -nameopt utf8» - при заполнении параметров ST/L/O/OU кириллицей,

где:

- test2.csr – наименование созданного запроса

```
ubuntu@ubuntu:~$ openssl req -in test2.csr -noout -text
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = RU, ST = Moscow, L = Moscow, O = The Ministry of Digital Development and Communications, CN = *.mydomain.ru
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b3:c4:73:be:f2:a2:f6:7e:5b:6c:aa:80:31:60:
                    1b:8a:98:7d:81:3f:99:f1:c2:6b:21:bd:8f:c7:e8:
                    a7:40:3d:61:e9:3d:34:66:ab:1d:ef:d5:7b:94:aa:
                    79:d8:21:ec:7a:ab:96:da:95:08:39:1e:9b:fd:b3:
                    78:96:58:53:85:2b:3b:b1:4a:7d:46:35:75:ac:09:
                    84:20:5e:59:ad:b7:bf:67:b1:da:29:1e:b5:21:e4:
                    9e:f0:e7:61:34:ea:3e:e2:6b:20:a7:17:83:43:43:
                    1b:f4:f6:9e:34:28:cd:5a:c0:2c:1c:ce:a9:b1:98:
                    95:f9:da:9d:37:26:86:2a:09:2d:f6:af:97:a7:0b:
                    88:07:08:9b:39:4d:77:9a:bf:54:f9:a8:d1:5e:91:
                    fe:cc:05:d8:3b:3c:60:3d:b1:77:d6:88:eb:50:6c:
                    92:1f:5e:a9:b3:92:32:51:98:eb:4a:b1:e9:07:db:
                    5e:00:c0:af:07:cb:87:a3:de:81:71:5d:d5:41:90:
                    9d:03:8b:39:c5:6d:55:d3:f1:18:f0:e9:8e:33:2e:
                    b0:5c:87:13:70:6b:99:88:c5:81:f2:f6:09:72:14:
                    3b:70:b8:ff:5d:f2:3f:79:30:df:88:3d:24:3b:03:
                    22:ff:fb:63:ef:00:9f:5f:26:5d:5f:6a:f4:35:51:
                    af:11
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
            X509v3 Subject Alternative Name:
                DNS:mydomain.ru, DNS:www.mydomain.ru, DNS:*.mydomain.ru, IP Address:192.168.7.1, URI:http://my.example.ru/
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
    Signature Algorithm: sha256WithRSAEncryption
         59:00:0c:d2:db:84:a9:6c:0a:b2:94:b1:02:41:88:12:e2:c1:
         fc:d5:a7:72:80:bb:ed:04:85:6a:3c:86:01:94:c3:30:b6:23:
         d1:aa:b6:b9:35:31:51:a9:93:ce:32:80:d6:b3:1c:68:ef:63:
         dc:7c:53:e4:79:7f:e4:18:bc:2f:2e:a3:c6:ae:60:a2:7b:41:
         03:d6:9a:18:9b:04:c5:ed:8f:60:9f:2f:b3:cf:1e:da:1a:83:
         9f:96:2a:22:14:bc:50:18:44:0d:e8:0b:89:0b:9b:46:48:c1:
         2a:22:a6:c8:f8:62:ed:72:5b:08:08:c0:fa:3d:82:cc:65:6b:
         f5:02:71:65:32:06:67:3f:bd:ff:65:33:49:6c:e9:35:3c:47:
```

Windows

В командной строке введите:
«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -out test4.csr -new -subj "/C=RU/ST=Moscow/L=Moscow/O=The Ministry of Digital Development and Communications/CN=*.mydomain.ru" -addext "keyUsage = digitalSignature, keyEncipherment" -addext "subjectAltName = DNS:mydomain.ru, DNS:www.mydomain.ru, DNS:*.mydomain.ru" -addext "extendedKeyUsage = serverAuth" -key /path/to/existsKey.key»,

где:

- test4.csr – наименование запроса, например, mydomain.csr
- C – двухбуквенный код страны, для России – RU
- ST – район, область, например, Moscow
- L – полное название города, например, Moscow
- официальное название организации, например, The Ministry of Digital Development and Communications
- CN – имя домена, на который оформляется TLS-сертификат, например *.mydomain.ru. Для доменных имён на русском языке следует указывать конвертированное с помощью метода punycode значение, например, xn--j1ail.xn--p1ai

При заполнении параметров ST/L/O/OU кириллицей **необходимо** создать в «C:\Program Files\OpenSSL-Win64\bin\cnf» конфигурационный файл mydomain.cnf, заполнить его так:

> «[req]
> prompt = no
> distinguished_name = dn
> [dn]
> C = RU
> ST = Москва
> L = Москва
> O = Тестовая Организация
> OU = Тестовый департамент
> CN = *.mydomain.ru»

и изменить команду перед выполнением:
«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -out test4.csr -new -addext "keyUsage = digitalSignature, keyEncipherment" -addext "subjectAltName = DNS:-mydomain.ru, DNS:www.mydomain.ru, DNS:*.mydomain.ru" -addext "extendedKeyUsage = serverAuth" **-utf8 -config "C:\Program Files\OpenSSL-Win64\bin\cnf\mydomain.cnf"** -key /path/to/existsKey.key»

где:

- keyUsage – расширение, определяющее назначение ключа; в запросе **обязательно** должны присутствовать digitalSignature и keyEncipherment, иные – при необходимости
- subjectAltName – расширение, определяющее альтернативное имя субъекта (DNS-имя). **Обязательно** должно быть указано хотя бы одно значение. Пример записи: subjectAltName = DNS:mydomain.ru
- extendedKeyUsage – расширение, определяющее расширенное назначение ключа; в запросе **обязательно** должно присутствовать serverAuth, иные – при необходимости
- newKey.key – наименование нового ключа, например, mydomain.key

```
C:\Users\Natalia>"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -out test4.csr -new -subj "/C=RU/ST=Moscow/L=Mosco
w/O=The Ministry of Digital Development and Communications/CN=*.mydomain.ru" -addext "keyUsage = digitalSignature, keyEn
cipherment" -addext "subjectAltName = DNS:mydomain.ru, DNS:www.mydomain.ru, DNS:*.mydomain.ru, IP:192.168.7.1, URI:http:
//my.example.ru/" -addext "extendedKeyUsage = serverAuth" -key "C:\Users\Natalia\existsKey.key"
```

Проверить созданный запрос можно с помощью следующей команды:
«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in "\path\to\test4.csr" -noout -text»,
«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in "\path\to\test4.csr" -noout -text -nameopt utf8» - при заполнении параметров ST/L/O/OU кириллицей,

где:

- test4.csr – наименование созданного запроса

```
C:\Users\Natalia>"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in "C:\Users\Natalia\test4.csr" -noout -text
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = RU, ST = Moscow, L = Moscow, O = The Ministry of Digital Development and Communications, CN = *.myd
omain.ru
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c1:81:2c:69:80:84:e5:16:fc:b7:06:17:14:42:
                    37:66:53:0b:76:1d:26:3d:21:02:4e:2e:c7:d9:b2:
                    6c:2b:4a:0a:f3:a1:f1:aa:bc:44:91:a6:c5:f8:be:
                    17:73:17:f1:7d:95:5f:5d:58:d0:ac:cc:cc:01:b8:
                    7a:20:24:d9:a3:85:31:a8:4e:3e:c3:44:31:ba:5b:
                    f0:e4:46:04:27:df:68:89:50:96:48:b2:db:d4:00:
                    11:14:a5:3f:43:fc:c2:98:9a:d6:51:c5:da:34:5c:
                    7d:b0:75:3d:5a:b8:cb:2c:1e:28:f2:44:d9:b8:11:
                    69:98:a7:89:0f:62:2e:d1:d6:ea:a7:f1:54:36:51:
                    2b:59:2f:55:c6:e1:91:f8:9b:4b:df:8f:02:fb:b6:
                    c8:b8:5b:78:96:65:16:f2:95:80:ad:c4:66:5e:17:
                    33:ff:23:85:5b:82:da:ed:30:ed:f4:37:0b:1e:d9:
                    1e:8c:0a:a1:ae:dc:e8:50:93:59:a5:74:6e:f2:96:
                    14:05:19:70:c2:18:37:ee:98:e8:2a:1f:e6:5c:37:
                    3b:43:28:65:2a:74:ac:d6:77:e7:13:d6:dd:4b:4b:
                    68:f2:09:bd:12:8b:ca:01:f9:ec:c6:8a:db:26:cd:
                    ef:ba:74:6f:16:b3:6f:c0:06:e9:e2:f2:5f:41:c8:
                    99:ef
                Exponent: 65537 (0x10001)
        Attributes:
            Requested Extensions:
                X509v3 Key Usage:
                    Digital Signature, Key Encipherment
                X509v3 Subject Alternative Name:
                    DNS:mydomain.ru, DNS:www.mydomain.ru, DNS:*.mydomain.ru, IP Address:192.168.7.1, URI:http://my.examp
le.ru/
                X509v3 Extended Key Usage:
                    TLS Web Server Authentication
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        12:f0:c1:7d:29:2b:c0:05:e1:d0:40:5b:98:e5:a3:40:5a:a0:
        a1:67:c2:19:8d:cd:3d:bf:83:21:c0:9f:3e:16:25:c2:a7:ad:
        07:f7:81:1b:2d:bf:33:f2:c5:ca:ba:38:be:c3:b9:a5:45:c7:
        b1:91:61:e3:39:9f:be:81:f2:95:35:99:38:66:de:71:ea:9e:
        22:63:e2:de:96:21:ab:8d:5e:72:52:32:f6:f4:de:82:f6:d5:
        ad:87:88:d3:2d:12:68:69:6d:a3:13:ee:bb:32:10:a0:c1:7d:
        81:ec:71:11:ee:d3:ae:06:9f:24:21:85:5a:28:6d:fe:43:70:
        6d:1b:ae:e4:ec:aa:2d:9e:dd:7a:47:6e:7e:82:f7:f9:e4:99:
```