

Для работы с этим модулем необходимо заключить договор на интернет-эквайринг с ПАО КБ «УБРиР», далее Банк. Это могут сделать только юридические лица или ИП. Для заключения договора можно обратиться в ближайший офис Банка.

Установка модуля.

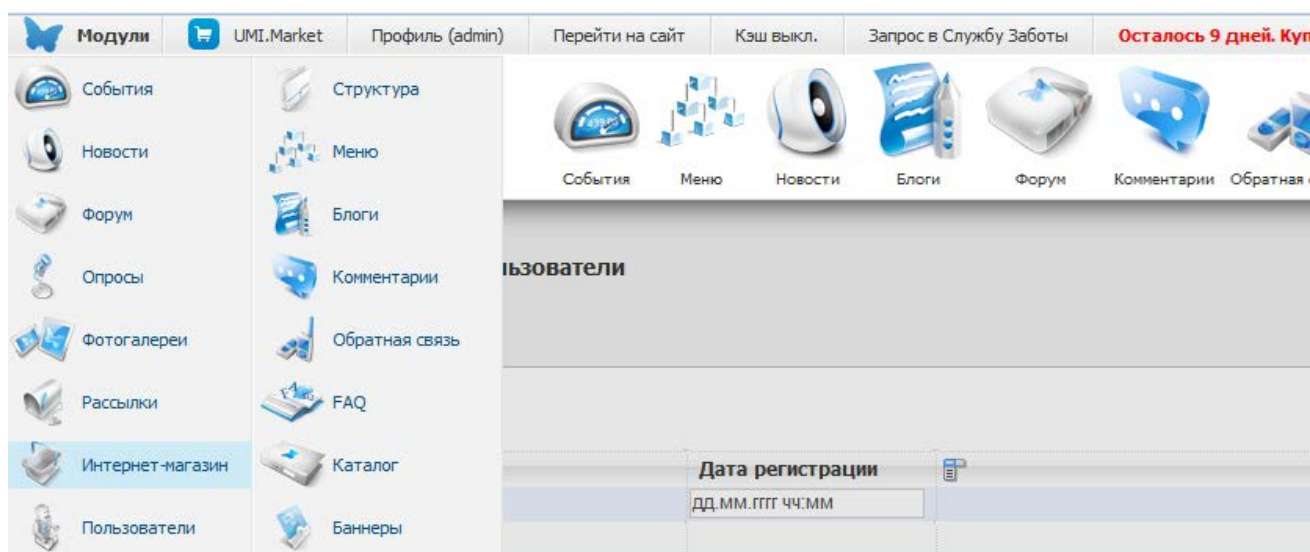
1. Разархивируйте папку в корень сайта
2. Затем перейдите по адресу корень_сайта/ubrir_installer/index.php;

Должно появиться сообщение – Готово!

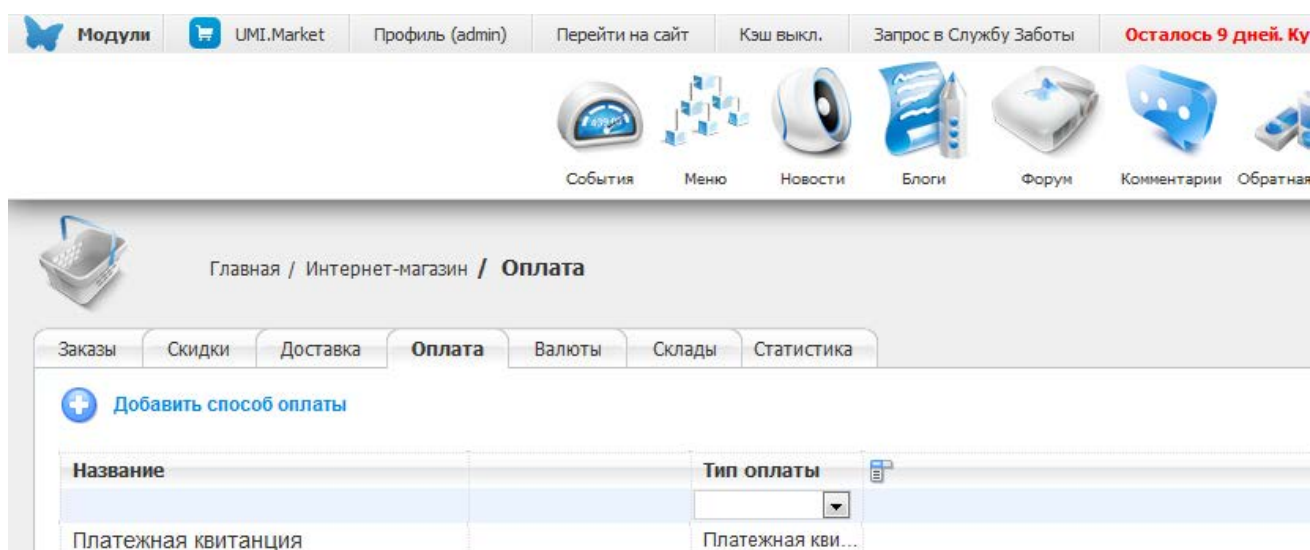
Это значит, что модуль установлен.

Настройка модуля.

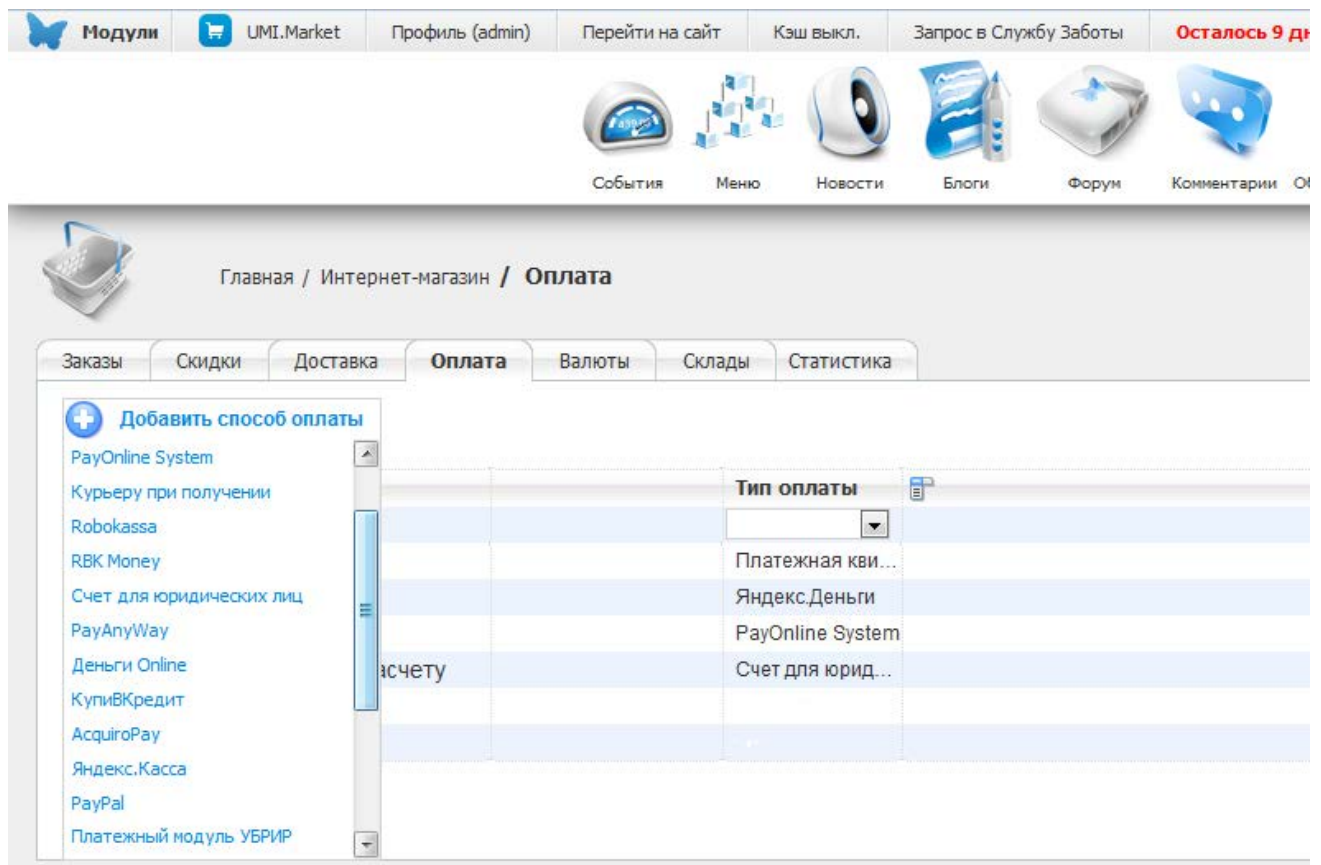
1. В панели управления сайтом перейдите в раздел «Модули» – «Интернет-магазин»;



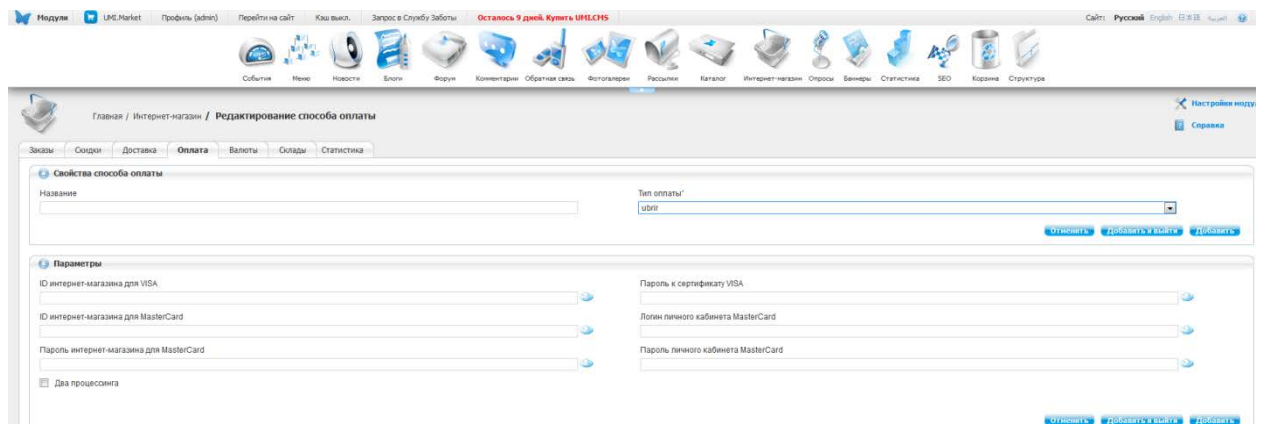
2. Выберите вкладку «Оплата» и нажимаем кнопку «Добавить способ оплаты»;



3. Из доступных способов оплаты выберите Платежный модуль УБРИР



4. Заполните необходимые данные и нажмите «Добавить и выйти».



Пароль к сертификату Visa задается самостоятельно при генерации закрытого ключа (смотреть инструкцию ниже).

Функция «Два процессинга» включается в случае, если планируется принимать к оплате карты Visa и MasterCard. Для приема оплаты картами MasterCard обязательно должны быть указаны:

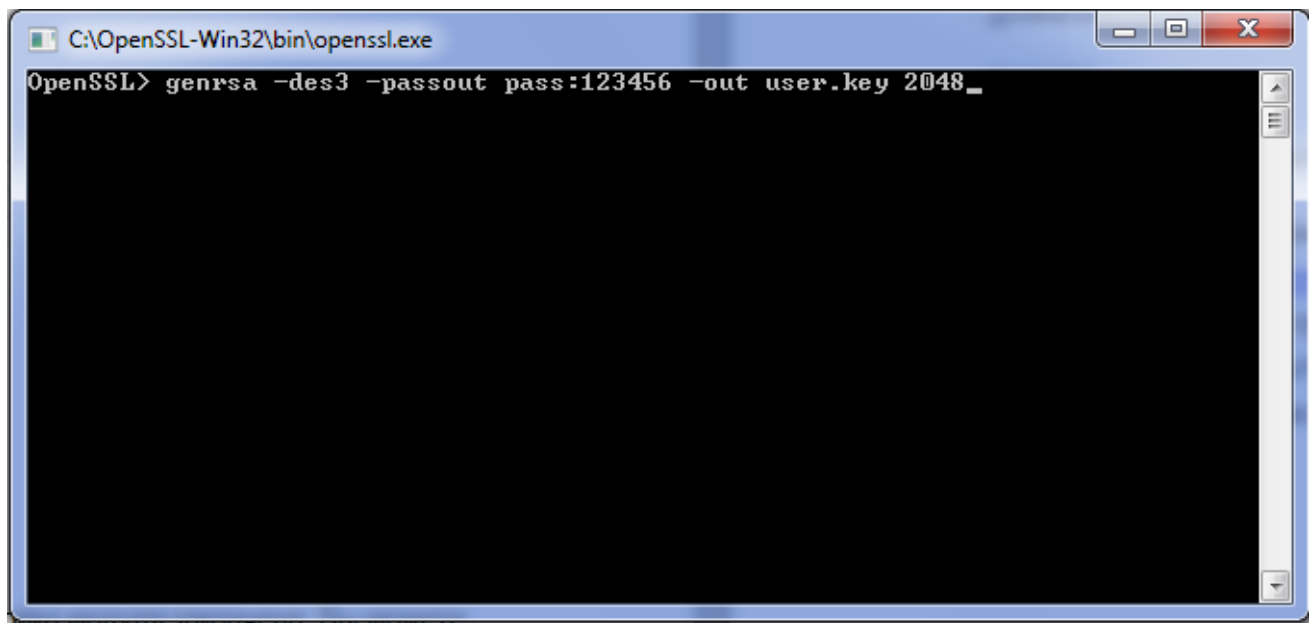
- ID интернет-магазина для MasterCard
- Логин личного кабинета MasterCard
- Пароль интернет-магазина для MasterCard
- Пароль личного кабинета MasterCard

Нажмите кнопку «Сохранить» и переходите к Выпуску ключей и сертификата.

Выпуск ключей и сертификата.

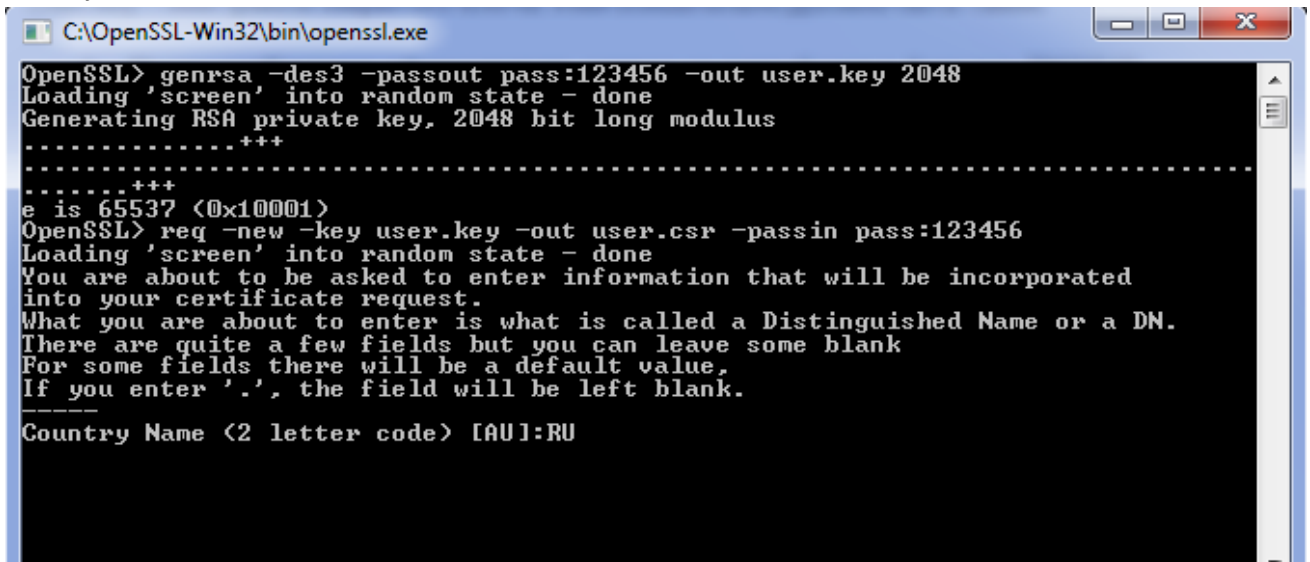
Необходимо самостоятельно создать ключи (ключевую информацию) с использованием программного обеспечения openssl со следующими параметрами:

- длина ключа 2048 bit;
 - SHA256;
 - в качестве Common Name указывается MerchantID (ID интернет-магазина для VISA);
1. Скачиваем и устанавливаем с сайта последнюю версию OpenSSL (<http://slproweb.com/products/Win32OpenSSL.html>);
 2. Запускаем файл openssl.exe;
 3. Выпускаем закрытый ключ
Для этого вводим команду: openssl genrsa -des3 -passout pass:123456 -out user.key 2048
123456 – это пароль к сертификату VISA, Вы задаете его самостоятельно.
User.key – имя файла закрытого ключа. Имя обязательно должно быть таким.



4. После необходимо сформировать запрос на сертификат в формате PKCS10
Запрос можно сформировать следующей командой:
openssl req -new -key user.key -out user.csr -passin pass:123456
123456 – пароль, который был задан при создании закрытого ключа.

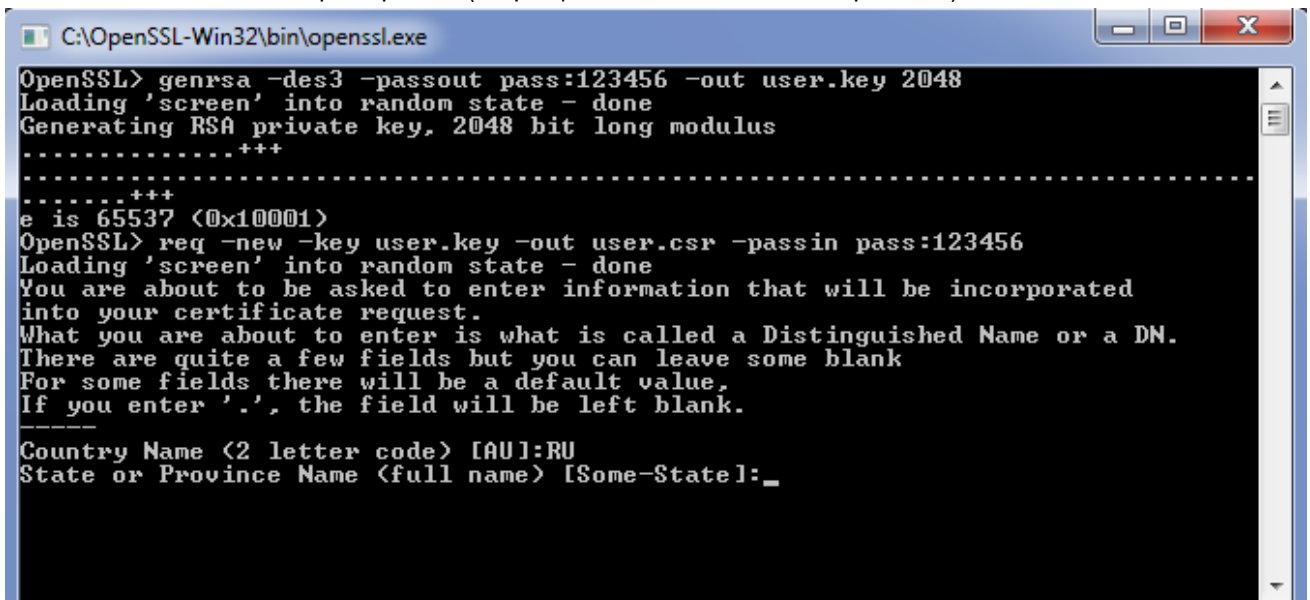
5. В запросе на сертификат, указываем следующие данные:
CountryName: RU



```
C:\OpenSSL-Win32\bin\openssl.exe

OpenSSL> genrsa -des3 -passout pass:123456 -out user.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
OpenSSL> req -new -key user.key -out user.csr -passin pass:123456
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
```

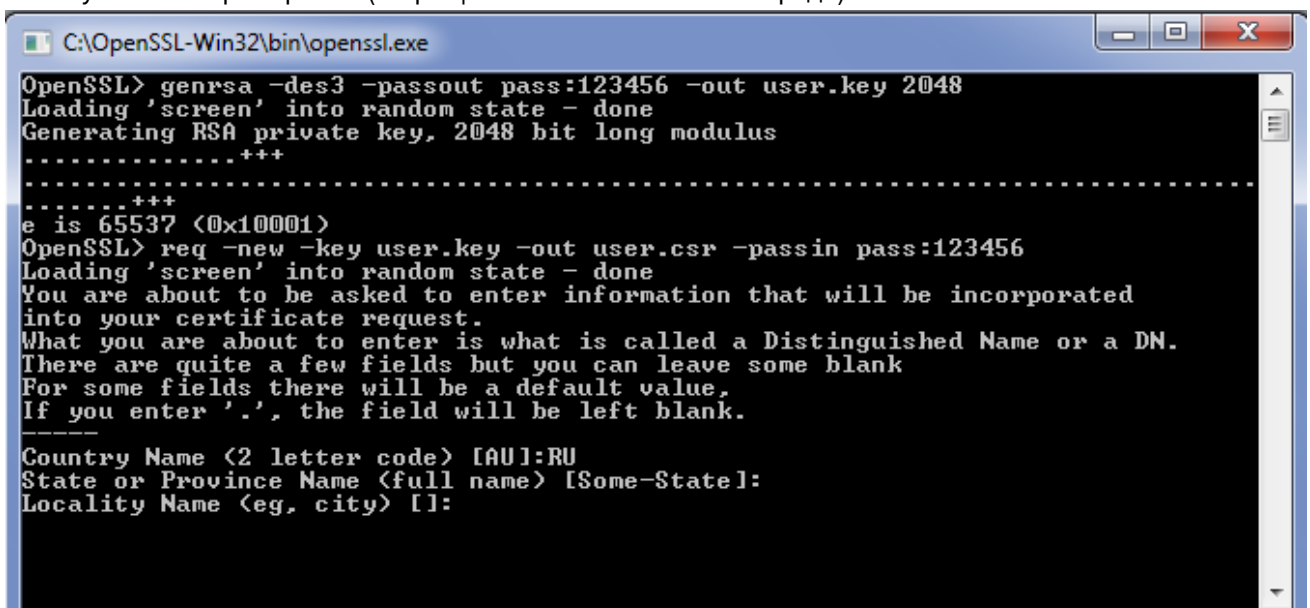
StateorProvinceName: например SVO (сокращенное название своего региона)



```
C:\OpenSSL-Win32\bin\openssl.exe

OpenSSL> genrsa -des3 -passout pass:123456 -out user.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
OpenSSL> req -new -key user.key -out user.csr -passin pass:123456
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:_
```

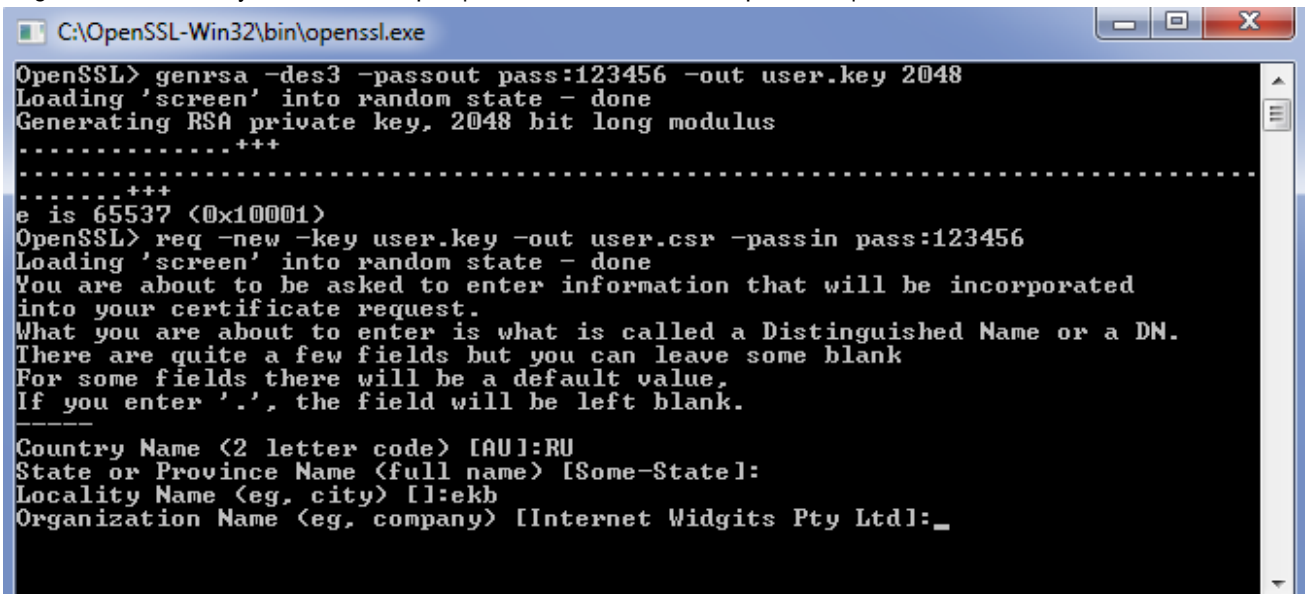
LocalityName: например ЕКВ (сокращенное название своего города)



```
C:\OpenSSL-Win32\bin\openssl.exe

OpenSSL> genrsa -des3 -passout pass:123456 -out user.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
OpenSSL> req -new -key user.key -out user.csr -passin pass:123456
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
```

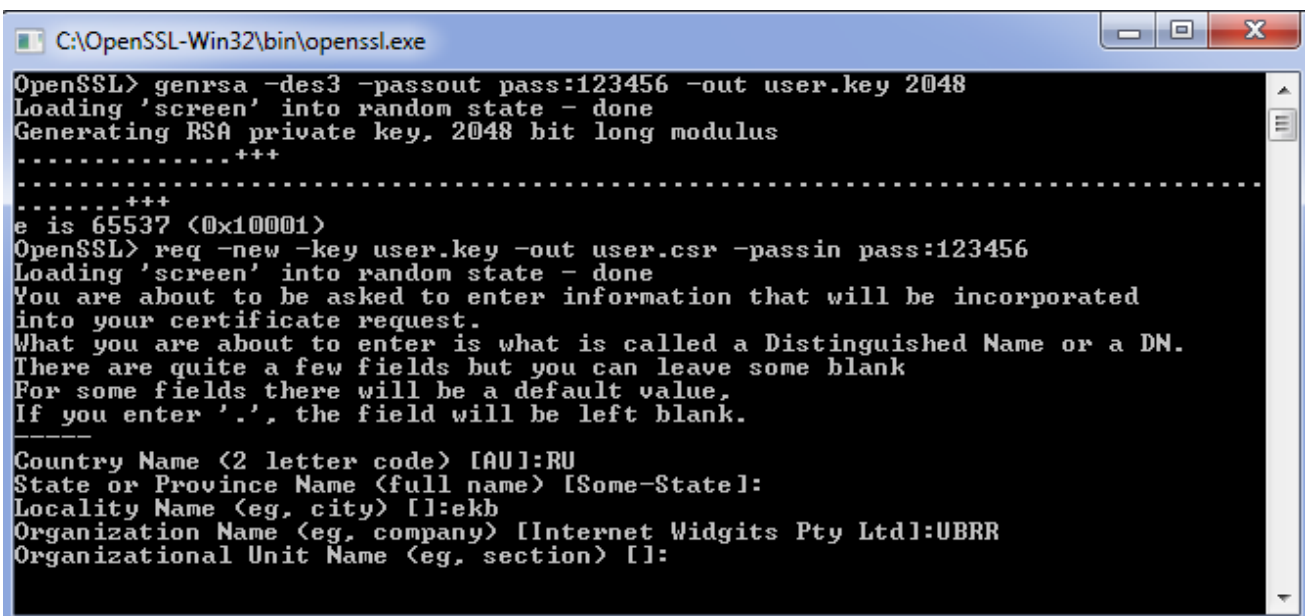
OrganizationName: указываем сокращенно название своей организации на английском.



```
C:\OpenSSL-Win32\bin\openssl.exe

OpenSSL> genrsa -des3 -passout pass:123456 -out user.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
OpenSSL> req -new -key user.key -out user.csr -passin pass:123456
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-Statel]:
Locality Name (eg, city) []:ekb
Organization Name (eg, company) [Internet Widgits Pty Ltd]:_
```

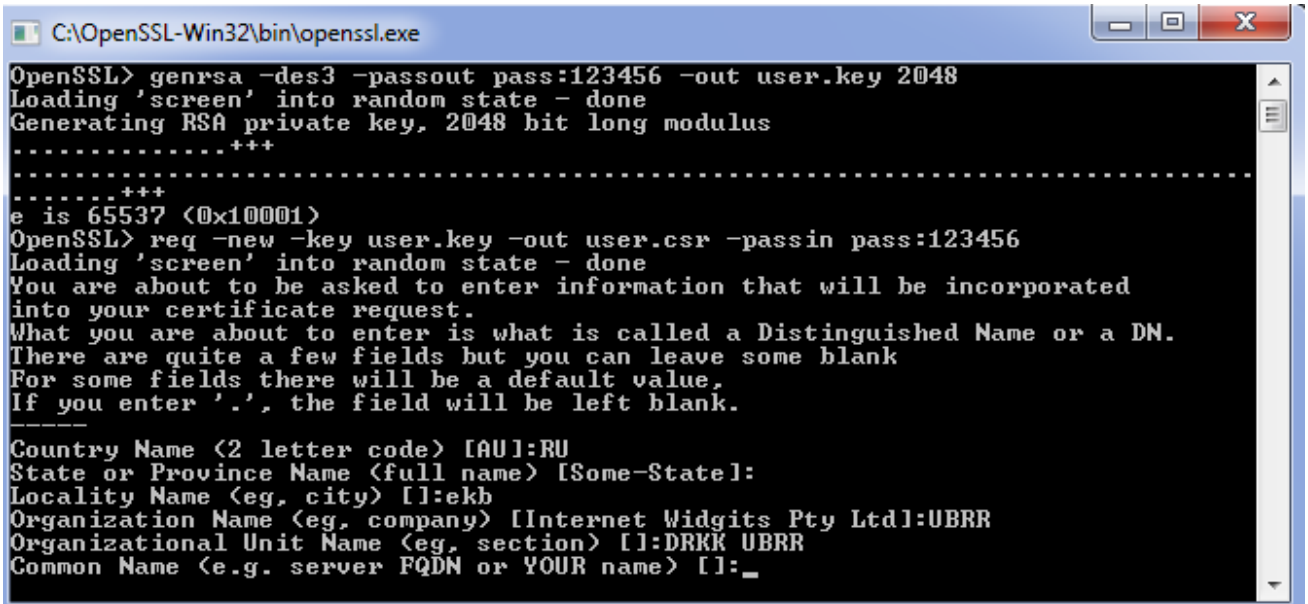
OrganizationalUnitName: указываем сокращенно название подразделения своей организации на английском.



```
C:\OpenSSL-Win32\bin\openssl.exe

OpenSSL> genrsa -des3 -passout pass:123456 -out user.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
OpenSSL> req -new -key user.key -out user.csr -passin pass:123456
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-Statel]:
Locality Name (eg, city) []:ekb
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UBRR
Organizational Unit Name (eg, section) []:
```

CommonName: указываем MerchantID (ID интернет-магазина для VISA)



```
C:\OpenSSL-Win32\bin\openssl.exe

OpenSSL> genrsa -des3 -passout pass:123456 -out user.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
OpenSSL> req -new -key user.key -out user.csr -passin pass:123456
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:ekb
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UBRR
Organizational Unit Name (eg, section) []:DRKK UBRR
Common Name (e.g. server FQDN or YOUR name) []:_
```

Остальные данные можно не заполнять, просто нажимая Enter.

6. Файл запроса user.csr необходимо отправить по электронной почте в Удостоверяющий Центр Банка на электронный адрес eqv@ubrr.ru. В теме письма обязательно указать «Запрос на сертификат для Интернет-эквайринга»;
7. После получения файла user.csr Банк выпускает сертификат в формате X.509 сроком действия один год с именем user.pem и направляет его вместе с сертификатом открытого ключа, на электронную почту, с которой пришел запрос;
В течение 2-х недель после получения сертификата необходимо предоставить в Банк заверенную со своей стороны распечатку сертификата открытого ключа.
После получения сертификата необходимо скопировать сгенерированные файлы личного сертификата и приватного ключа в папку:
корень_сайта/classes/modules/emarket/classes/payment/systems/ubrr_files/certs именами user.pem и user.key соответственно.