госуслуги

Создание запроса на выпуск DV-сертификата с алгоритмом шифрования RSA

1. Создайте конфигурационный файл mydomain.cnf и заполните его согласно примеру:

```
[ req ]
distinguished_name = req_distinguished_name
req_extensions = v3_req
x509_extensions = v3_req
prompt = no
string_mask = utf8only
utf8 = yes

[ req_distinguished_name ]
CN = mydomain.ru
C = RU

[ v3_req ]
keyUsage = digitalSignature, keyEncipherment, keyAgreement
extendedKeyUsage = serverAuth, clientAuth
subjectAltName = DNS:mydomain.ru
```

2. Замените значения внутри файла на ваши:

   – C — двухсимвольный код страны согласно ГОСТ 7.67-2003, для России — RU

   – CN — имя домена, на который оформляется TLS-сертификат, например mydomain.ru. Для доменных имён, состоящих из русских букв, укажите значение, конвертированное с помощью метода punycode, например xn--i1afg.xn--d1acufc.xn--p1ai

   – keyUsage — расширение, определяющее назначение ключа. В запросе обязательно должны присутствовать значения digitalSignature, keyEncipherment и keyAgreement, иные не допускаются

   – extendedKeyUsage — расширение, определяющее расширенное назначение ключа. В запросе обязательно должны присутствовать значения serverAuth и clientAuth, иные не допускаются

   – subjectAltName — расширение, определяющее альтернативное имя субъекта — DNS-имя, равное указанному в CN. В запросе обязательно должно быть указано одно значение. Не допускаются значения типа WildCard: *.mydomain.ru. Пример верной записи: DNS:mydomain.ru

3. Установите приложение OpenSSL и откройте командную строку

Для Linux

4. Для создания запроса в командной строке введите команду: $ openssl req -out mydomain.csr -new -newkey rsa:2048 -nodes -keyout newkey.key -config mydomain.cnf

5. Замените значения внутри команды на ваши:

   – mydomain.csr — имя файла запроса, который будет создан при выполнении команды из п. 4

   – newkey.key — имя файла закрытого ключа, который будет создан при выполнении команды из п. 4

```
user@4d004-nb2:~$ openssl req -out mydomain.csr -new -newkey rsa:2048 -nodes
-keyout newkey.key -config mydomain.cnf
.............+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++*...+.......+...+..+.+.....+.........+..................+..................+
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+..+...+...
...+.........+......+.+...+.....+......+...+..........+...+..................
..+............+.+..+....+......++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++
.+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*......
..+..+...+....+...+.....+..........++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++*...+.+...++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++
-----
```

6. Проверьте созданный запрос с помощью команды: $ openssl req -in mydomain.csr -noout -text -nameopt utf8 -config mydomain.cnf

```
user@4d004-nb2:~$ openssl req -in mydomain.csr -noout -text -nameopt utf8 -co
nfig mydomain.cnf
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN=mydomain.ru, C=RU
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

Для Windows

4. Для создания запроса в командной строке введите команду: > "C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -out mydomain.csr -new -newkey rsa:2048 -nodes -keyout newkey.key -config mydomain.cnf

5. Замените значения внутри команды на ваши:

   – mydomain.csr — имя файла запроса, который будет создан при выполнении команды из п. 4

   – newkey.key — имя файла закрытого ключа, который будет создан при выполнении команды из п. 4

```
C:\Users\User>"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -out mydom
ain.csr -new -newkey rsa:2048 -nodes -keyout newkey.key -config "C:\OpenSSL\m
ydomain.cnf"
....+.........+.....+..........++++++++++++++++++++++++++++++++++++++++*......
.+..++++++++++++++++++++++++++++++++++++*.....................+...+.....
...+.+........+............+.+.....+.......+..............+............+....
.....+.....+.+...+......+.....+.+...+..+.........+.......+........++++++
...+..+...++++++++++++++++++++++++++++++++++++*.....++++++++++++++++++++
++++++++++++++++*.+...+.........+.+......+...+.....+.............+..+...+...
+....+.....+......+..........+..+...+..........+.........+..+......+.......+.
..+..+..........+..+...+.+..............+......+...+...........+.+...+..+...
......+.......+..++++++
-----
```

6. Проверьте созданный запрос с помощью команды: > "C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in mydomain.csr -noout -text -nameopt utf8 -config "mydomain.cnf"

```
C:\Users\User>"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in mydoma
in.csr -noout -text -nameopt utf8 -config "C:\OpenSSL\mydomain.cnf"
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN=mydomain.ru, C=RU
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

7. Если поля с русскими буквами отображаются неправильно, выполните команду: > chcp 65001 и повторите команду проверки запроса

```
C:\Users\User>chcp 65001
Active code page: 65001
```