

RSB FAQ Openssl Windows and macOS

Оглавление

[Инструкция на Русском языке для Windows 2](#_Toc363482344)

Инструкция на Русском языке для macOS 3

[Instruction in English for Windows 4](#_Toc363482345)

Instruction in English for macOS 5

# Инструкция на Русском языке для Windows

Важно: сертификат имеет ограниченный срок действия.

1. Создайте директорию в корне диска с названием не более 8 символов. (К примеру: **C:\ssl\_rsb\**).
2. В данную директорию поместите файлы из архива: **openssl.exe** и **openssl\_rsb.cnf**
3. Выполните команду, где **C:\ssl\_rsb\** указывает на расположение созданной директории:

* cmd.exe /k cd /D **C:\ssl\_rsb\**

1. Запустите команду для генерации файла приватного ключа (private key) без пароля (без использования алгоритма шифрования) ***MerchantID.key (Merchant ID = 929…….)***:

* openssl.exe genrsa -out **MerchantID**.key 2048

1. Запустите команду для генерации файла запроса на сертификат ***MerchantID.req***:

* openssl.exe req -new -config openssl\_rsb.cnf -key **MerchantID**.key -out **MerchantID**.req

1. Во время генерации запроса необходимо придерживаться требованиями ниже, поля заполнять **латинскими символами**:

|  |  |
| --- | --- |
| **Country Name (2 letter code)** | Двухбуквенный код страны (по умолчанию: RU) |
| **City Name (eg, locality)** | Название Города или населённого пункта (по умолчанию: Moscow) |
| **Subject Name (eg, state)** | Субъект: Республика, Край, Область (по умолчанию: Moscow) |
| **Company or Sole trader Title** | Название организации или Ф.И.О. ИП |
| **Department Name in the Company** | Подразделение или название отдела в организации |
| **Merchant ID (Common Name) (CN)** | Номер организации: MerchantID |
| **Company Contact E-mail Address** | Электронный адрес организации |

1. Банк получает данный запрос ***MerchantID.req***

Важно: в Банк направляется только запрос на сертификат \*.req.

1. Банк генерирует сертификат ***MerchantID.pem***и передаёт его обратно в организацию вместе с цепочкой сертификатов **chain-ecomm-ca-root-ca.crt** и сертификатами по отдельности **ecomm-ca.crt** и **root-ca.crt**.

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

Узнать срок действия сертификата можно командой: openssl x509 -in **MerchantID.pem** -noout -text

1. Клиент загружает приватный ключ, сертификат, цепочку сертификатов на сервер или в приложение. Настраивает программное обеспечение. Ниже пример настройки curl на PHP.

|  |  |
| --- | --- |
| **Пример для PHP curl** |  |
| **Директива** | **Значение** |
| $ch = curl\_init(); |  |
| curl\_setopt($curl, CURLOPT\_URL, **$this->bank\_server\_url**); | **https://testsecurepay.rsb.ru:9443/ecomm2/MerchantHandler** |
| curl\_setopt($curl, CURLOPT\_HEADER, FALSE); |  |
| curl\_setopt($curl, CURLOPT\_POST, TRUE); |  |
| curl\_setopt($curl, CURLOPT\_USERAGENT, "User-Agent=Mozilla/5.0 Firefox/1.0.7"); |  |
| curl\_setopt($curl, CURLOPT\_RETURNTRANSFER, TRUE); |  |
| curl\_setopt($curl, CURLOPT\_SSL\_VERIFYHOST, 0); |  |
| curl\_setopt($curl, CURLOPT\_SSLCERT, **$this->pem\_file**); | ***MerchantID.pem*** |
| curl\_setopt($curl, CURLOPT\_SSLKEY, **$this->key\_file**); | ***MerchantID.key*** |
| curl\_setopt($curl, CURLOPT\_SSL\_VERIFYPEER, TRUE); |  |
| curl\_setopt($curl, CURLOPT\_CAINFO, **$this->chain\_file**); | **chain-ecomm-ca-root-ca.crt** |
| curl\_setopt($curl, CURLOPT\_POSTFIELDS, **$this->post**); | Требуемая команда и её переменные |
| curl\_setopt($curl, CURLOPT\_RETURNTRANSFER, TRUE); |  |
| $result\_curl = curl\_exec($ch); |  |
| curl\_close($ch); |  |
| echo $result\_curl; | Визуальный вывод полученного результата |

# Инструкция на Русском языке для macOS.

Важно: сертификат имеет ограниченный срок действия.

1. Необходима последняя версия Openssl (или последняя версия OS X).
2. Создайте директория на диске для ключей (например: Documents**\ssl\_rsb\**).
3. Выполните команды в **terminal.app** (терминале):

* cd ~/Documents/ssl\_rsb

1. Запустите команду для генерации файла приватного ключа (private key) без пароля (без использования алгоритма шифрования) ***MerchantID.***key ***(Merchant ID = 929…….)***:

* openssl genrsa -out **MerchantID**.key 2048

1. Запустите команду для генерации файла запроса на сертификат ***MerchantID.***req:

* openssl req -new -key **MerchantID**.key -out **MerchantID**.req

1. Во время генерации запроса необходимо заполнить **латинскими символами** следующие поля:

|  |  |
| --- | --- |
| **Country Name (2 letter code)** | Двухбуквенный код страны (по умолчанию: RU) |
| **City Name (eg, locality)** | Название Города или населённого пункта (по умолчанию: Moscow) |
| **Subject Name (eg, state)** | Субъект: Республика, Край, Область (по умолчанию: Moscow) |
| **Company or Sole trader Title** | Название организации или Ф.И.О. ИП |
| **Department Name in the Company** | Подразделение или название отдела в организации |
| **Merchant ID (Common Name) (CN)** | Номер организации: MerchantID |
| **Company Contact E-mail Address** | Электронный адрес организации |

1. Банк получает данный запрос ***MerchantID.req***

Важно: в Банк направляется только запрос на сертификат \*.req.

1. Банк генерирует сертификат ***MerchantID.pem***и передаёт его обратно в организацию вместе с цепочкой сертификатов **chain-ecomm-ca-root-ca.crt** и сертификатами по отдельности **ecomm-ca.crt** и **root-ca.crt**.

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

Узнать срок действия сертификата можно командой: openssl x509 -in **MerchantID.pem** -noout -text

1. Клиент загружает приватный ключ, сертификат, цепочку сертификатов на сервер или в приложение. Настраивает программное обеспечение. Ниже пример настройки curl на PHP.

|  |  |
| --- | --- |
| **Пример для PHP curl** |  |
| **Директива** | **Значение** |
| $ch = curl\_init(); |  |
| curl\_setopt($curl, CURLOPT\_URL, **$this->bank\_server\_url**); | **https://testsecurepay.rsb.ru:9443/ecomm2/MerchantHandler** |
| curl\_setopt($curl, CURLOPT\_HEADER, FALSE); |  |
| curl\_setopt($curl, CURLOPT\_POST, TRUE); |  |
| curl\_setopt($curl, CURLOPT\_USERAGENT, "User-Agent=Mozilla/5.0 Firefox/1.0.7"); |  |
| curl\_setopt($curl, CURLOPT\_RETURNTRANSFER, TRUE); |  |
| curl\_setopt($curl, CURLOPT\_SSL\_VERIFYHOST, 0); |  |
| curl\_setopt($curl, CURLOPT\_SSLCERT, **$this->pem\_file**); | **MerchantID.pem** |
| curl\_setopt($curl, CURLOPT\_SSLKEY, **$this->key\_file**); | **MerchantID.key** |
| curl\_setopt($curl, CURLOPT\_SSL\_VERIFYPEER, TRUE); |  |
| curl\_setopt($curl, CURLOPT\_CAINFO, **$this->chain\_file**); | **chain-ecomm-ca-root-ca.crt** |
| curl\_setopt($curl, CURLOPT\_POSTFIELDS, **$this->post**); | Required command and its variables |
| curl\_setopt($curl, CURLOPT\_RETURNTRANSFER, TRUE); |  |
| $result\_curl = curl\_exec($ch); |  |
| curl\_close($ch); |  |
| echo $result\_curl; | The visual output of the result |

# Instruction in English for Windows

Important: the certificate has a limited validity period.

1. Create a directory in the root of the disk with the name not more than 8 characters. (Example: **C:\ssl\_rsb\**).
2. Place the following files into this directory: **openssl.exe** and **openssl\_rsb.cnf**
3. Run the command, where **C:\ssl\_rsb\** points to the location of created directory:

* cmd.exe /k cd /D **C:\ssl\_rsb\**

1. Run the command to generate a private key file without password (without using any encryption algorithm) ***MerchantID.key (Merchant ID = 929…….)***:

* openssl genrsa -out **MerchantID**.key 2048

1. Run the command to generate a certificate request file ***MerchantID.req*** :

* openssl.exe req -new -config openssl\_rsb.cnf -key **MerchantID**.key -out **MerchantID**.req

1. When generating a request, you must fill in the following fields in **Latin characters** (only):

|  |  |
| --- | --- |
| **Country Name (2 letter code)** | Two-letter Country code (default: RU) |
| **City Name (eg, locality)** | Name of the City or Locality (default: Moscow) |
| **Subject Name (eg, state)** | State, Region, Province, (default: Moscow) |
| **Company or Sole trader Title** | Company or Sole trader title |
| **Department Name in the Company** | Division or department name in the company |
| **Merchant ID (Common Name) (CN)** | Company Number: MerchantID |
| **Company Contact E-mail Address** | Company e-mail address |

1. Bank receives the request ***MerchantID.req***

Important: send to the Bank only \*.req file.

1. Bank generates certificate ***MerchantID.pem*** and returns it back to the company including certificates’ chain **chain-ecomm-ca-root-ca.crt** and certificates separately **ecomm-ca.crt** and **root-ca.crt**.

Important: the certificate has a limited validity period. The organization should control the validity period of the certificate and timely provide a new certificate request to the Bank. After receiving the new certificate from the Bank, the organization must replace the old private key and a certificate for the new private key and a certificate.  
In order to check the certificate validity please use the command: openssl x509 -in **MerchantID**.pem -noout -text

1. Merchant uploads the private key, certificate, certificate chain to the server or application. Configures the software. Please see the configuration example for PHP curl.

|  |  |
| --- | --- |
| **Example for PHP curl** |  |
| **Directive** | **Value** |
| $ch = curl\_init(); |  |
| curl\_setopt($curl, CURLOPT\_URL, **$this->bank\_server\_url**); | **https://testsecurepay.rsb.ru:9443/ecomm2/MerchantHandler** |
| curl\_setopt($curl, CURLOPT\_HEADER, FALSE); |  |
| curl\_setopt($curl, CURLOPT\_POST, TRUE); |  |
| curl\_setopt($curl, CURLOPT\_USERAGENT, "User-Agent=Mozilla/5.0 Firefox/1.0.7"); |  |
| curl\_setopt($curl, CURLOPT\_RETURNTRANSFER, TRUE); |  |
| curl\_setopt($curl, CURLOPT\_SSL\_VERIFYHOST, 0); |  |
| curl\_setopt($curl, CURLOPT\_SSLCERT, **$this->pem\_file**); | **MerchantID.pem** |
| curl\_setopt($curl, CURLOPT\_SSLKEY, **$this->key\_file**); | **MerchantID.key** |
| curl\_setopt($curl, CURLOPT\_SSL\_VERIFYPEER, TRUE); |  |
| curl\_setopt($curl, CURLOPT\_CAINFO, **$this->chain\_file**); | **chain-ecomm-ca-root-ca.crt** |
| curl\_setopt($curl, CURLOPT\_POSTFIELDS, **$this->post**); | Required command and its variables |
| curl\_setopt($curl, CURLOPT\_RETURNTRANSFER, TRUE); |  |
| $result\_curl = curl\_exec($ch); |  |
| curl\_close($ch); |  |
| echo $result\_curl; | The visual output of the result |

# Instruction in English language for macOS.

Important: the certificate has a limited validity period.

1. Required any latest version of Openssl (or latest version of OS X).
2. Create a directory on the disk for keys (example: Documents**\ssl\_rsb\**).
3. Run the commands in the **terminal.app**:

* cd ~/Documents/ssl\_rsb

1. Run a command to generate a private key file without password (without using any encryption algorithm) ***MerchantID.***key:

* openssl genrsa -out **MerchantID**.key 2048

1. Run a command to generate a certificate request file ***MerchantID.***req:

* openssl req -new -key **MerchantID**.key -out **MerchantID**.req

|  |  |
| --- | --- |
| **Country Name (2 letter code)** | Two-letter Country code (default: RU) |
| **City Name (eg, locality)** | Name of the City or Locality (default: Moscow) |
| **Subject Name (eg, state)** | State, Region, Province, (default: Moscow) |
| **Company or Sole trader Title** | Company or Sole trader title |
| **Department Name in the Company** | Division or department name in the company |
| **Merchant ID (Common Name) (CN)** | Company Number: MerchantID |
| **Company Contact E-mail Address** | Company e-mail address |

1. Bank receives the request ***MerchantID.req***

Important: you should send to the Bank only \*.req file.

1. Bank generates certificate ***MerchantID.pem*** and returns it back to the company including certificates' chain **chain-ecomm-ca-root-ca.crt** and certificates separately **ecomm-ca.crt** and **root-ca.crt**.

Important: the certificate has a limited validity period. The organization should control the validity period of the certificate and timely provide a new certificate request to the Bank. After receiving the new certificate from the Bank, the organization must replace the old private key and a certificate for the new private key and a certificate.  
In order to check the certificate validity please use the command: openssl x509 -in **MerchantID**.pem -noout -text

1. Merchant uploads the private key, certificate, certificate chain to the server or application. Configures the software. Please see the configuration example for PHP curl.

|  |  |
| --- | --- |
| **Example for PHP curl** |  |
| **Directive** | **Value** |
| $ch = curl\_init(); |  |
| curl\_setopt($curl, CURLOPT\_URL, **$this->bank\_server\_url**); | **https://testsecurepay.rsb.ru:9443/ecomm2/MerchantHandler** |
| curl\_setopt($curl, CURLOPT\_HEADER, FALSE); |  |
| curl\_setopt($curl, CURLOPT\_POST, TRUE); |  |
| curl\_setopt($curl, CURLOPT\_USERAGENT, "User-Agent=Mozilla/5.0 Firefox/1.0.7"); |  |
| curl\_setopt($curl, CURLOPT\_RETURNTRANSFER, TRUE); |  |
| curl\_setopt($curl, CURLOPT\_SSL\_VERIFYHOST, 0); |  |
| curl\_setopt($curl, CURLOPT\_SSLCERT, **$this->pem\_file**); | **MerchantID.pem** |
| curl\_setopt($curl, CURLOPT\_SSLKEY, **$this->key\_file**); | **MerchantID.key** |
| curl\_setopt($curl, CURLOPT\_SSL\_VERIFYPEER, TRUE); |  |
| curl\_setopt($curl, CURLOPT\_CAINFO, **$this->chain\_file**); | **chain-ecomm-ca-root-ca.crt** |
| curl\_setopt($curl, CURLOPT\_POSTFIELDS, **$this->post**); | Required command and its variables |
| curl\_setopt($curl, CURLOPT\_RETURNTRANSFER, TRUE); |  |
| $result\_curl = curl\_exec($ch); |  |
| curl\_close($ch); |  |
| echo $result\_curl; | The visual output of the result |