# Выпуск ключа

**Запрос на сертификат**

Установка OpenSSL

**Windows:**

1. Скачайте подходящую версию с сайта:

[**https://slproweb.com/products/Win32OpenSSL.html**](https://slproweb.com/products/Win32OpenSSL.html)

2. Запустите скачанный файл для установки утилиты

3. Выполните команду:

 openssl genrsa -des3 -out **{private}**.key 2048

 Где **{private}** - название файла с приватным ключом. Заполняется на латинице. например **private**

**На сообщение: “Enter pass phrase for {private}.key:”** придумайте и введите пароль для файла приватного ключа

**На сообщение: “Verifying - Enter pass phrase for {private}.key:”** Повторите ввод пароля.

Приватный ключ сформирован.

# Выпуск CSR сертификата

**Выполните команду:**

openssl req -new -key private.key -out **{key}**.csr

 Где {**key**} - название файла с приватным ключом. Заполняется на латинице. например **key**

**На сообщение “Enter pass phrase for private.key:”** введите пароль ранее указанный для файла приватного ключа **{private}.key**

Далее начните вводить данные:

-----

Country Name (2 letter code) []:RU - Двухсимвольный код страны, согласно ISO-3166.«RU» для России

State or Province Name (full name) []:Moscow - название области или региона без сокращений

Locality Name (eg, city) []:Moscow - название города или населенного пункта

Organization Name (eg, company) []:IP Ivanova Anna Ivanovna - название организации в латинском эквиваленте

Organizational Unit Name (eg, section) []: - название подразделения, для которого заказывается сертификат (необяз. поле)

Common Name (eg, fully qualified host name) []:Ivanova A.A. - ФИО ответственного лица

Email Address []:123456@gmail.com - контактный email (необяз. поле)

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []: - не заполняется

# Отображение открытой части сертификата

**Для просмотра открытого ключа, выполните команду:**

openssl req -in **{private-name}**.csr –text

Где **{private-name}** это имя сертификата

Пример открытого ключа в **Modulus:**

Certificate Request:

 Data:

 Version: 0 (0x0)

 Subject: C=RU, ST=Moscow, L=Moscow, O=IP Ivanova Anna Ivanovna, CN=Ivanova A.I./emailAddress=123456@gmail.com

 Subject Public Key Info:

 Public Key Algorithm: rsaEncryption

 RSA Public-Key: (2048 bit)

 **Modulus:**

 00:f5:01:09:1b:77:6d:60:58:47:a5:1e:4c:a6:8e:

 eb:48:bd:7b:e1:ec:9a:ba:ce:6b:fd:e4:85:1f:47:

 2f:1e:72:90:3f:c3:ea:0f:b2:52:42:d8:4c:01:0f:

 5a:26:d2:67:3e:c8:05:2b:27:49:95:12:11:e8:81:

 85:dd:24:80:80:80:28:aa:ff:b1:ce:0f:c5:02:e7:

 a1:d6:2b:56:39:c4:99:10:5b:28:60:7d:59:98:21:

 89:34:53:71:fc:1f:25:39:a2:09:ec:6d:a5:f8:bf:

 a8:fa:d3:46:95:1c:cc:85:4d:4f:49:cd:58:9d:a8:

 3d:b2:a4:56:09:3c:01:d0:c3:63:d0:00:99:58:4a:

 b9:f4:fa:87:6d:8e:93:6e:6a:41:89:e2:8c:d0:eb:

 ec:54:45:61:3c:dd:82:40:8b:0f:22:71:fb:12:33:

 1a:f9:31:22:a6:f2:04:a4:57:44:d6:b9:36:1e:4c:

 8d:d3:e0:40:14:e7:7b:c1:6e:78:24:7e:04:e2:f2:

 8b:2c:b6:f1:a3:03:98:60:2f:de:da:e2:d4:88:41:

 58:23:91:73:da:c9:a5:4c:19:0e:3a:06:73:f1:ba:

 f9:3d:97:80:6d:29:fa:3f:0b:91:45:b2:0d:92:bf:

 8f:3c:a3:da:f4:06:20:ac:5d:3b:5a:d1:32:0d:ff:

 7e:e1

 Exponent: 65537 (0x10001)

 Attributes:

 a0:00

 Signature Algorithm: sha256WithRSAEncryption

 32:7c:ae:e1:66:0d:2d:b3:b7:b4:9c:d7:aa:19:f3:39:e9:8f:

 b5:1e:fd:76:92:37:0e:d7:ae:6c:4e:71:56:7c:3c:0c:57:72:

 19:dc:87:ed:5d:5f:a6:7f:94:d3:81:2a:45:f9:33:2e:d9:f7:

 9c:7f:a3:62:65:07:ee:d0:2c:8d:40:c7:c0:3a:e7:bf:9f:ef:

 94:a6:2c:10:ba:34:b3:3d:14:41:8d:e3:d0:80:bc:83:a6:89:

 3b:ef:c3:d1:23:1d:72:9e:e2:cb:1f:5c:1a:85:99:69:84:98:

 21:95:81:a3:41:d5:89:da:0d:c8:71:35:e9:96:f2:dc:9e:45:

 34:fa:0e:a0:35:45:bf:79:c0:11:ff:97:42:88:81:20:54:6a:

 35:da:32:99:2c:36:97:c3:1c:a6:bc:ab:3a:fb:ec:ad:0b:29:

 da:72:96:83:ff:4c:f5:16:f7:f6:bf:3d:c2:eb:c1:0c:2f:5b:

 4e:5e:50:53:0c:0f:68:0e:87:d4:bf:e0:4a:8e:b5:3f:bc:f0:

 eb:f4:80:77:00:a3:64:bf:f7:bf:1b:b6:3e:1c:7c:7c:41:92:

 2e:e3:57:99:35:ee:7b:8d:2e:7d:b6:23:60:59:79:8b:61:72:

 4e:55:d6:ac:13:43:a1:d7:81:52:2d:80:f6:26:93:52:ab:78:

 64:c6:3c:c3

-----BEGIN CERTIFICATE REQUEST-----

MIIC0zCCAbsCAQAwgY0xCzAJBgNVBAYTAlJVMQ8wDQYDVQQIDAZNb3Njb3cxDzAN

BgNVBAcMBk1vc2NvdzEjMCEGA1UECgwaSVAgTWFpb3JvdmEgQWxsYSBWYWxlcmV2

bmExFjAUBgNVBAMMDU1haW9yb3ZhIEEuQS4xHzAdBgkqhkiG9w0BCQEWEDE0MzM5

MEBnbWFpbC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQD1AQkb

d21gWEelHkymjutIvXvh7Jq6zmv95IUfRy8ecpA/w+oPslJC2EwBD1om0mc+yAUr

J0mVEhHogYXdJIB5Ryiq/7HOD8UC56HWK1Y5xJkQWyhgfVmYIYk0U3H8HyU5ogns

baX4v6j600aVHMyFTU9JzVidqD2ypFYIPAHQw2PQAJlYSrn0+odtjpNuakGJ4ozQ

6+xURWE83YJAiw8icfsSMxr5MSKm8gSkV0TWuTYeTI3T4EAU53vBbngkfgTi8oss

tvGjA5hgL97a4tSIQVgjkXPayaVMGQ46BnPxuvk9l4BtKfo/C5FFsg2Sv488o9r0

BiCsXTta0TIN/37hAgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEAMnyu4WYNLbO3

tJzXqhnzOemPtR79dpI3DteubE5xVnw8DFdyGdyH7V1fpn+U04EqRfkzLtn3nH+j

YmUH7tAsjUDHwDrnv5/vlKYsELo0sz0UQY3j0IC8g6aJO+/D0SMdcp7iyx9cGoWZ

aYSYIZWBo0HVidoNyHE16Zby3J5FNPoOoDVFv3nAEf+XQoiBIFRqNdoymSw2l8Mc

pryrOvvsrQsp2nKWg/9M9Rb39r89wuvBDC9bTl5QUwwPaA6H1L/gSo61P7zw6/SA

dwCjZL/3vxu2Phx8fEGSLuNXmTXue40ufbYjYFl5i2FyTlXWrBNDodeBUi2A9iaT

Uqt4ZMY8ww==

-----END CERTIFICATE REQUEST-----

**При утрате пароля или компрометации закрытого ключа, сертификат необходимо перевыпустить.**