

Порядок выпуска клиентского и самоподписанного сертификатов

1. Порядок выпуска клиентского сертификата

Для подключения к TLS-шлюзу Банка Партнеру необходимо получить клиентский сертификат.

1. Необходима последняя версия Openssl.

Запустите команду для генерации файла приватного ключа (private key) без пароля (без использования алгоритма шифрования) **name.key** (**Name = наименование Партнера**):

```
openssl genrsa -out privatekey.pem 2048
```

2. Запустите команду для генерации файла запроса на сертификат **name.csr**:

```
openssl req -new -key privatekey.pem -out name.csr
```

3. Сертификат должен выпускаться со следующими параметрами:

| Параметр | Описание и значения |
|-------------------------------|---|
| Signature Algorithm | Идентификатор алгоритма подписи, «id-sha256-with-rsa-encryption» |
| Country Name (C) | Двухсимвольный код страны следует вводить в соответствии с ГОСТ 7.67-2003. Для России следует указывать RU. Количество символов должно быть равно 2 (двум) символам |
| State (ST) | Интерфейс подключения Партнера Для стационарных устройств (кассах): INTE = INTEGRATION, фиксированное значение из четырех латинских символов Для мобильных устройств (приложения для ОС Android / iOS): MOBI = MOBILE, фиксированное значение из пяти латинских символов Для интернет ресурса (интернет магазин): ECOM = ECOMM, фиксированное значение из пяти латинских символов Для комплексного решения, в случае использования партнером нескольких методов по взаимодействию с партнером реализации функционала: MULT = MULTI, фиксированное значение из пяти латинских символов |
| Locality Name (L) | Город нахождения Владельца сертификата латинскими буквами, например, «Moscow». Количество символов не должно превышать 128 (сто двадцать восемь) символов |
| Organization Name (O) | Сокращенное наименование юридического лица латинскими буквами, соответствующее ИНН, указанного в «Organizational Unit Name (OU)», например, «JSC Test Bank». Количество символов не должно превышать 64 (шестьдесят четыре) символа |
| Organizational Unit Name (OU) | Индивидуальный номер налогоплательщика (ИНН) |
| Common Name (CN) | Полностью Фамилия Имя Отчество физического лица (латинскими буквами) владельца сертификата – сотрудника организации, ответственного за использованием данного сертификата. Количество символов не должно превышать 64 (шестьдесят четыре) символа |
| Public-Key | Открытый ключ, длина 2048 бит |
| emailAddress | |

4. Направьте в Банк:

А. Данный запрос в формате *.csr по e-mail адресу: sertsbp@rsb.ru

В. Параметры запроса в формате *.doc/*.docx/*.txt по e-mail адресу: sertsbp@rsb.ru

Параметры запроса можно получить посредством команды «req» в OpenSSL, пример:

```
openssl req -in name.csr -text -out text.txt
```

Пример параметров запроса находится в Приложении №1.

5. Банк в течении трех рабочих дней генерирует сертификат **name.pem** и передаёт его обратно Партнёру вместе с **root-ca.pem**.

Важно: сертификат имеет ограниченный срок действия. Партнёру необходимо отслеживать срок действия сертификата и заблаговременно направить новый запрос на сертификат в Банк. После получения нового сертификата, Партнёру необходимо заменить старые приватный ключ и сертификат на новые.

Узнать срок действия сертификата можно командой: `openssl x509 -in name.pem -noout -text`

Партнёр загружает приватный ключ, сертификат на сервер или в приложение, настраивает программное обеспечение.

2. Порядок выпуска самоподписанного сертификата

Для подписи операций «Возврат» (qrRefund) и B2C (requestTransferB2C), Партнеру необходимо выпустить самоподписанный сертификат.

1. Необходима последняя версия Openssl.

Запустите команду для генерации файла приватного ключа (private key) без пароля (без использования алгоритма шифрования) **name.key** (**Name = наименование Партнера**):

```
openssl genrsa -out signkey.pem 2048
```

2. Запустите команду для генерации файла запроса на сертификат **name.csr**:

```
openssl req -new -key signkey.pem -out name.csr
```

3. Сертификат должен выпускаться со следующими параметрами:

| Параметр | Описание и значения |
|-------------------------------|---|
| Signature Algorithm | Идентификатор алгоритма подписи, «id-sha256-with-rsa-encryption» |
| Country Name (C) | Двухсимвольный код страны следует вводить в соответствии с ГОСТ 7.67-2003. Для России следует указывать RU. Количество символов должно быть равно 2 (двум) символам |
| State (ST) | Интерфейс подключения Партнера Для стационарных устройств (кассах): INTE = INTEGRATION, фиксированное значение из четырех латинских символов Для мобильных устройств (приложения для ОС Android / iOS): MOBI = MOBILE, фиксированное значение из пяти латинских символов Для интернет ресурса (интернет магазин): ECOM = ECOMM, фиксированное значение из пяти латинских символов Для комплексного решения, в случае использования партнером нескольких методов по взаимодействию с партнером реализации функционала: MULT = MULTI, фиксированное значение из пяти латинских символов |
| Locality Name (L) | Город нахождения Владельца сертификата латинскими буквами, например, «Moscow». Количество символов не должно превышать 128 (сто двадцать восемь) символов |
| Organization Name (O) | Сокращенное наименование юридического лица латинскими буквами, соответствующее ИНН, указанного в «Organizational Unit Name (OU)», например, «JSC Test Bank». Количество символов не должно превышать 64 (шестьдесят четыре) символа |
| Organizational Unit Name (OU) | Индивидуальный номер налогоплательщика (ИНН) |
| Common Name (CN) | Полностью Фамилия Имя Отчество физического лица (латинскими буквами) владельца сертификата – сотрудника организации, ответственного за пользованием данного сертификата. Количество символов не должно превышать 64 (шестьдесят четыре) символа |
| Public-Key | Открытый ключ, длина 2048 бит |
| emailAddress | |

4. Подписать запрос **name.csr** командой:

```
openssl x509 -signkey signkey.pem -in name.csr -req -days 3650 -out public.pem
```

5. Полученный сертификат **public.pem** направить в Банк по e-mail адресу: sertsbp@rsb.ru

3. Приложение № 1

!Примечание: курсивный текст в квадратных скобках подлежит удалению.
Курсивный текст в круглых скобка необходимо заполнить.

Запрос на Сертификат

Certificate Request:

[Параметры запроса:]

«Data:

Version: 0 (0x0)

Subject: C=RU, ST=MULT, L=Moscow, O=Test Ромашка, OU=LA0000001076, CN=Test

Ромашка/emailAddress=tech@ Ромашка.ru

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:cb:ac:42:52:db:58:ef:53:84:e4:c6:96:c3:54:
ac:7a:d2:7a:6d:7c:53:3c:f0:2a:03:dd:21:27:38:
cc:43:33:da:4e:18:95:8c:ad:28:a3:87:93:62:e6:
42:59:7c:c9:62:71:ac:96:dd:ff:46:0e:73:66:99:
c8:f5:19:c3:1f:16:df:6e:47:c8:b7:44:9b:e5:30:
f5:da:c8:25:94:8b:3e:c4:6d:9b:49:01:0d:98:84:
7a:18:10:87:b5:d1:31:3f:a0:80:0a:a6:a4:96:b3:
56:70:ec:13:c0:b6:96:73:a9:71:52:18:c9:bd:23:
e0:45:92:10:39:44:f8:b7:79:d7:32:28:db:dc:fd:
e0:8e:fb:f7:9e:62:62:bd:64:b4:2e:96:b3:bb:9d:
c8:25:a4:60:7a:3c:5d:82:67:cb:68:46:80:1f:a9:
c3:03:90:2f:71:43:bc:96:07:e9:a3:69:f3:82:77:
cf:0e:36:cb:f3:a7:b0:7b:8e:f3:0e:0f:45:98:c2:
54:18:2e:a1:27:11:03:7b:a3:9c:bd:a6:15:87:c0:
68:66:e5:45:07:44:32:32:92:4b:e5:88:99:11:28:
e2:80:7a:60:b1:af:3c:55:9a:d5:b6:a2:40:43:e3:
84:5d:87:83:21:f3:b0:b4:d5:50:a7:8a:8e:34:fe:
4d:c7

Exponent: 65537 (0x10001)

Attributes:

a0:00

Signature Algorithm: sha256WithRSAEncryption

21:9d:43:44:4c:dc:f2:db:dd:2c:7e:9b:c9:24:c6:4f:46:a2:
f4:eb:06:d8:b5:70:b0:4f:11:d8:86:bc:10:9c:4a:a3:54:da:
20:d2:2e:c6:89:78:c3:b4:2a:00:0c:c1:c9:c2:87:82:08:3e:
10:61:20:f7:12:0c:30:e7:08:d9:74:b7:50:60:d2:fc:81:00:
b6:e0:c4:24:f3:ae:dc:6e:9a:d0:e1:3e:92:62:8d:b8:ed:67:
a4:fb:e7:10:f4:25:ae:ab:95:59:cf:11:23:1f:3c:bf:07:c3:
e0:db:01:4c:17:c9:cc:69:31:7a:5a:ed:f6:06:6d:58:3b:07:
1b:3a:e2:ee:5f:3f:af:85:67:00:27:60:61:09:94:f2:75:3b:
26:b0:ad:bd:ac:4c:e8:7a:cc:05:67:e2:67:d8:4f:cc:b8:53:
aa:02:77:c6:9e:5d:80:c3:39:6c:10:3f:a4:2d:8a:76:c7:ae:
dd:98:3a:cf:ed:7e:e5:62:e4:f4:a8:1f:23:61:ab:4e:7e:29:
ec:6c:5f:ac:98:2d:7a:64:96:a1:81:14:8e:81:c1:be:fe:11:
2b:db:25:39:9a:8d:9e:e9:69:ab:72:d8:97:11:5c:be:df:a8:
40:a3:b9:7f:18:df:fc:83:2c:87:53:11:4f:58:2f:e9:ae:5a:
58:a5:0b:74

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

MIIC3jCCAcYCAQAwgZgx CzAJBgNVBAYTAIjVMQ0wCwYDVQQIDARNVUxUMQ8wDQYD
VQQHDAZnb3Njb3cxZmFzAVBgNVBAoMDIRlc3QgUGF5S2VlcGVyMRUwEwYDVQQLDAXM
QTAWMDAwMDEwNzYxZmFzAVBgNVBAMMDIRlc3QgUGF5S2VlcGVyMSAwHgYJKoZIhvcN
AQkBFhF0ZWNoQHBheWtlZXBlci5ydTCCASlwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAMusQlLbWO9ThOTGlsNUrHrSem18UzzwKgPdISc4zEMz2k4YIYtKKOH
k2LmQlI8yWJxrJbd/OYOc2aZyPUZwx8W325HyLdEm+Uw9drIJZSLPsRtm0kBDZIE
ehgQh7XRMT+ggAqmpJazVnDsE8C2InOpcVIYyb0j4EWSIEDIE+Ld51zlo29z94I77
955iYr1ktC6Ws7udyCWkYHo8XYJny2hGgB+pwwOQL3FDvJYH6aNp84J3zw42y/On
sHuO8w4PRZjCVBguoSra3ujnL2mFYfAaGblRQdEMjKSS+WImREo4oB6YLGvPFWa
1baiQEPjhF2HgyHzsLTVUKeKjJT+TccCAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IB
AQAhNUNETNzy290sfpvJIMZPRqL06wbYtXCwTxHYhrwQnEqjVNogOi7GiXjDtCoA
DMHJwoeCCD4QYSD3Egww5wjZdLdQYNL8gQC24MQk867cbprQ4T6SYo247Wek++cQ
9CWuq5VZzxEjHzy/B8Pg2wFMF8nMaTF6Wu32Bm1YOWcbOuLuXz+vhWcAJ2BhCZTy
dTsmSK29rEzoeswFZ+Jn2E/MuFOqAnfGnl2AwzlsED+kLYp2x67dmDrP7X7IYuT0
qB8jYatOfinsbF+smC16ZJahgRSOgcG+/hEr2yU5mo2e6WmrctiXEVy+36hAo7I/
GN/8gyyHUxFPWC/prlpYpQt0

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