**Райфайзенбанк България ЕАД**



**Платежен портал„e- Commerce Connect Gateway”**

**Комуникационен интерфейс**

**Ръководство за администратора на електронен магазин**

[1.](#_3dy6vkm) Общи положения 3

[2.](#_1t3h5sf) Постъпково ръководство за търговци 4

[3.](#_4d34og8) Генериране на ключ 6

[4.](#_2s8eyo1) Данни, предавани от търговеца 9

[5.](#_30j0zll) Връщане на резултатите от обработката на заявката за авторизация на електронния магазин 11

[*6.* Заявка за възстановяване на средства/отмяна от търговеца 13](#_1fob9te)

[6.](#_3znysh7) NOTIFY\_URL 14

[7.](#_17dp8vu) Кодове за отговор на транзакцията 19

[8.](#_2et92p0) Заявка за статуса на транзакцията от страна на търговеца 20

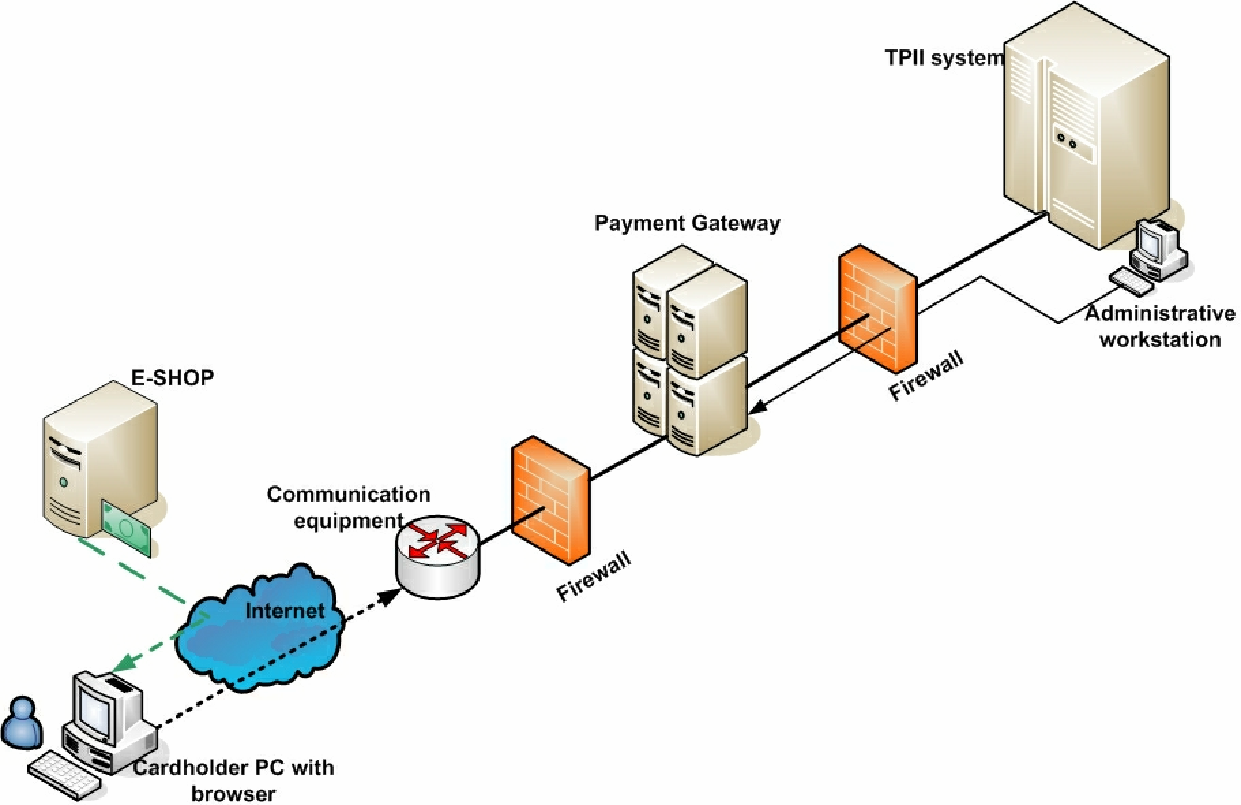
[9.](#_tyjcwt) Преавторизация / поставторизация 21

[10.](#_3rdcrjn) Пример за програмите 22

[Пример в PHP : 22](#_26in1rg)

# **Общи положения**

По време на фазата на проверка на покупателната способност на картата се осъществява взаимодействие между електронен магазин и платежен портал, което става в края на така наречения процес „каса“. За тази фаза е типично клиентът вече да е определил списък с покупки и услуги, техните стойности, условия на доставка и т.н., както и да се е съгласил да извърши плащане с кредитна карта. В този момент основната задача на електронния магазин е да пренасочи клиента към защитена страница на платежния сървър, както и да предаде всички необходими данни за транзакцията чрез линия за пренасочване.



След приключване на пренасочването към защитената страница на портала взаимодействието с клиента се осъществява чрез защитен протокол https. За тази цел платежният портал е снабден със SSL сертификат, издаден от сертифицирана агенция (например агенция „VeriSign“). Въпреки това, за целите на удостоверяване на магазина и за да се защитят данните от модификации по време на процеса на пренасочване, всички критични данни се защитават с MAC (код за удостоверяване на съобщение).

За да осъществява взаимодействие с портала, софтуерът на електронния магазин трябва да има следните страници:

1. Страница с готови стойности за предаване на заявка до платежния портал.
2. Страница (**SUCCESS\_URL**) за пренасочване на браузъра на потребителя в случай на успешна транзакция. Резултатите от обработката се предават в параметрите на отговора.
3. Страница (**FAILURE\_URL**) за пренасочване на браузъра на потребителя в случай на неуспешна транзакция. Резултатите от обработката се предават в параметрите на отговора.
4. Страница (**NOTIFY\_URL**) за предаване на резултатите от транзакцията директно от портала до електронния магазин (незадължителна).

Ако страница 4 не се използва, всички резултати от обработката се предават през страницата на браузъра до адреса на електронния магазин (страници 2, 3). Внедряването на тази страница дава възможност за предаване на резултатите от транзакциите от портала директно до търговеца. Така се повишава нивото на сигурност – търговецът разчита на връзката с портала(адресът на този източник е фиксиран), а не на тази с браузъра на клиента. Още повече, след това одобрение, по време на пренасочването на клиента (стр. 2, 3) в параметрите на отговора се предава само некритична част от резултатите от обработката, като по този начин се гарантира скриването на най-критичните данни от клиента.

Някои софтуери използват динамични елементи за формиране на URL. Обикновено това се случва, когато сървърният софтуер или браузърът не поддържат или изключват системата за поддръжка на бисквитки. В този случай търговецът трябва да осигури схема за формиране на URL.

# **Постъпково ръководство за търговци**

Търговецът (собственикът на електронния магазин) изтегля и попълва регистрационния формуляр. Той се намира на <http://ecommerce.upc.ua/site/docs.html>. Попълненият формуляр се изпраща на [rbbg.vpos@raiffeisen.bg](mailto:rbbg.vpos@raiffeisen.bg) / [ec@upc.ua](mailto:ec@upc.ua).

След известно време търговецът ще получи от UPC имейл със следното съдържание, включително потребителско име и парола:

*Good time of the day,*

*Data for testing:*

*Gateway address:* https://ecg.test.upc.ua/ecgtest/enter/

*MerchantID=1753019*

*TerminalID=E7881019*

*Merchant interface:* https://ecg.test.upc.ua/ecgtest/merchant/

*Login/Password: 1753019 / 1753019*

*Sever certificate: In the attachment*

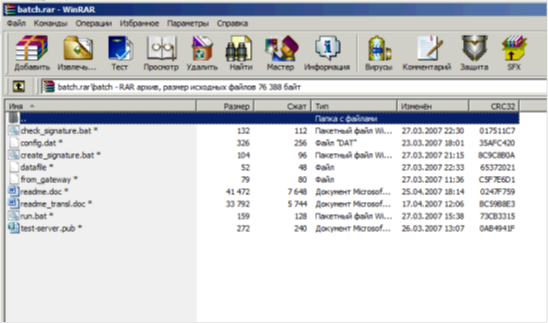
*It is necessary for you to send us a Merchant certificate (file named 1753019.crt) to the following e-mail address:* [*ec@upc.ua*](mailto:ec@upc.ua)

*All necessary documentation can be found here:* [*http://ecommerce.upc.ua/site/docs.html*](http://ecommerce.upc.ua/site/docs.html)

*Test cards:* [*http://ecommerce.upc.ua/docs/Testing.pdf*](http://ecommerce.upc.ua/docs/Testing.pdf)

*(See attached file: test-server.cert)*

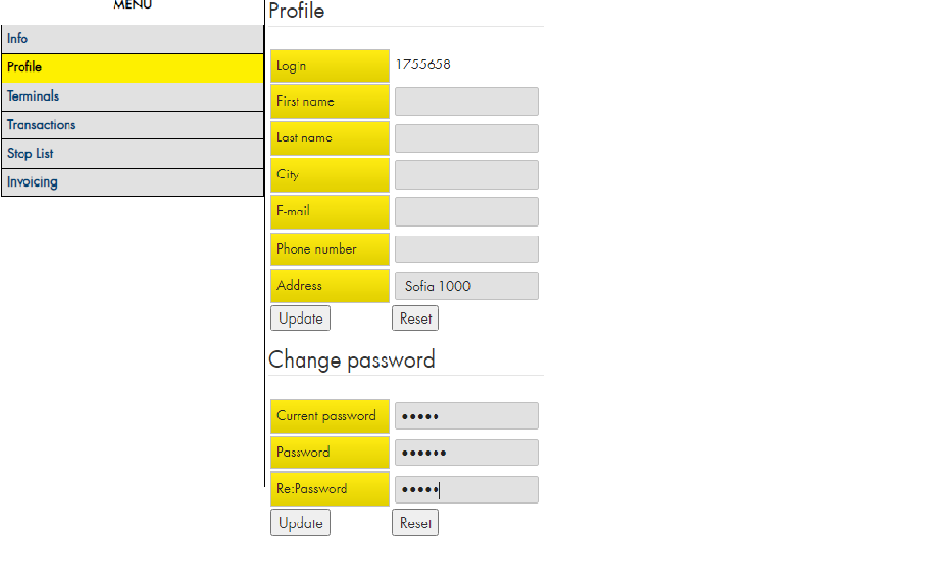
*In the batch.rar archive, please find documents and examples of signature generation.*



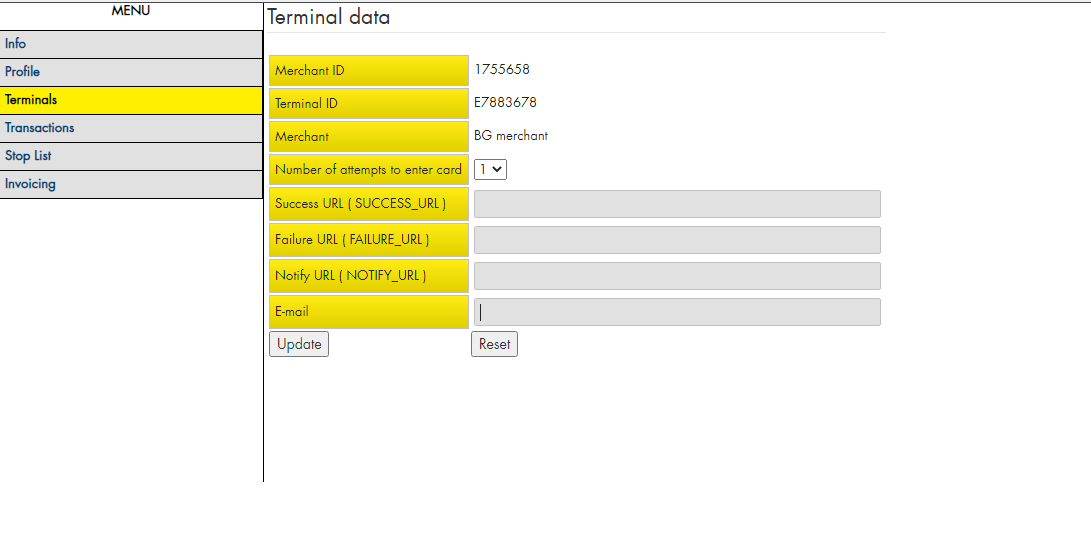
Логата се намират в архива image.rar.

(Вижте прикачения файл: image.rar)

Търговецът отваря връзката [https://ecg.test.upc.ua/ecgtest/merchant/](https://secure.upc.ua/ecgtest/merchant/) и променя паролата на профилната страница:



На страница „Terminal” (терминал) търговецът избира уебсайт и посочва URL за страниците за успешни и неуспешни транзакции.



Също така трябва да се генерира и да ни се изпрати сертификат (трябва да съдържа публични и частни ключове).

# **Генериране на ключ**

Настройка на OpenSSL

Първо трябва да изтеглите Win32 OpenSSL, който се намира на: <http://www.slproweb.com/products/Win32OpenSSL.html>.

За настоящото ръководство е използвана версия [Win32 OpenSSL v0.9.8e](http://www.slproweb.com/download/Win32OpenSSL-0_9_8e.exe).

След настройване на софтуера е важно да се въведе variablePath за каталог bin.

1. В системните променливи:

Variable PATH → “Change”

Поставете точка и запетая в края на реда и въведете път до папката bin: c:\OpenSSL\bin

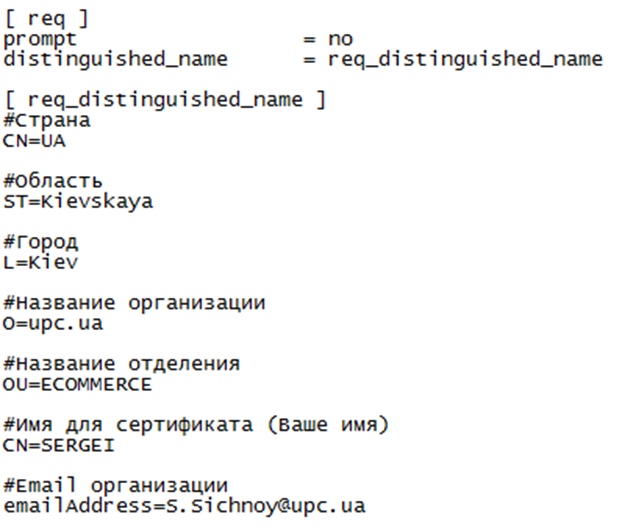
Следващата стъпка е да отворите папката batch в конзолата и да изпълните run.bat (един от прикачените файлове към имейла, получен от UPC).

1. Командата може например да се изпълни във FAR. За да го направите, поставете курсора върху файла run.bat, натиснете Ctrl Enter и добавете MERCHANT ID с интервал.

Генериране на ключ

Ключът се генерира и обменя, след като търговецът изпрати заявка за регистрация и получи атрибути за електронен магазин по интернет (включително идентификатор на търговеца).

Преди генериране на ключа файлът config.dat трябва да се редактира според данните за електронния магазин. Данните във файла config.dat няма напълно да съвпадат с данните в заявката; тези данни не се използват нито за генериране на подпис, нито за проверка на подписа, а само за идентифициране на файла със сертификата.



Командата run.bat с параметъра MerchanID (напр. run.bat 1770000) генерира три файла:

1770000.pem – частен ключ

1770000.pub – публичен ключ

1770000.crt – сертификат

Сега файлът 1753019.crt трябва да се изпрати на [ec@upc.ua](mailto:ec@upc.ua) и да се изчака отговор от UPC. В отговор изпращаме съобщение, че сертификатът е зареден.

Търговецът трябва да има поне следното на сървъра:

1. test-server.cert – файл, изпратен от UPC в имейла за потвърждение на регистрацията (използва се за проверка на отговорите)
2. pem – файл (частен ключ), генериран от търговеца (използва се за подписване на доставените данни)

Генериране на подпис

Подписът се генерира въз основа на два файла: \*.pem и datafile. Datafile съдържа данни (полета), за които се генерира ключът.

Имайте предвид, че трябва да се запази редът на полетата, защото в противен случай заявката ще бъде отхвърлена с код 405 (невалиден подпис).

Полетата се записват в datafile в следния ред (този ред трябва да се спазва и при внедряване на софтуера):

* MerchantId;TerminalId;PurchaseTime;OrderId,Delay;CurrencyId,AltCurrencyId;Amount,AltAmount;SessionData(SD);

Броят знаци ; трябва да остане същия. При липса на дадено поле трябва да се използва ;;. Ако например липсва полето SessionData(SD), datafile ще изглежда така:

* MerchantId;TerminalId;PurchaseTime;OrderId,Delay;CurrencyId,AltCurrencyId;Amount,AltAmount;;

В случай че липсват полетата Delay, AltCurrency или AltAmount, се пропуска запетаята преди тях. Например:

* MerchantId;TerminalId;PurchaseTime;OrderId;CurrencyId,AltCurrencyId;Amount,AltAmount;;
* MerchantId;TerminalId;PurchaseTime;OrderId,Delay;CurrencyId;Amount;;
* MerchantId;TerminalId;PurchaseTime;OrderId;CurrencyId;Amount;;

За да се генерира правилен ключ, datafile не трябва да съдържа допълнителни символи (интервали, въвеждания, нови редове). Datafile трябва да се проверява за ненужни знаци в редактор на HEX или FAR (F3, F4).

Данните трябва да се подреждат по същия начин при базирана на софтуер обработка на подписа.

За генериране на подпис се стартира create\_signature.bat със стойност \*.pem, напр. create\_signature.bat 1770000.pem. В резултат на това се актуализират или създават два файла: signature.bin (подпис) и signature (base64-кодиран подпис). Данните от файла с подписа се изпращат в заявката като подпис. (Бележка: името на полето не може да се въвежда в заявката с малки букви, т.е. полето с име „merchantid” няма да бъде регистрирано като правилно).

Забележка: Генериране на подпис (код)

Вижте примерите в края на документа.

Ако транзакцията е успешна, скриптът ще върне „good”, което означава, че плащането е успешно.

Бележка:

Важно е променливата $data да се поддържа правилна. Генерира се по следния начин:

* MerchantId;TerminalId;PurchaseTime;OrderId,Delay;Xid;CurrencyId,AltCurrencyId;Amount,AltAmount;SessionData;TranCode;ApprovalCode;

Правилата са същите като за полетата Delay, AltCurrencyId, AltAmount – запетаята пред тях се изтрива.

Ако в заявката до портала е налично полето Ref3, то се включва в създаването на подписа. Например

MerchantId;TerminalId;PurchaseTime;OrderId;CurrencyId;Amount;SessionData(SD);Ref3;

**Заявка за възстановяване на средства/отмяна (генериране на подпис)**

Ако има заявка за възстановяване на средства/отмяна, данните се добавят със следните полета: ApprovalCode, RRN. В случай че заявката съдържа полетата RefundAmount и/или Ref3, тези полета се включват в подписа – вижте примерен datafile, съдържащ всички полета:

MerchantId;TerminalId;PurchaseTime;OrderId;CurrencyId;Amount;SessionData(SD);ApprovalCode;RRN;RefundAmount;Ref3;

Ако незадължителното поле (RefundAmount или Ref3) липсва, това поле не се включва. Пример:

MerchantId;TerminalId;PurchaseTime;OrderId;CurrencyId;Amount;SessionData(SD);ApprovalCode;RRN;Ref3;

MerchantId;TerminalId;PurchaseTime;OrderId;CurrencyId;Amount;SessionData(SD);ApprovalCode;RRN;RefundAmount;

MerchantId;TerminalId;PurchaseTime;OrderId;CurrencyId;Amount;SessionData(SD);ApprovalCode;RRN;

За да се създаде правилен подпис, datafile не трябва да съдържа допълнителни символи (интервали, нов ред, въвеждане).

В редактор на HEX или FAR (F3, F4) се потвърждава, че няма допълнителни символи.

По същия начин тези данни трябва да са налични при програмната реализация на подписа.

За създаване на подписа използвайте create\_signature.bat с параметър \*.pem.

Например create\_signature.bat 1770000.pem.

В резултат на това се актуализират или създават два файла: signature.bin (подпис) и signature (подпис в код base64). Данните от файла с подписа се изпращат в заявката като подпис. (Бележка: имената на полетата не могат да се въвеждат в заявката с малки букви, така че полето с име „merchantid” не се счита за валидно).

Проверка на подписа

Полетата трябва да се въвеждат във файла from\_gateway за проверка на подписа на данните в портала в следния ред:

* MerchantId;TerminalId;PurchaseTime;OrderId,Delay;Xid;CurrencyId,AltCurrencyId;Amount,AltAmount;SessionData;TranCode;ApprovalCode;

Всички изисквания по предходната точка са задължителни и за генериране на from\_gateway.

Подписът на данните в портала трябва да се постави във файл с подпис за проверка.

Имайте предвид, че броят значими знаци на един ред от файла с подпис не трябва да надвишава 64 (дължината на реда).

Стартирайте check\_signature.bat, за да се провери подписът.

* MerchantId;TerminalId;PurchaseTime;OrderId,Delay;Xid;CurrencyId,AltCurrencyId;Amount,AltAmount;SessionData;TranCode;ApprovalCode;

# **Данни, предавани от търговеца**

Електронният магазин трябва да предаде редица параметри, когато препраща към защитена страница на портала. Тези параметри са посочени в следната таблица.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Параметър | Структура | | | Формат | | | Описание на параметъра | | Допълнителни коментари | |
| Version | | F | n4 | | | Версия на интерфейса SG | | Версия на интерфейсния протокол. Текущата версия е 0001. Това е помощен параметър за модула за обработка на входящите данни в портала. Използва се избор на по-добра опция за обработка на данните. | | |
| MerchantID | | L | an15 | | | Идентификатор на търговеца | | Определя се от Райфайзенбанк. | | |
| TerminalID | | F | an8 | | | Идентификатор на терминала | | -- // -- | | |
| TotalAmount | | F | n12 | | | Стойност на покупката | | В най-малките единици на валутата (, центове) | | |
| Currency | | F | n3 | | | Валута | | Съгласно договора с Райфайзенбанк | | |
| AltCurrency | | F | n3 | | | Алтернативна валута | | Незадължителен параметър  Използва се в случай че магазинът иска да посочи сумата на плащането в различна валута. | | |
| AltTotalAmount (O) | | F | N1..12 | | | Стойност на поръчката (алтернативна валута) | | Незадължителен параметър  В най-малките единици на валутата (, центове) | | |
| PurchaseTime | | F | n12 | | | Час на покупката във формат ММддччммсс | | гг - година  ММ - месец  дд - ден  ЧЧ - час (0-23)  мм - минута  сс - секунда  З - часова зона (RFC 822)  Формат за зоната -  [+|-] часове минути  Пример  +0300 , -0200  Ако в параметрите не е посочена зона, приема се, че е същата като тази на портала. | | |
| Locale | | F | a2 | | | Език на интерфейса ( en, bg ) | | Език на интерфейса на защитената страница на портала | | |
| OrderID | | L | ans…20 | | | Номер на поръчката с дължина до 20 байта | | Стойността на XID се определя въз основа на OrderID. Ако не може да се използва OrderID, трябва да се използва параметърът XID. | | |
| SD (O) | | Var | an...99 | | | Данни за сесията | | Спомагателен параметър, който може да се използва от електронния магазин за администриране на потребителските сесии. | | |
| PurchaseDesc (О) | | L | ans...125 | | | Кратко описание на покупката | | Незадължителен параметър, предвиден в спецификацията на 3-D Secure. | | |
| Signature | | Var | an….40 | | | Стойност на MAC-код | | Дължината на параметъра зависи от избраната схема за изчисление на MAC-кода. | | |
| Delay | | F | N1 | | | Идентификатор на преавторизацията на плащането | | За преавторизация стойността трябва да е равна на 1, като в противен случай ще е 0 или празна. | | |
| Ref3 (O) | | L | Ans 1 150 | |  | | |  | | |

*Анотация:*

|  |  |
| --- | --- |
| 1. *Описание на структурата*   F – цяло поле  L – изравнено отляво  R – изравнено отдясно  S – допълнено с интервали  Z – допълнено с нули  Var – поле с променлива дължина | *B. Описание на формата*  n - цифров знак, стойност 0..9,  an - буквен или цифров знак, стойност 0..9 или A..Z или ..z,  ans - буквен, цифров или специален знак |

Забележка:

Параметрите AltTotalAmount, AltCurrency се дефинират, ако търговецът трябва да посочи сумата на плащането във валута, различна от валутата по договора с Райфайзенбанк.

Същевременно трябва да се изпратят 4 параметъра до портала:

TotalAmount, Currency – сумата и валутата съгласно условията на договора. Имайте предвид, че транзакцията ще бъде изпълнена съгласно параметрите TotalAmount, Currency. Търговецът е отговорен за съгласуването на общата сума между две различни валути (правилни изчисления по обменния курс). AltTotalAmount, AltCurrency – общата сума и валутата, посочени за плащане в магазина. Валутни кодове: 643 руска рубла, 840 щатски долар, 978 евро, 980 украинска гривна

Тези параметри се предават на страницата на портала в определен HTML-формат по метода HTTPS/POST за допълнително въвеждане на данните за платежната карта от клиента (картодържателя).

*Example:*

<form method="POST" action="https://ecg.test.upc.ua/ecgtest/enter">

<input type="hidden" value="1"name="Version">

<input type="hidden" value="1700000" name="MerchantID">

<input type="hidden" value="E7000000" name="TerminalID">

<input type="hidden" value="30000" name="TotalAmount">

<input type="hidden" value="980" name="Currency">

<input type="hidden" value="ru" name="locale">

<input type="hidden" value="0001" name="OrderID">

<input type="hidden" name="SD" value="sdfhsdfsdfn3432n4jn23j4">

<input type="hidden" value="131222155090" name="PurchaseTime">

<input type="hidden" value="tran\_test" name="PurchaseDesc">

<input type="hidden" name="Signature" value="…..">

<input type="submit">

</form>

По-късно на страницата на портала получените данни се допълват с Card Number (номер на картата), ExpYear (година на изтичане), ExpMonth (месец на изтичане), CVV2 и Card Type (тип карта). Преди това порталът извършва серия от проверки (съществуване на регистрационните параметри на търговеца в базата данни, съответствие на валутата с регистрираната стойност, лимит за авторизация на търговеца, проверка на електронния подпис).

След това порталът предоставя на браузъра на клиента страницата за въвеждане на данните за платежната карта. Същевременно купувачът може да посочи типа карта (при условие че търговецът приема този тип карта). Освен това клиентът може да въведе кода CVV2 (тази функция не се поддържа за карти MEASTRO).

На следващия етап заявката се обработва чрез 3D-Secure или по стандартна схема (криптиране на канал за електронна търговия), в зависимост от параметрите на обслужващата банка.

# **Връщане на резултатите от обработката на заявката за авторизация на електронния магазин**

Резултатите от обработката (резултатите от транзакцията) могат да се предават по два начина:

* препращане на резултатите до адреса NOTIFY\_URL и пренасочване на браузъра на клиента към страница „успешно/неуспешно”
* препращане на резултатите чрез браузъра на клиента към страница „успешно/неуспешно”

В първия случай резултатите от обработката се предават от портала до страницата на електронния магазин по метода HTTP/HTTPS POST. При тези условия може да се постигне ниво на допълнителна защита за електронния магазин чрез ограничаване на достъпа до определен URL само до заявките за портала.

Порталът, използван в сесията, може да получи потвърждение на известието от електронния магазин за състоянието и параметрите на изпълнената транзакция. Едно от предимствата е, че параметрите на обратната транзакция няма да се появят на страницата на клиента.

Списък с параметрите на отговорите до уебсайта на електронния магазин:

|  |  |  |  |
| --- | --- | --- | --- |
| Параметър | Формат | Описание на параметъра | Допълнителни коментари |
| MerchantID | an15 | Идентификатор на търговеца | Подобен на данните в заявката за авторизация |
| TerminalID | an8 | Идентификатор на терминала |  |
| TotalAmount | n12 | Стойност на покупката |  |
| Currency | n3 | Валута |  |
| PurchaseTime | n12 | Час на заявката за покупка (ГГММДДччммсс) |  |
| OrderID | ans..20 | Идентификатор на поръчката |  |
| XID | ans28 | Идентификатор на транзакцията (номер на поръчката с дължина до 20 байта) |  |
| SD | an... 99 | Данни за сесията |  |
| ApprovalCode | n6 | Авторизационен код на хоста |  |
| Rrn | n10 | Референтен номер на извличането | Уникален номер на транзакцията в системата за авторизация и сетълмънт на обслужващата банка |
| ProxyPan | N13…19 | Последните 4 цифри от номера на картата | Стойност на PAN (последните четири цифри), допълнена с водещи нули до дължината на PAN |
| TranCode | n3 | Код за завършване на транзакцията |  |
| Signature | an…40 | Стойност на MAC-кода за избраната схема на комуникацията между порталаи електронния магазин | Дължината на параметъра зависи от избраната схема за изчисление на MAC-кода |

След приключване на сесията на портала с хоста на електронния магазин се извършва окончателно препращане до браузъра. Това изглежда като „одобрена/отхвърлена” транзакция. Предават се минималният брой параметри, включително: OrderID, TranCode и SD.

Адресите на уеб страниците на електронния магазин се извличат от портала от неговата база данни, т.е. те трябва да се предоставят предварително от търговеца по време на регистрацията.

Във втория случай резултатите от обработката се предават чрез страницата на браузъра, където съответстващ формуляр се предава през адреса на уебсайта на търговеца до страница „успешно/неуспешно”. Операцията по иницииране на формуляра се изпълнява от Java Script. Ако не е възможно изпълнение на този език, се показва съобщение за необходимост от ръчно потвърждение на формуляра.

За свързване на клиента със съответната сесия на електронния магазин се използва параметъра purchase SD (данни за сесията), който се предава чрез браузъра на клиента при процеса на обратно пренасочване.

*Example*:

<INPUT TYPE="HIDDEN" NAME="SD" VALUE="584sds565hgj76GGjh6756248">

# ***6.* Заявка за възстановяване на средства/отмяна от търговеца**

Заявката за възстановяване на средства/отмяна се изпълнява само за авторизационна транзакция. За да се извърши отмяната, магазинът изпраща заявката до портала Може да се изпълни чрез изпращане на заявка POST до страницата на портала с параметрите, посочени в таблица request 5:

**Таблица 5**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Параметър | Структура | Формат | Име на параметъра (предназначение) | Допълнителен коментар |
| MerchantID | L | an15 | Идентификатор на търговеца | Определя се от Райфайзенбанк |
| TerminalID | F | an8 | Идентификатор на терминала | -- // -- |
| TotalAmount | F | N1..12 | Сума на заявката | Посочва се в малките валутни единици (центове) |
| Currency | F | n3 | Валута | Определена в договора с Райфайзенбанк |
| PurchaseTime | F | n12..17 | Час на заявката във формат ггММддЧЧммсс или ггММддЧЧммссЗ |  |
| OrderID | L | Ans…20 | Номер на поръчката с дължина до 20 байта |  |
| ApprovalCode | F | An6 | Авторизационен код на хоста |  |
| Rrn | F | n12 | Референтен номер на извличането | Уникален номер на транзакцията в системата за авторизация и сетълмънт на обслужващата банка |
| SD (O) | Var | an...99 | Данни за сесията | Спомагателен параметър, който може да се използва от търговската система за управление на потребителските сесии |
| Signature | Var | Зависи от схемата | Значение на MAC-кода или подписа | Дължината на параметъра зависи от избраната схема за изчисление |
| Ref3 (O) | L | ans..1 150 |  |  |

Порталът създава отговор под формата на текстова страница с параметрите в таблица 6.

**Таблица 6**

|  |  |  |  |
| --- | --- | --- | --- |
| Параметър | Формат | Име на параметъра (предназначение) | Допълнителен коментар |
| TranCode | N3 | Код за завършване на транзакцията | Вижте таблица 3 |
| MerchantID | an15 | Идентификатор на търговеца |  |
| TerminalID | an8 | Идентификатор терминала | --- // --- |
| CardType | an4 | Идентификатор терминала | VISA – Visa  MAST – MasterCard  MAES – Maestro |
| ERROR (0) | ans | Съдържа кратка информация за грешката | Не е задължително и се формира само при възникване на грешка по време на обработката на заявката |

Отмяната се смята за успешна, ако стойността на полето TranCode е = “000”

Example:

<html>

<body>

<form method='POST' action="https://ecg.test.upc.ua/ecgtest/repayment">

<input type='hidden' name='MerchantID' value='1752493' />

<input type='hidden' name='TerminalID' value=' E7880293' />

<input type='hidden' name='OrderID' value='PAY160601124534' />

<input type='hidden' name='Currency' value='980' />

<input type='hidden' name='TotalAmount' value='12550' />

<input type='hidden' name='PurchaseTime' value='160601124534' />

<input type='hidden' name='ApprovalCode' value='123456' />

<input type='hidden' name='RRN' value='2222222222' />

<input type='hidden' name='RefundAmount' value='12000' />

<input type='hidden' name='Signature' value='45F345Fafde4455445Gvb550' />

<input type='submit' value='go'>

</form>

</body>

<html>

# **NOTIFY\_URL**

Успешното и гарантирано пренасочване на браузъра с параметрите на резултатите от плащането е необходимо условие за получаване на плащането в електронния магазин. В някои случаи обаче то може да е неуспешно поради следните ситуации:

1) срив на браузъра, замръзване на компютъра;

2) неправилни действия на потребителя към момента на доставка на отговора;

3) прекъсване на връзката с доставчика на интернет;

4) неправилна работа на браузъра при зададените защитни параметри, което може повлияе на експлоатационните характеристики на браузъра.

Може да възникне ситуация, в която плащането с карта е извършено, но резултатът не е доставен до магазина. В същото време започва разследване между купувача и магазина, за да се елиминира блокирането на сумата на плащането и за да се определи транзакцията като „Платена“ или да се извърши връщане. В такива случаи се препоръчва магазинът да внедри схема с доставка на отговор от портала.

Платежният портал инициира доставка на съобщение. За тестовия сървър съобщението се изпраща от IP-адрес 195.85.198.16, а за работния от – 195.85.198.15. Резултатите се препращат чрез HTTP/HTTPS POST от портала до страницата на електронния магазин (портове 80/443).

Съобщение за заявка за известие:

PurchaseTime = '090929152500'

ProxyPan = '499999\*\*\*\*\*\*\*0011'

Currency = '980'

ApprovalCode = '111111'

MerchantID = '1752493'

OrderID = '111111111111111111'

Signature = test'

Rrn = '2222222222'

XID = '333333-4444444'

Email = 's.sichnoy@upc.ua'

SD = '24ee6084a5343e3d'

TranCode = '000'

TerminalID = 'E7880293'

TotalAmount = '500'

Магазинът връща отговор в основната част на обработената страница. Всеки параметър и неговата зададена стойност като Parameter=Setting се връща на нов ред. Редовете се разделят с цифра.

В допълнение към първоначално зададените параметри (TerminalID, OrderID, Currency, TotalAmount, XID, PurchaseTime) в отговора се връщат 3 нови параметъра:

|  |  |  |
| --- | --- | --- |
| Параметър | Настройка | Описанието |
| Response. action | approve / reverse | Настройката „approve” означава, че магазинът одобрява покупката.  Настройката „reverse” означава, че порталът отменя успешната транзакция и задава код за завършване 503 – «Транзакция, отменена от електронния магазин». |
| Response.reason | An … 255 | Обяснение на отговора на магазина (незадължително)  Например – основание за задаване на Response.action.  Това поле се създава от магазина и се използва само за неговите нужди. В UPC то се записва само в регистрите на транзакциите. |
| Response.forwardUrl | An … 255 | Настройка на URL за пренасочване на браузъра на потребителя вместо  SUCCESS\_URL или NOTIFY\_URL.  Дава възможност за използване на динамични връзки за пренасочване на клиентите. |

echo "MerchantID="1752493"\n";

echo "TerminalID="E7880293"\n";

echo "OrderID="ID0009992"\n";

echo "Currency="980"\n";

echo "TotalAmount="980"\n";

echo "XID="333333-4444444"\n";

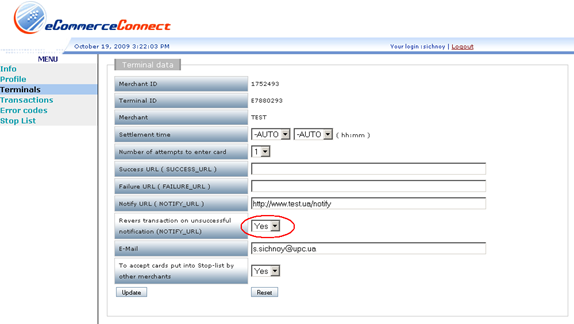
echo "PurchaseTime="090929152500"\n";

**echo "Response.action=\n";**

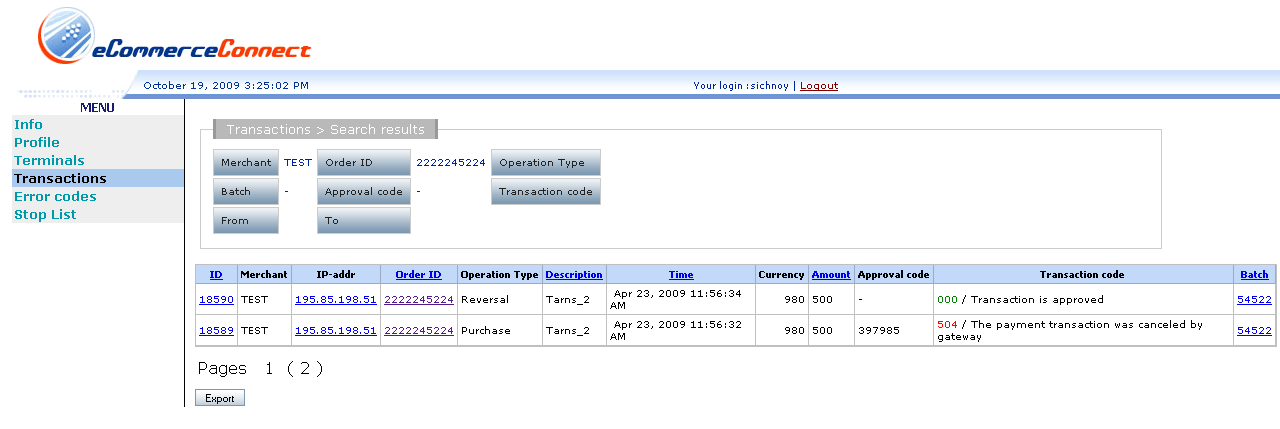
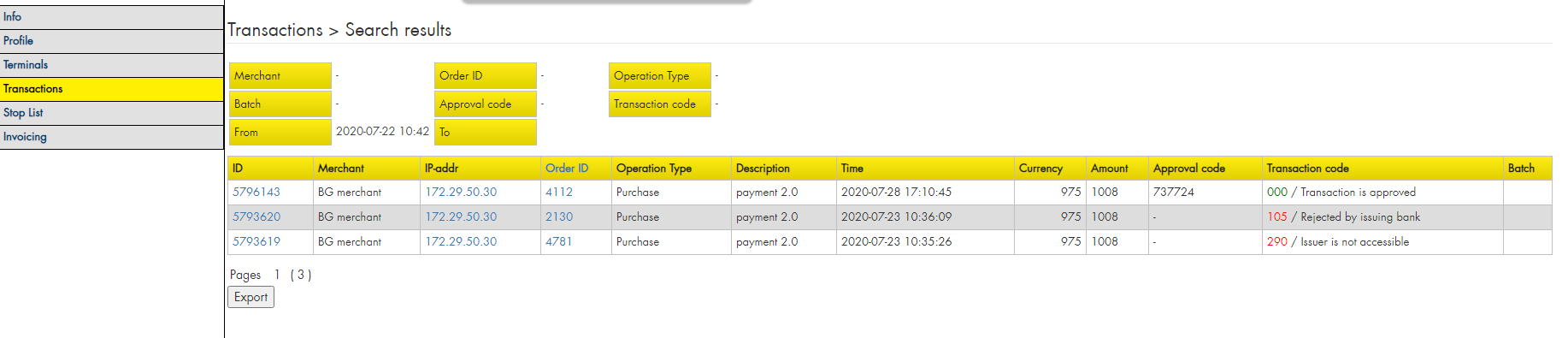
**echo "Response.reason=\n";**

**echo "Response.forwardUrl=\n;**

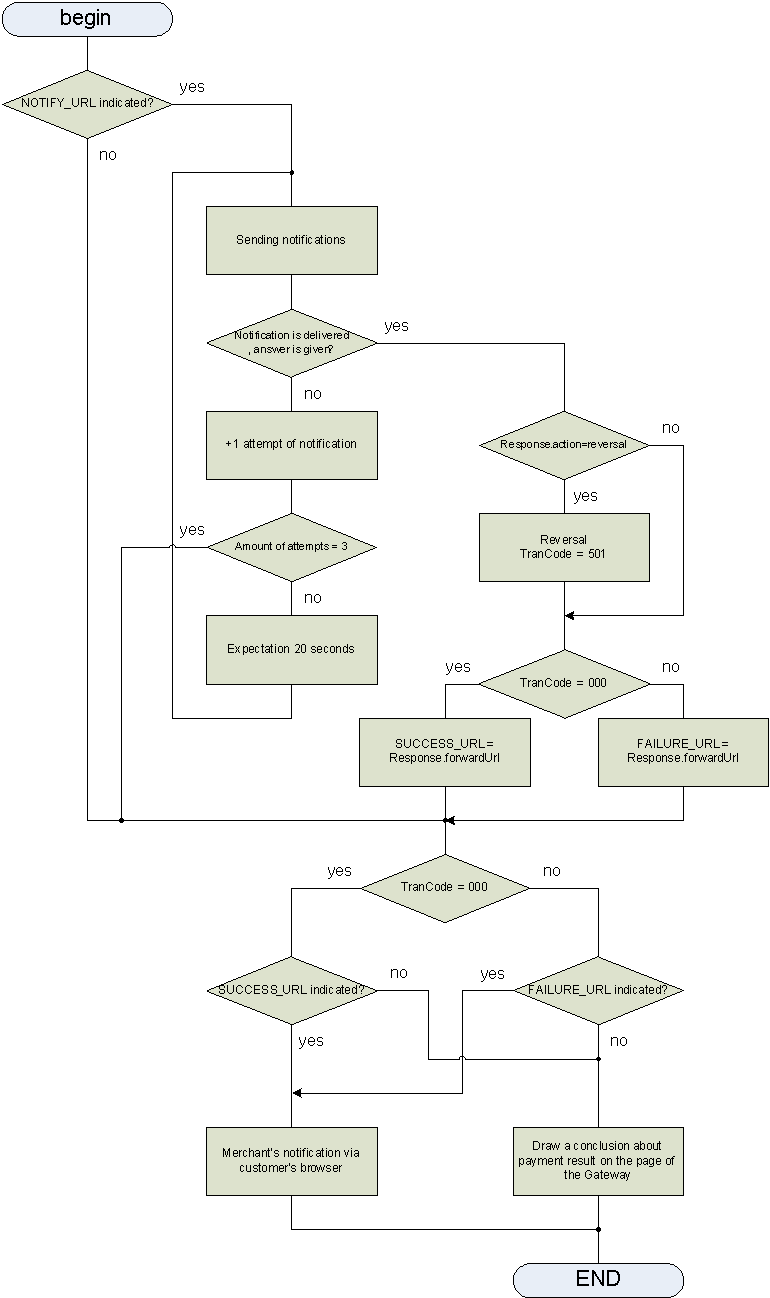
Освен това администраторът на магазина може да разреши избор или ограничаване на транзакциите, за които не се извършва доставка до NOTIFY\_URL. Тази схема дава възможност за автоматично отчитане на системите, които предоставят услуги. По нея се използва информация от платежния портал, за да се избегнат несъответствия в данните, в случай че съобщението не бъде доставено до NOTIFY\_URL.



В случай че по някаква причина схемата за доставка на отговор от платежния портал не работи, транзакцията се отменя автоматично.



В такъв случай, ако първоначалната транзакция е с тип операция „purchase” (покупка) и код на транзакцията „504/This request for payment is not permitted by the gateway” (504/Тази заявка за плащане не е разрешена от портала), платежният сървър автоматично извършва отмяна с код на транзакцията „000/Transaction is completed successfully” (000/Транзакцията е изпълнена успешно).



По-долу е изложена логиката на доставката на отговор от портала.

Това е предпочитаният и препоръчителен метод за предаване на отговора до магазина. Той дава възможност за намаляване на броя неправилно изпълнени транзакции (например такива причинени от грешки в браузъра на потребителя или неправилни действия). Дори в случай на проблемни ситуации електронният магазин ще разполага с информация за резултатите от обработката на транзакцията.

# **Кодове за отговор на транзакцията**

Кодовете за отговор на транзакцията са разделени на няколко класа и подкласа и се използват за информиране на търговеца за резултатите от транзакцията. За посочване на успешна транзакция е необходим един код за отговор. Голяма част от кодовете за отговор предоставят на търговеца обобщена информация за причините за неуспешна транзакция.

|  |  |  |
| --- | --- | --- |
| Кодове въз основа на отговорите на хоста на авторизацията | | Коментари |
| Интегрирани кодове за отговор за електронни магазини | Тълкуване на кодовете | Кодове за отговор в съобщението 1110 |
| 000 | Успешна авторизация | 00x |
|  |  |  |
| 105 | Да не се уважи – от издаващата банка | 100, 103,104,105…107, |
| 116 | Недостатъчни средства | 116 |
| 111 | Несъществуваща карта | 111,125,200,202 |
| 108 | Изгубена или открадната карта | 208,209 |
| 101 | Невалидна дата на изтичане на валидността | 101,201 |
| 130 | Надвишен лимит на сумата | 121,123 |
|  |  |  |
| 290 | Издателят е недостъпен | 905…908,910 |
| 291 | Технически или комуникационен проблем | 9xx (освен посочените по-горе) |
|  |  |  |
| Кодове въз основа на отговорите, генерирани от платежния сървър без препратка към банката хост | |  |
| Вътрешни кодове за грешка на платежния сървър в съответствие с метода за обработка |  |  |
| 401 | Грешка във формата |  |
| 402 | Грешка в параметрите на прихващата организация/търговеца |  |
| 403 | Грешка при свързване с ресурсите на платежната система (DS) |  |
| 404 | Грешка при удостоверяване на клиента |  |
| 405 | Грешка в подписа |  |
| 501 | Транзакцията е отменена от потребителя |  |
| 502 | Изтекла сесия на браузъра |  |

# **Заявка за статуса на транзакцията от страна на търговеца**

За получаване на статуса на плащането се препоръчва търговецът да използва схема, която включва NOTIFY\_URL. В този случай порталът ще се опита да достави резултатите директно на магазина, без да разчита на това, че параметрите ще бъдат изпратени чрез браузъра на потребителя.

Освен това магазинът може да изпрати заявката за статуса на транзакцията от своята страна със следните параметри:

MerchantID=

TerminalID=

OrderID=

Currency=

TotalAmount=

PurchaseTime=

Порталът връща текстова страница с допълнителни параметри –

XID=

TranCode=

ApprovalCode=

Транзакцията се смята за успешна, ако стойността на полето TranCode е = “000”.

Този механизъм за доставка на резултатите от авторизацията се смята за незадължителен, но може да се използва при възникване на определени проблеми с доставката на резултатите чрез браузъра на картодържателя.

<html>

<body>

<form method='POST' action="https://ecg.test.upc.ua/ecgtest/service/01">

<input type='hidden' name='MerchantID' value='6352045'>

<input type='hidden' name='TerminalID' value='ECI62791'>

<input type='hidden' name='OrderID' value='VHS-23684'>

<input type='hidden' name='Currency' value='980'>

<input type='hidden' name='TotalAmount' value='12550'>

<input type='hidden' name='PurchaseTime' value='031227105500'>

<input type='submit' value='go'>

</form>

</body>

<html>

# **Преавторизация / поставторизация**

Търговецът може да използва тип плащане, наричано „Preauthorisation” (преавторизация). Изпраща се заявка до портала, която съдържа допълнителен параметър, наричан **Delay.**

Параметърът е със стойност „1”. Въвежда се до полето OrderId заедно с подписа и неговата проверка. Разделят се със запетая.

Този тип плащане се използва, когато сумата е резервирана на картата, но може да се извърши сетълмънт на друга сума. Може например да се използва в хотелиерството за извършване на предплащане за стая.

Процедурата е както следва:

1. Търговецът изпраща заявка с параметър Delay=1 и с необходимата сума.

2. Картодържателят има обичайна процедура за плащане по схемата 3D-Secure или чрез въвеждане на CVC2.

3. При успешна транзакция се блокират средствата на картодържателя, а транзакцията се определя като тип операция „Preauthorisation”.

4. Тази транзакция не се пренася за допълнителен сетълмънт. За плащането (превод по сметката на търговеца) администраторът го избира (Find: Type of operation=Preauthorisation, Code of transaction=Successful) и посочва окончателна сума за плащане.

5. За тази транзакция има определени ограничения:

- окончателната сума не може да надвишава сумата на първоначалната транзакция с повече от 20%;

- след изтичане на 30 дни от транзакция „Preauthorisation” същата се изтрива автоматично.

6. След успешно окончателно плащане транзакцията „Preauthorisation” се променя в „Postauthorisation” (поставторизация). Това показва, че окончателното плащане е извършено, като се формира нова транзакция за плащане, наричана „Purchase” (покупка).

7. В допълнение към успешната транзакция „Purchase” може да се изпълни само една транзакция „Return” (връщане).

Възможни грешки:

506 – Времето за плащане по транзакция „Preauthorisation” е изтекло (над 30 дни)

507 – Плащането по транзакция „Preauthorisation” вече е извършено (повторен опит)

508 – Грешна сума на плащането (стойността е грешна или надвишава сумата на първоначалната транзакция с повече от 20%)

Test Cards

|  |  |  |
| --- | --- | --- |
| Общи кодове за отговор за електронни магазини | Приблизително тълкуване на отговора на страницата за връщане на отговора на електронния магазин | Номер на картата (дата на изтичане на валидността 12/2050; CVV2-999 |
| 000 | Авторизирани транзакция | 4999999999990011 |
| 105 | Транзакцията не е разрешена от издаващата банка | 4999999999990029 |
| 116 | Недостатъчни средства | 4999999999990037 |
| 111 | Несъществуваща карта | 4999999999990045 |
| 108 | Изгубена или открадната карта | 4999999999990052 |
| 101 | Грешна дата на изтичане на валидността | 4999999999990060 |
| 130 | Разрешеният лимит на овърдрафта е надвишен | 4999999999990078 |
| 290 | Недостъпна издаваща банка | 4999999999990086 |
| 291 | Технически или комуникационен проблем | 4999999999990094 |
| 401 | Грешка във формата |  |
| 402 | Грешка в параметрите на прихващата организация/търговеца |  |
| 403 | Грешка при свързване с източника на платежната система (DS) | 4999999999990102 |
| 404 | Грешка при удостоверяване на купувача | 4999999999990110 |
| 405 | Грешка в подписа |  |
| 501 | Транзакцията е отменена от потребителя |  |
| 502 | Изтекла сесия на браузъра |  |

# **Примери на програмите**

## ***Примери в PHP :***

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<title>Buy</title>

</head>

<body>

<?php

$MerchantID = '1753019';

$TerminalID = 'E7881019';

$OrderID = 19;

$PurchaseTime = date("ymdHis") ;

$TotalAmount = 242;

$CurrencyID = 980;

$data = "$MerchantID;$TerminalID;$PurchaseTime;$OrderID;$CurrencyID;$TotalAmount;;";

$fp = fopen("$MerchantID.pem", "r");

$priv\_key = fread($fp, 8192);

fclose($fp);

$pkeyid = openssl\_get\_privatekey($priv\_key);

openssl\_sign( **$data\*** , $signature, $pkeyid);

openssl\_free\_key($pkeyid);

$b64sign = base64\_encode($signature);

?>

<form action="https://ecg.test.upc.ua/ecgtest/enter" method="post" >

<input name="Version" type="hidden" value="1" />

<input name="MerchantID" type="hidden" value="<?php echo $MerchantID?>" />

<input name="TerminalID" type="hidden" value="<?php echo $TerminalID?>" />

<input name="TotalAmount" type="hidden" value="<?php echo $TotalAmount?>" />

<input name="Currency" type="hidden" value="<?php echo $CurrencyID?>" />

<input name="locale" type="hidden" value="RU" />

<input name="PurchaseTime" type="hidden" value="<?php echo $PurchaseTime ?>" />

<input name="OrderID" type="hidden" value="<?php echo $OrderID?>" />

<input name="Signature" type="hidden" value="<?php echo "$b64sign" ?>"/>

Sum: <?php echo $TotalAmount?> <input type="submit"/>

</form>

</body>

</html>

**\*Забележка**

**$data** се генерира по следния начин:

MerchantId;TerminalId;PurchaseTime;OrderId,Delay;CurrencyId,AltCurrencyId;Amount,AltAmount;SessionData(SD);