

uniteller

self @ online & onlife

e-Commerce Integration manual

Version 1.16 rev.4

Date of creation: 2010-09-30

Date of revision: 2012-03-23

Contents

Terms and definitions	4
General	5
1 Functional features provided within the service of Internet-acquiring.....	5
2 Trade unit activation.....	6
2.1 e-Shop activation.....	6
2.2 e-Shop deactivation.....	6
3 Test connection	7
3.1 The purpose of the test connection and e-shop preparation	7
3.2 Test connection parameters	7
3.3 Test plan.....	8
3.3.1 Test variants	8
3.3.2 Successful payment test	8
3.3.3 Unsuccessful payment test	9
4 Main operations procedure	10
4.1 Authorization request.....	10
4.1.1 General sequence	10
4.1.2 Payment form on the Merchant's e-shop website and its parameters	13
4.1.3 Payment page display methods. Payment page integration into the Merchant's e-shop website.....	17
4.1.4 Payment page on the Uniteller website according to the sent values of the MeanType and EMoneyType parameters	18
4.1.5 Payment in the background mode	22
4.1.6 Payment via external form.....	25
4.2 Payment preauthorization.....	25
4.2.1 General	25
4.2.2 Payment preauthorization process.....	26
4.2.3 Verification of the payment with preauthorization	26
4.3 Recurring payments.....	28
4.3.1 General	28
4.3.2 Recurring payments peculiarities and principles of their arrangement in the Uniteller system.....	29
4.3.3 Recurring payments execution	30
4.4 Credit cards registration for the repeated payments	31
4.4.1 General information about the credit cards registration	31
4.4.2 The necessity of the credit cards registration and general binding procedures.....	32
4.4.3 Security and division of responsibility	32
4.4.4 Routine usage scenarios	33
4.5 Payment cancellation and refund.....	41
4.5.1 Payment cancellation request and possible response formats	41
4.5.2 Cancellation of the payment with preauthorization	43
4.5.3 Refund.....	43
4.6 Authorization results verification	44



4.6.1	Authorization results request	44
4.6.2	Restrictions for the authorization results request	47
4.6.3	e-Shop server notification about the transaction status	47
5	Uniteller Back-office	49
5.1	Browsing the operations list	49
5.2	Refund operation in the Uniteller Back-office	49
6	Technical support	50
7	Help information	50
7.1	Possible fields of S_FIELDS parameters	50
7.2	'Response_code' field value	51
7.3	Response formats	52
7.3.1	Transaction status request	52
7.3.2	Transaction cancellation request	57
7.3.3	Recurring payment request	62
7.4	PHP code samples	63
7.4.1	Obtaining the executed transaction report via SOAP	63
7.5	Payment page signing	64



Terms and definitions

Term	Definition
CVV2 (CVC2)	CVV2 (Card Verification Value 2) – three or four-digit code for a Visa payment system card identifier verification. Protection code for the cards of MasterCard payment system is Card Validation Code 2 (CVC2).
HTTP	Hypertext transfer protocol. An open protocol for data transfer in Internet.
ID	Identifier
IP-адрес	A network address of a node in the PC network built via IP protocol.
PAN	The payment card number (Primary Account Number), credit or debit, which identifies a Card holder's payment system and personal account.
PCI DSS	Payment Card Industry Data Security Standard, a set of security requirements to Cardholders' data, developed by VISA, MasterCard, American Express, JCB, Discover international payment systems.
Uniteller	SJSC Preprocessing center
Authorization	The process of the access rights granting or other authority to the Purchaser to the program or process.
Card holder or Purchaser	The Merchant's e-shop visitor with the purpose to examine and buy the goods/services.
Order	An order in the Uniteller system corresponds to the order in the Merchant's e-shop. Key parameters of the order belong to the Merchant's e-shop, order number, amount, status.
Shop; e-shop	The Merchant's e-Shop web-site which accepts payments from customers; the data are exchanged with the Uniteller system through the website software.
Merchant	A company which has signed <i>CREDIT CARD ACCEPTANCE INFORMATION AND TECHNOLOGICAL SUPPORT SERVICE AGREEMENT</i> with Uniteller.
Operation	The operation in the Uniteller system corresponds to the attempt to pay the order via the method chosen (credit card or the payment via electronic payment system).
Password	Secret line of symbols which serves for Purchaser's authentication.
Protocol	Data exchange method used in networks.
Recurring payment	A payment arranged in the automatic mode as to the set schedule without a Cardholder's participation, on condition that this kind of payment was preliminary agreed and scheduled.
Server	The computer providing the services to other computers of a network.



General

This document is an integration manual which contains the required information to connect and further obtain the uninterrupted Internet-acquiring service provided by Uniteller company.

This integration manual is intended for technical specialists, providing the connection for the Merchant's web resources to the service of Internet-acquiring.

1 Functional features provided within the service of Internet-acquiring

Internet-acquiring is an acceptance of payment cards over in the Internet using a specially developed web-interface that allows making the settlements in the e-shops.

Within the Internet-acquiring service Uniteller processing center provides the following opportunities to its Merchants:

- Acceptance of the following payment methods on the Merchant's e-shop web-site:
 - Credit cards of the main international payment systems (VISA, MasterCard, JCB, Diners Club, ChinaUnionPay);
 - Popular electronic payment systems: PayPal, QIWI Кошелек, WebMoney WMR, Dengi@Mail.Ru, Euroset, Yandex.Money;
 - Payment from the account of a mobile phone (mobile phone payment (Beeline, Megafon, MTS)).
- Detailed customization of the payment page displayed to the Purchaser.
- Payments with preauthorization.
- Recurring payments.
- Credit cards registration to simplify further payments.
- Integration with the main systems for booking and selling the airline tickets.
- The Uniteller system Back-office with a wide range of features for payments monitoring and management.



2 Trade unit activation

2.1 e-Shop activation

The e-shop is activated only on condition if the Merchant is connected to the Uniteller system.

The Merchant is considered connected to the Uniteller system when:

1. The 'Service Agreement on the Information and technological support of the credit cards acceptance' is signed between the Merchant and Uniteller.
2. Cardholder service Agreement is signed with a Bank-acquirer.
3. **MERCHANT_ID** value is obtained from Uniteller.

If the e-shop data, specified in the request, meet the requirements of Uniteller, Bank-acquirer and International payment system, Uniteller starts the e-shop activation and registers it on the Uniteller server with a **TERMINAL_ID** assigned.

To connect the e-shop to the Uniteller system the following steps are required:

- A manager of the Uniteller Sales Department, responsible for this e-shop, enters the following information into the system:
 - Parameters of the concluded 'Service Agreement on the Information and technological support of the credit cards acceptance',
 - Trade units (e-shops) information with the **TERMINAL_IDs** assigned. For each activated e-shop its **Shop_IDP**¹ identifier is given to the Merchant.
- To activate the service of payments acceptance for goods and services with the currencies of electronic payment systems, additional e-money service agreement must be signed. A manager of the Uniteller Sales Department also enters the information under this Agreement into the Uniteller system.

2.2 e-Shop deactivation

The e-shop deactivation means the termination of providing the Uniteller service, including unavailable information on the Merchant's Back-office for this e-shop.

Uniteller can block and deactivate the e-shop upon a written request from the Merchant.

¹ Due to the implemented changes to the Uniteller System, the sales unit (e-shop) identifier has changed its name to **Uniteller Point ID** in the Uniteller Back-office. Its value is available in "e-Shops" menu item, **Uniteller Point ID** column. Should you face any issues, please, contact Uniteller Technical support.

3 Test connection

3.1 The purpose of the test connection and e-shop preparation

The test connection of the Merchant's e-shop to the Uniteller system is an obligatory stage of the Internet-acquiring service and is performed with the following purpose:

- Initial registration of the Merchant's e-shop in the Uniteller system. (Uniteller assigns an e-shop ID to each Merchant's e-shop during its activation);
- Implementation of the algorithms for the data exchange with the Uniteller website in the e-shop website software and verification of their accurate work;
- The familiarization of the Merchant's employees with the functional peculiarities of the Uniteller system Back-office;
- Training the Merchant's employees to accept the credit card payments.

The test connection is performed only on the Uniteller test server.

For the test connection, Uniteller provides the following information to the Merchant:

- Test cards data with the information required for the test connection (see Section 3.2.2 'Successful payment test', page 8 and Section 3.3.3 'Unsuccessful payment test', page 8).
- E-shop test number
- Key addresses on the Uniteller test server (see Section 3.2 'Test connection parameters', page 7)
- Test plan (see Section 3.3 'Test plan', page 7).



Only Uniteller test cards must be used during the test activation. Real credit cards data are not allowed.

To arrange a test connection of the Merchant's e-shop to the Uniteller system, it is necessary to examine the general sequence of the sale operation (see Section 4.1.1 'General sequence of the sale operation, page 10) and add the payment form onto the e-shop website page (see Section 4.1.2 'Payment form on the Merchant's e-shop website and its parameters', page)

In the process of the preparation to the test connection and testing, it is recommended to keep in contact with Uniteller Technical support to agree steps and solve the arising issues (contact details of the Uniteller Technical support are given in the Section 6 'User technical support', page 13).

3.2 Test connection parameters

The following server addresses must be used for the test connection:

- As an address of the payment page of the payment gateway (URL-address must be specified in the payment HTML-form on the e-shop website) - <https://test.wpay.uniteller.ru/pay/>
- To obtain authorization results - <https://test.wpay.uniteller.ru/results/>
- To obtain WSDL file - <https://test.wpay.uniteller.ru/results/wsd/>
- To access the test Back-office- <https://test.lk.uniteller.ru/>.

The Merchant is provided with the login test parameters (login and password) to the Uniteller system.



Notice: The function of the payment with electronic currencies is not supported during the test connection. Thus, **MeanType** and **EMoneyType** parameters must not be sent in the payment test request or their values must be empty (according to calculation algorithm of the **Signature**, the obligatory parameter, specified in Table 1, page 12). The value of md5 hash-function of an empty string must be substituted instead of the **MeanType** and **EMoneyType** parameter values.

3.3 Test plan

3.3.1 Test variants

Uniteller provides two test variants to the Merchant:

1. **Successful payment test** – payment with a test card #1 with correct parameters.

This test allows checking the case when the Purchaser makes credit card payment with correct parameters on the Merchant's website. As a result: the payment is accepted, the successful payment message is displayed, the order is sent to be processed, etc.

- **Unsuccessful payment test** – payment with a test card #2 with incorrect data (wrong card number, not enough funds, etc.)

This test allows checking the case when the Purchaser makes credit card payment with incorrect parameters on the Merchant's website. As a result: the payment is not accepted, the unsuccessful payment message is displayed, the order is not sent to be processed, etc.

3.3.2 Successful payment test

All fields on the credit card payment form are obligatory.

Test card #1 parameters:

- Cardholder Name
- Country
- City
- Address
- Phone number
- E-mail
- Card type: VISA
- Card number: 4405050300000000
- Expiration date: 12/2015
- CVV2: 123
- Issuing bank name: any, for example, UCS
- Phone number of a bank tech support: any

After a successful transaction, the page with the transaction information and **[Back to e-shop]** button is displayed to the Purchaser. When this button is clicked the Purchaser's browser should be redirected to the Merchant's website to the page address specified for the **URL_RETURN_OK** variable, which corresponds to the successful transaction.

The test environment also allows generating the payment system error while purchasing via this credit



card.

The payment amount defines the transaction result in the following way:

- If the amount is within $0 \leq \text{amount} \leq 1000.01$, successful payment message is displayed.
- If the amount is within $1000.01 \leq \text{amount} \leq 2000.00$, "Not sufficient funds" error is displayed.
- If the amount is within $2000.01 \leq \text{amount} \leq 3000.00$, "Your payment is rejected. Please, check if your credit card information is entered correctly and try again" message is displayed.
- If the amount is > 3000.00 , the server response time is increased up to 110 seconds.

3.3.3 Unsuccessful payment test

All fields on the credit card payment form are obligatory.

Test card #2 parameters:

- Cardholder Name
- County
- City
- Address
- Phone number
- E-mail
- Card type: VISA
- Card number: 4405050300000001
- Expiration date: 12/2015
- CVV2: 123
- Issuing bank name: any, for example, UCS
- Phone number of a bank tech support: any

As a result of the transaction with this card, the payment page with the corresponding message error must be displayed. If the Purchaser clicks the **[Return without payment]** button, the browser will be redirected to the Merchant's website to the page address specified for the **URL_RETURN_NO** variable, which corresponds to the unsuccessful transaction.



uniteller

self @ online & onlife

4 Main operations procedure

4.1 Authorization request

4.1.1 General sequence

General sequence of the authorization request is shown on the image 1 below:

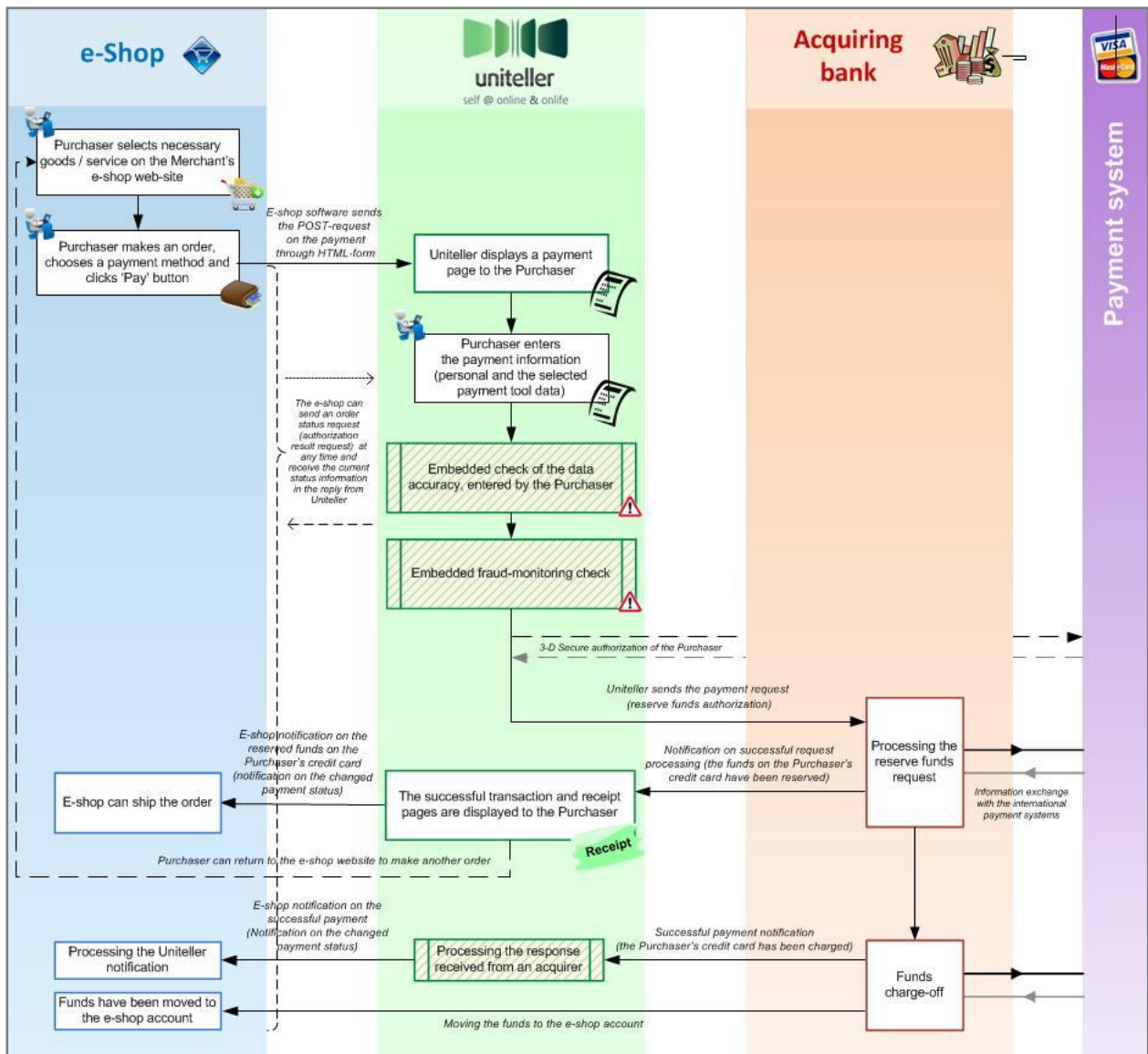


Image 1 - General sequence of the authorization request

Authorization request has the following stages:

1. Authorization request in the Uniteller system is initiated when the field values of the HTML-form with the required payment parameters are received from the Merchant's e-shop website. This form can be placed, for example, on a "Basket" page and the information it contains is sent when the Purchaser clicks [Pay] button on the form on the Merchant's e-shop website. The template sample of the HTML-form is given in Section 4.1.2 "Payment form on the Merchant's e-shop website and its parameters", page 13.

2. There are the following payment methods:

- Credit cards of the international payment systems (VISA, MasterCard, Diners Club, JCB, AMEX)
- Electronic payment systems (EasyPay, Moneybookers, MoneyMail, PayPal, Platezh.ru, QIWI Wallet, RBK Money, WebCredits, WebMoney WMR, Yota.money, VKontakte, Money@Mail.Ru, Euroset, Beeline Mobile payment, Megafon Mobile payment, MTS Mobile payment, PlatFon, Yandex.Money)

Payment method can be either preliminary specified by the Merchant by fixing the transferred value of the **MeanType** and **EMoneyType** parameters sent from the form (see Section 4.1.4 “Payment page on the Uniteller website depending on the transferred values of the MeanType and EMoneyType parameters”, page 18) or, if not specified by the Merchant, is chosen by the Purchaser in the process of payment.

3. As a result of sending the above given parameters of the form, a payment page will be displayed to the Purchaser. The look of the page will depend on either a payment method has been preliminary selected or only needs to be selected (see Section 4.1.4 “Payment page on the Uniteller website depending on the transferred values of the MeanType and EMoneyType parameters”, page 18), and also on a selected payment page template and its settings (see Section 4.1.3 “Payment page display methods. Payment page integration into the e-shop website”, page 17). If the payment method was not preliminary selected, the Purchaser will see the page he should select a payment method on, otherwise, the page with the selected payment method will be displayed.

4. On the page with the chosen payment method, the Purchaser must enter the data required for the payment (for example, credit card data) and click **[Pay]**. After it, an order and a credit card or electronic currency operation are created in the Uniteller system (for the payment via credit card or electronic currency, correspondingly).

5. The Uniteller system executes a range of tests to check the accuracy of the entered data and prevent any fraud, and also, in case of payment with 3-D Secure authorization, the Purchaser passes the 3-D Secure authorization on the server of the payment system.

6. If Uniteller internal check and 3-D Secure authorization are successful, the Uniteller system sends the authorization request on reserve the funds to the bank-acquirer.

7. The bank-acquirer executes its own check of the data sent in the payment request and, if the result is successful, reserves the funds on the required amount on the Purchaser’s account and notifies Uniteller about the finished authorization of the funds reservation (see Section 4.6.3 ‘The e-shop server notification about the payment status’, page 47)

8. The Uniteller system displays the page with the success payment message to the Purchaser and also the receipt page with the main information of the payment (the list of the obligatory receipt fields is given below).

At the same time the Uniteller system sends the reserved funds notification for the paid order to the e-shop website. Basing on this notification the e-shop can ship the goods under the order.

9. Basing on the authorization request on hold on the funds, sent to the bank-acquirer, Uniteller continues the payment processing until the payment amount is transferred in the e-shop account from the Purchaser’s account. When the charge-off from the Purchaser’s account is successful, the bank-acquirer sends the corresponding notification to the Uniteller system and Uniteller system, in its turn, notifies the e-shop (see Section 4.6.3 ‘The e-shop server notification about the payment status’, page 47)

Depending on the chosen method, the payment will be performed on one of the following schemes:

- **in the background mode** – the Purchaser stays on the Uniteller website and enters, if necessary, required additional information. In case of a successful payment, a payment result or a receipt page is displayed (see Section 4.1.5 “Payment in the background mode” Section, page 22)

- **through the external form** – the Purchaser is redirected to a website of the chosen payment system to continue the payment operation without Uniteller involved (see Section 4.1.6 “Payment through external form” Section, page 25). Along with it, the Uniteller system tracks the payment status.

If the payment was done via an electronic payment system, an invoice is displayed to the Purchaser to be paid on.

The Purchaser can return from the payment page to the e-shop website by clicking the **[Back to e-shop]** button. The Purchaser will be redirected to the address specified for the **URL_RETURN_OK** parameter (if this parameter is set) or **URL_RETURN** parameter (if only this parameter is set) with the **GET**-parameter of the **Order_ID** which is equal to **Order_IDP**. If the **GET**-parameter of the **Order_ID** already exists in the URL-address, its value will be changed.

Example:

```
URL_RETURN_OK = http://example.com/pay/ok/?param1=value1&param2=value2
```

When the transaction is done, the redirection will happen to:

```
http://example.com/pay/ok/?param1=value1&param2=value2&Order_ID=1234
```

In any case, the page code of the Merchant’s website must send the request, specified in the Section 4.6 “Authorization results verification”, page 45, to the **wpay.uniteller.ru** server, using **Order_ID** and make sure that the transaction with this **Order_ID** really exists and has correct status and amount. In case of an error, the Purchaser’s browser will be redirected to another (or the same) page on the Merchant’s website which must inform the Purchaser about the failed (unsuccessful) transaction.

If the redirection to the page with the successful payment results on the Merchant’s website does not happen (for example, for the reason of a browser session error on the Purchaser’s side), it is recommended to:

- Use the notification mechanism described in the Section 4.6.3 “e-Shop server notification about the transaction status”, page 47, or
- Check the transaction status (Section 4.6 “Authorization results verification”, page 44) with any Purchaser’s activity on the website, in case when a transaction is not verified by the corresponding redirection to the successful transaction page (**URL_RETURN_OK**), unsuccessful transaction page (**URL_RETURN_NO**) or transaction verification page (**URL_RETURN**).

In case of a successful transaction, the Merchant must e-mail an electronic copy of the receipt to the Cardholder. The receipt must contain the following data:

- Merchant’s business name ("Doing business as" name)
- e-Shop name in Latin assigned by Uniteller (this name is given to a Merchant together with **MERCHANT_ID**).
- E-Shop URL
- Company contact e-mail and phone
- Transaction amount in the currency, fixed by Uniteller in the agreement
- Transaction date
- Unique transaction ID
- Cardholder Name
- Verification code

- Operation type (sale)
- Goods/service name
- Refund/return conditions, if determined
- Expiry date of the demo period (if any)

Card number **MUST NOT** to be specified on the receipt.

The required parameters and conditions to execute a transaction, together with individual processing cases, are given further.

4.1.2 Payment form on the Merchant's e-shop website and its parameters

On the page of the e-shop website the payment is done on, the Merchant must place an HTML-form which identifies parameters of the forthcoming payment.

The HTML-form must transfer the following obligatory (see Table 1, page 13) and optional (see Table 2, page 15) parameters to <https://wpay.uniteller.ru/pay/>.



Table 1 - Obligatory payment page parameters on the Merchant's website

No	Parameter	Description
1	Shop_IDP	The e-shop identifier in the Uniteller system. (Due to the made changes to the Uniteller system, the e-shop identifier was renamed to Uniteller Point ID in the Back-office.) This identifier is visible to the Merchant in his/her Back-office in "e-Shops" menu item, Uniteller Point ID column on the 'Merchant's e-shops'.
2	Order_IDP	An order number in the e-shop account system which corresponds to the transaction. The order number can be of any not empty string up to 127 symbols long and cannot contain blanks only.
3	Subtotal_P	The purchase amount in the currency, specified in the Agreement with the Bank-acquirer. A dot is used as a decimal delimiter. For example, 12.34.
4	Signature	The signature that ensures transaction critical data invariability (amounts, Order_IDP) (see Section 7.5 "Payment page signing", page 65) Signature is calculated using the following algorithm: <pre>Signature = uppercase(md5(md5(Shop_IDP) + & + md5(Order_IDP) + & + md5(Subtotal_P) + & + md5(MeanType) + & + md5(EMoneyType) + & + md5(Lifetime) + & + md5(Customer_IDP) + & + md5(Card_IDP) + & + md5(IData) + & + md5(PT_Code) + & + md5(password)))</pre> where: <ul style="list-style-type: none"> • password – password from "Authorization results" Section on the Uniteller system Back-office. • '+' – text lines concatenation operation (all lines are converted to bytes in ASCII encoding). • '&' – 'field delimiter' symbol. If optional parameter is not sent in the

№	Parameter	Description
		<p>form, '&' symbol which corresponds this field (following it) is saved in the string to calculate the Signature.</p> <ul style="list-style-type: none"> • md5 –cryptographic hash-function (lower case symbols). • uppercase – uppercase function • MeanType – payment system of the credit card. If MeanType is not sent in the form, it should be received as an empty string (md5 value of the empty string — d41d8cd98f00b204e9800998ecf8427e – is placed into the calculation formula) • EMoneyType – electronic currency type. If EMoneyType is not sent in the form, it should be received as an empty string (md5 value of the empty string — d41d8cd98f00b204e9800998ecf8427e – is placed into the calculation formula) • Lifetime - payment form lifetime in seconds. If Lifetime is not sent in the form, it should be received as an empty string (md5 value of the empty string — d41d8cd98f00b204e9800998ecf8427e – is placed into the calculation formula) • Customer_IDP – Purchaser identifier, used by some e-shops. If Customer_IDP is not sent in the form, it should be received as an empty string (md5 value of the empty string - d41d8cd98f00b204e9800998ecf8427e – is placed into the calculation formula) • Card_IDP – an identifier of the registered card. If Card_IDP is not sent in the form, it should be received as an empty string (md5 value of the empty string — d41d8cd98f00b204e9800998ecf8427e – is placed into the calculation formula) • IData – «long record». If IData is not sent in the form, it should be received as an empty string (md5 value of the empty string — d41d8cd98f00b204e9800998ecf8427e – is placed into the calculation formula) • PT_Code – payment type. If PT_Code is not sent in the form, it should be received as an empty string (md5 value of the empty string — d41d8cd98f00b204e9800998ecf8427e – is placed into the calculation formula)
5	Parameter URL_RETURN or two parameters: URL_RETURN_OK , URL_RETURN_NO (see below).	These parameters are described in Table 2, page 15.



Table 2 - Optional payment page parameters on the Merchant's website

No	Parameter	Description
1	Lifetime	The form (page) lifetime in seconds, starting from the moment it was displayed. It should be in the form of integer positive number. If the Purchaser stays on the page longer than it is determined, the form will be considered stale and payment will not be accepted. In this case, the Purchaser will be offered to return to the Merchant's website for reordering.
2	Customer_IDP (64 symbols)	The Purchaser's identifier used by some e-shops.
3	Card_IDP (up to 128 symbols)	The identifier of the registered card.
4	PT-Code	The payment type. A random line up to ten symbols long. This parameter is not used in most activation schemes for e-shops.
5	MeanType	The credit card payment system. Values: 0 – any, 1 – Visa, 2 – MasterCard, 3 – Diners Club, 4 – LCB, 5 – AMEX (is not supported at the moment).
6	EMoneyType	The type of electronic currency type. Possible values of electronic currency type are provided in Table 3, page 16.
7	BillLifetime	The lifetime of an order payment in the payment system in hours (from 1 to 1080 hours). The value of BillLifetime parameter is applied only for QIWI-payments. If BillLifetime is not sent, the QIWI-payment life time for an order to be paid is set by default – 72 hours.
8	Preauth	The indicator of a payment preauthorization. Can take on value "1".
9	URL_RETURN (up to 255 symbols)	Page URL the Purchaser must be returned to when a transaction is performed in the Uniteller system.
10	URL_RETURN_OK (up to 255 symbols)	Page URL the Purchaser must be returned to in case of successful transaction in the Uniteller system. If this parameter is determined, it overlays URL_RETURN parameter.
11	URL_RETURN_NO (up to 255 symbols)	Page URL the Purchaser should be returned to in case of unsuccessful transaction in the Uniteller system. If this parameter is determined, it overlays URL_RETURN parameter.
12	Language (2 symbols)	The interface language code of the payment page. Can be 'eng' or 'ru'.
13	Comment (up to 1024 symbols)	Payment comments
14	FirstName (64 symbols)	First name
15	LastName (64 symbols)	Last name
16	MiddleName (64 symbols)	Middle name
17	Email	E-mail

№	Parameter	Description
	(64 symbols)	
18	Phone (64 symbols)	Phone
19	Address (128 symbols)	Address
20	Country (3 symbols)	Purchaser's country
21	State (3 symbols)	State/region code
22	City (64 символа)	City
23	Zip (64 symbols)	Zip

Email, Phone, Address, City parameters, sent in the request to the payment page from the Merchant's website, are substituted in the corresponding fields on the payment page automatically, but, nevertheless, the Purchaser is able to change them.

Table 3 - Possible values of the EMoneyType parameter

Parameter value	Description
0	Any system of electronic payments
1	Yandex.Money
2	RBK Money
3	MoneyMail
4	WebCreds
5	EasyPay
6	Platezh.ru
7	Money@Mail.Ru
8	Megafon Mobile payment
9	MTS Mobile payment
10	Beeline Mobile payment
11	PayPal
12	VKontacte
13	Euroset
14	Yota.money
15	QIWI Wallet
16	PlatFon



Parameter value	Description
17	Moneybookers
29	WebMoney WMR

HTML-form can be placed, for example, on a “Basket” page. Character encoding on the page, the HTML form is placed on, and the fields content he same as the fields content should be **UTF-8**.

HTML-form template:

```
<FORM ACTION="https://wpay.uniteller.ru/pay/" METHOD="POST">
<INPUT TYPE="HIDDEN" NAME="Shop_IDP" VALUE="Your Shop_ID">
<INPUT TYPE="HIDDEN" NAME="Order_IDP" VALUE="Your Order_ID">
<INPUT TYPE="HIDDEN" NAME="Subtotal_P" VALUE="Payment amount">
<INPUT TYPE="HIDDEN" NAME="Lifetime" VALUE="Form lifetime">
<INPUT TYPE="HIDDEN" NAME="Customer_IDP" VALUE="Visitor's identifier">
<INPUT TYPE="HIDDEN" NAME="Card_IDP" VALUE="Registered card identifier">
<INPUT TYPE="HIDDEN" NAME="Signature" VALUE="Payment signature">
<INPUT TYPE="SUBMIT" NAME="Submit" VALUE="Pay">
<INPUT TYPE="HIDDEN" NAME="URL_RETURN_OK" VALUE="http://example.com/pay/ok/">
<INPUT TYPE="HIDDEN" NAME="URL_RETURN_NO" VALUE="http://example.com/pay/fail/">
<INPUT TYPE="HIDDEN" NAME="MeanType" VALUE="0">
<INPUT TYPE="HIDDEN" NAME="EMoneyType" VALUE="0">
</FORM>
```

4.1.3 Payment page display methods. Payment page integration into the Merchant's e-shop website

The Uniteller system supports three methods to display the payment page:

- on the Uniteller website at <https://wpay.uniteller.ru/pay/> (“Standard” page template)
- on the Merchant's e-shop website via iframe element (“For iframe” template)
- on a mobile device, if the e-shop website is optimized for mobile devices (“For mobile devices” template).

The procedure of selection the method to display the payment page and setup the corresponding template is performed in the Uniteller Back-office in the settings for the particular e-shop (see “The Uniteller payment system Back-office. Merchant's employee guide”).

If it is necessary to display the payment form directly on the e-shop website via iframe element, for the integration the following steps should be performed:

1. Connect the jQuery library (the library is necessary to use the **animate()** function) to the page the payment form via iframe will be placed on, as described at: <http://api.jquery.com/animate/>.

Connection line, sample:

```
<script src="http://ajax.googleapis.com/ajax/libs/jquery/1.7.1/jquery.min.js"
type="text/javascript"></script>
```

2. Add the following code to the page with iframe:

```
<script type="text/javascript">
function listener(event) {
    if ( event.origin !== 'https://wpay.uniteller.ru' ) {
        return;
    }
}
```

```

    $('#pay_iframe').animate({height: event.data + 'px'}, 500);
  }
  if (window.addEventListener) {
    window.addEventListener('message', listener, false);
  } else {
    window.attachEvent('onmessage', listener);
  }
}
</script>

```

where:

pay_iframe — is id of the iframe element; **500** — standard size for a bank 3-D Secure page (500x500 pixels).

3. Add the following code into the necessary place of the page code, the iframe is placed on:

```

<iframe width="630" height="332" name="pay_iframe" id="pay_iframe"
src="https://wpay.uniteller.ru/pay/"></iframe>
<script type="text/javascript">
  if ($.browser.msie && Number($.browser.version) < 9) {
    $('#pay_iframe').width(630 + 4);
    $('#pay_iframe').height(332 + 22);
  }
  if ($.browser.webkit) { // Chrome adds an indent before body.
    $('#pay_iframe').height(332 + 10);
  }
</script>

```

where:

pay_iframe — is id of the iframe element; **630** — iframe width; **332** — iframe height (these values can be changed to others according to the page design).


4.1.4 Payment page on the Uniteller website according to the sent values of the MeanType and EMoneyType parameters

When the Purchaser clicks **[Pay]** button on the payment page of the Merchant's website, the Purchaser will be redirected to one of the pages on the Uniteller website, according to the sent values of the **MeanType** and **EMoneyType** parameters.

The Purchaser can be redirected to one of the following pages on the Uniteller website:

- **Payment method page** (see Image 2, page 19) — the page with the list of the supported payment systems for credit card payment or supported electronic currencies to be chosen. If **MeanType** or **EMoneyType** parameter, which corresponds to a definite credit card / electronic currency type, is sent to the Uniteller server, it will be impossible to choose this payment method on the page.
- **Credit card payment page** (see Image 3, page 19) — the page with the list of the supported payment systems for credit card payment. If **MeanType** parameter, which corresponds to a definite credit card type, is sent to the Uniteller server, the type selection will not be available.
- **Electronic system payment page** (see image 4, page 20) — the page for the payment via electronic payment system, which corresponds to the sent **EMoneyType** parameter.
- **Error page** — see Table 5, page 22.

Payment page




Order payment to: www.testshop.ru


Order ID: 2012-01-26-14493


Order Amount: **301.35 RUB**


Comments on the payment: Comments


Select the payment method

































Enter the payment data using "Credit Card"

Card Number (from 12 to 19 digits)

Expiry Date (MM/YY)

 /

Cardholder's Name



[Back without payment](#)

Pay

Security Warranty

In the Uniteller system, the transactions as well as the information you have entered are secured by the SSL protocol and other special tools. Your personal information is stored only on our secured servers and in no way will not be disclosed to any third party, except the cases stipulated by the law.

Should you have any questions, please, contact Uniteller technical support: +7 495 987 19 60 or support@uniteller.ru











Image 2 — Payment method page

Payment page



Order payment to: www.testshop.ru

Order ID: 2012-01-26-14493

Order Amount: **301.35 RUB**

Comments on the payment: Comments


Enter the payment data using "Credit Card"

Card Number (from 12 to 19 digits)

Expiry Date (MM/YY)

 /

Cardholder's Name



[Back without payment](#)

Pay

Security Warranty

In the Uniteller system, the transactions as well as the information you have entered are secured by the SSL protocol and other special tools. Your personal information is stored only on our secured servers and in no way will not be disclosed to any third party, except the cases stipulated by the law.

Should you have any questions, please, contact Uniteller technical support: +7 495 987 19 60 or support@uniteller.ru













Image 3 — Credit card payment page, sample

Payment page

 Order payment to: www.testshop.ru
 Order ID: 2012-01-26-14493
 Order Amount: 301.35 RUB
 Comments on the payment: Comments





 **MOБИЛЬНЫЙ ПЛАТЕЖ** Enter the payment data using "Mobile payment Megafon" 

For invoicing fill the fields and press "Pay" button

Mobile phone number

Mobile phone number, which will be billed.
 Number indicated in the ten-digit format. For example, 9123456780.

[Back without payment](#) **Pay**

Security Warranty    

In the Uniteller system, the transactions as well as the information you have entered are secured by the SSL protocol and other special tools. Your personal information is stored only on our secured servers and in no way will not be disclosed to any third party, except the cases stipulated by the law.

Should you have any questions, please, contact Uniteller technical support: +7 495 987 19 60 or support@uniteller.ru

Image 4 —Electronic currency payment page, sample

If the following conditions are met, the Purchaser will be redirected to one of the pages on the Uniteller website specified in the Table 4 below:

- Internet-acquiring service agreement is signed between the Merchant and Uniteller company and is registered in the Uniteller system;
- Electronic currencies service agreement is signed between the Merchant and Uniteller company and is registered in the Uniteller system with “Active” status;
- The conditions of the Electronic currencies service agreement allow servicing the e-shop with the required **Shop_IDP**.

Table 4 — Dependence of the page on the Uniteller website, the Purchaser is redirected to from the payment page on the Merchant’s website, according to the value of the MeanType and EMoneyType parameters

#	The value of MeanType parameter (N — an integer value in the permissible range)	The value of EMoneyType parameter (N — an integer value in the permissible range)	Page on the Uniteller website
1	Not sent	Not sent	Payment method page (see Image 2, page 19).
2	0	Not sent	Credit card payment page (see Image 3, page 19).
3	N	Not sent	Credit card payment page (see Image 3, page 19).
4	Nor sent	0	Payment method page without credit card types (see Image 2, page 19).
5	Not sent	N	Payment method in the corresponding electronic payment system (see Image 4, page 20).
6	0	0	Payment method page (see Image 2, page 19).
7	N	0	Payment method page (see Image 2, page 19).

#	The value of MeanType parameter (N — an integer value in the permissible range)	The value of EMoneyType parameter (N — an integer value in the permissible range)	Page on the Uniteller website
8	0	N	Payment method page (see Image 2, page 19) with the ability to choose only credit cards or an electronic payment system specified.
9	N	N	Payment method page (see Image 2, page 19) with the ability to choose only credit cards or an electronic payment system specified.

If the **MeanType** parameter is sent and one of the following conditions is met (electronic currency payments are not allowed to the e-shop):

- Electronic currencies service Agreement between the Merchant and Uniteller company is not registered in the Uniteller system or the registered one does not have “Active” status, if any;
- Electronic currencies service Agreement between the Merchant and Uniteller company is registered in the Uniteller system and has “Active” status, but it is not allowed to service the e-shop with the sent **Shop_IDP** identifier or the electronic currency payments are not allowed for the sent **EMoneyType** parameter;

the Purchaser will be redirected to the credit card payment page (see Image 3, page 19).

If an integration error occurs while downloading the payment page (for example, the Merchant has sent parameters with errors), the “**Payment page download error**” page (see Image 5, page 21) will be displayed.

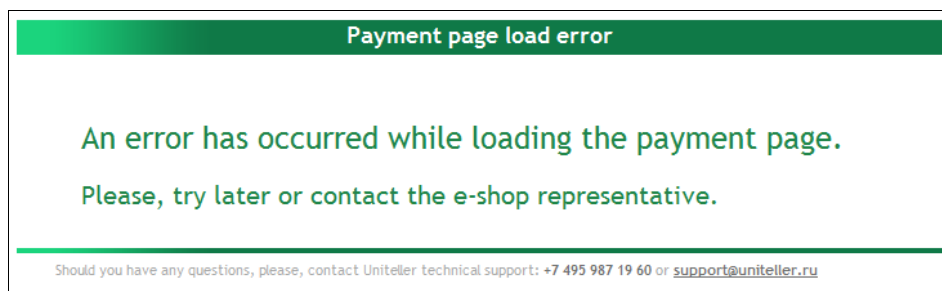


Image 5 — “Payment page download error” page

To read the error text (for example, to examine the integration issue while the test connection) it is necessary to open the source code of the “**Payment page download error**” page and read the error description in HTML-comment right after `<body>` tag.

For Example:

```
...
<body>
<!-- MERCHANT ERROR: Signature is not valid -->
<div id="page">
  <div id="header">Payment page download error</div>
...

```

Error message will be displayed in the situations specified in Table 5 below.

Table 5 — Possible error messages specified by the sent values of MeanType and EMoneyType parameters

#	Condition	The value of MeanType parameter	The value of EMoneyType (N — an integer value in the permissible range)	Error message
1	Electronic currencies service agreement does not have “Active” status in the Uniteller system or the conditions of the agreement with “Active” status do not allow servicing the e-shop with the required Shop_IDP	Not sent	Not sent	“Unfortunately, you cannot pay this order. There is a restriction on the e-shop. “
2	The conditions of the active Electronic currencies service agreement in the Uniteller system do not allow servicing the required electronic currency (EMoneyType=N).	Not sent	N	“Unfortunately, you cannot pay this order. There is a restriction on the e-shop. “

4.1.5 Payment in the background mode

A range of the payment methods (for example, credit card payment, mobile phone payment (MTS, Beeline, Megafon, Euroset, QIWI) execute payment in the so called background mode, it means that the Purchaser is not redirected from the Uniteller website to the website of a payment system to make the payment, but enters all necessary information and gets the transaction result page directly on the Uniteller website.

In general the payment in the background mode has the following sequence:


1. The Purchaser chooses a payment method on the Uniteller website (see Image 2, page 19), which is executed in the background mode, or a parameter which defines the corresponding payment method is sent from the Merchant’s payment form.
2. The Purchaser is redirected to the payment page according to the payment method chosen (see Image 3 and Image 4, page 20) and enters, if necessary, the required information to make the payment.
3. If the provided information was successfully verified, the payment will be sent to be processed. If the provided information is not correct, the corresponding error message will be displayed to the Purchaser.
4. If the transaction (payment) is sent successfully, the following actions are performed:
 - In case of a credit card payment, the funds on the order amount are reserved on the credit card (**Subtotal_P** parameter) - authorized transaction. The order and the credit card operation are created in the Uniteller system with the “Successful authorization” status.
 - Transaction result page for the credit card payment contains the following information (see Image 6, page 24), which will be also sent to the specified Purchaser’s e-mail:
 - Order number — a number sent to the payment page in **Order_IDP** parameter.

- Transaction amount.
- Purchaser — Cardholder’s name entered on the payment page by the Purchaser.
- Card number — masked card number (only four last digits are shown and the rest are replaced with stars).
- Authorization code — a number of the processing that identifies the transaction in a bank-acquirer.
- Transaction date — transaction date and time.
- For “Mobile phone payment” payment (MTS, Beeline, Megafon) SMS-message with the notification of the submitted invoice will be sent on the Purchaser’s mobile phone.
- In case of electronic currency payment, an order and electronic currency operation with “Pending payment” status are created in the Uniteller system and the invoice result page is displayed to the Purchaser (see Image 7, page 24).

For Euroset payment, the payment result page will contain such information as “**Payment recipient**” (“MoneyOnline”) and “**Payment number in Euroset**” the Purchaser will be able to pay the order in Euroset shop at (see Image 8, page 24).

5. In case of a transaction error, the corresponding error page will be displayed to the Purchaser:

Payment page



uniteller

Order payment to: www.testshop.ru

Order ID: 2012-01-26-25197

Order Amount: **301.35 RUB**

Comments on the payment: [Comments](#)

You Credit Card payment has been successful.

Please, save the payment information below for your reference

[Back to e-shop](#)

Transaction ID:
2012-01-26-25197

Amount:
301.35 RUB

Purchaser:
Ivan Ivanov

Credit card number:
440505*****0000

Authorization code:
9DB882

2012-01-26 14:30:48

Security Warranty

In the Uniteller system, the transactions as well as the information you have entered are secured by the SSL protocol and other special tools. Your personal information is stored only on our secured servers and in no way will not be disclosed to any third party, except the cases stipulated by the law.

Should you have any questions, please, contact Uniteller technical support: +7 495 987 19 60 or support@uniteller.ru











Image 6 — Credit card payment result page

Payment page







Order payment to:	www.testshop.ru
Order ID:	2012-01-26-61874
Order Amount:	311.13 RUB
Comments on the payment:	Comments

Invoice to e-commerce company
Магазин Emoney [www.testshop.ru]
has been successfully created.

[Back to e-shop](#)

Amount:
311.13 RUB

2012-01-26 15:57:11


Security Warranty





In the Uniteller system, the transactions as well as the information you have entered are secured by the SSL protocol and other special tools. Your personal information is stored only on our secured servers and in no way will not be disclosed to any third party, except the cases stipulated by the law.

Should you have any questions, please, contact Uniteller technical support: +7 495 987 19 60 or support@uniteller.ru

Image 7 — The result page with the submitted invoice to be paid via electronic currency, sample

Payment page



Order payment to:	www.testshop.ru
Order ID:	2012-01-26-97295
Order Amount:	312.13 RUB
Comments on the payment:	Comments

Invoice to e-commerce company
Магазин Emoney [www.testshop.ru]
has been successfully created.

Please, save the payment information below for
your reference





[Back to e-shop](#)

Amount:
312.13 RUB

Payee:
ДеньгиOnline

Transaction Number:
45909583

2012-01-26 15:58:20

Security Warranty





In the Uniteller system, the transactions as well as the information you have entered are secured by the SSL protocol and other special tools. Your personal information is stored only on our secured servers and in no way will not be disclosed to any third party, except the cases stipulated by the law.

Should you have any questions, please, contact Uniteller technical support: +7 495 987 19 60 or support@uniteller.ru

Image 8 — The result page with the submitted invoice for “Euroset” payment

4.1.6 Payment via external form

For the payment with the following payment methods: Yandex.Money, RBK Money, MoneyMail, WebCredits, EasyPay, Platesh.ru, Money@Mail.Ru, PayPal, VKontakte, Yota.money, WebMoney WMR, the payment is performed via the external form of the chosen electronic payment system with the Purchaser redirected to the website of this payment system.

In general, the payment via external form has the following sequence:

1. The Purchaser chooses a payment method on the Uniteller website (see Image 2, page 19) which is performed via the external form, or a parameter which defines the corresponding payment method is sent from the Merchant's payment form.
2. The Purchaser is redirected to the electronic currency payment page (see Image 4, page 20) and enters, if necessary, the required information to make the payment.
3. If the provided information is successfully verified, or additional information is not required, the Purchaser will be redirected to the website of the corresponding electronic payment system. At the same time, an order and electronic currency operation with "Pending payment" status are created in the Uniteller system.

If the provided information is not correct, the corresponding error message will be displayed to the Purchaser.

4. On the website of the electronic payment system the Purchaser makes the payment following the given instructions. There are several peculiarities:
 - Different payment systems provide different payment variants - on-line invoice payment and time periods for the invoice issuing and its payment.
 - Amount of the information about the initial Purchaser's order in the Merchant's e-shop, which is displayed on the payment page of the payment system, varies according to the page design and payment process of the corresponding payment system.
 - Not all payment systems provide the ability (button, link, etc.) to return to the Merchant's e-shop the initial order was done at from their payment pages.

4.2 Payment preauthorization

4.2.1 General

The Uniteller payment system provides the ability to perform the payments with preauthorization.

Preauthorization – is the possibility to reserve the required funds on the Purchaser's credit card without sending the settlement to a payment system.

The period of the funds reservation for the payments with preauthorization is set by an acquiring bank and can be changed upon agreement with it. When this period is over, the Acquirer automatically cancels the funds reservation, without any notification sent to the Merchant and Uniteller.

For the Acquirer to charge-off the required amount from the Purchaser's credit card and move it to the Merchant's account, the Merchant must send the payment confirmation command for each preauthorization (see Section 4.2.3 "Verification of the payment with preauthorization", page 26).

The Merchant can cancel the payment preauthorization at any time or make a refund for the finished transaction via "Refund" command.

4.2.2 Payment preauthorization process

For any shop and generated order, the Merchant is able to set the following options:

- **Perform the payment in a standard mode** (successful transaction from the Purchaser, nothing more is required), or
- **Payment with preauthorization** (the payment is processed only when additional verification is sent on the operation)

For the payment preauthorization, the Merchant must send the "Preauth" optional parameter. If this parameter is sent and has value "1", it is considered that the current preauthorization requires additional confirmation before the payment complete command is sent. For the Purchaser, the payment process has the same sequence, as it is described in Section 4.1 Authorization request, page 10.

Also, to obtain the authorization results, the Merchant's software can contact definite addresses on the WPay server.

If the "URL address for the e-shop notification" parameter is set for the Merchant's e-shop, HTTP POST request is sent to this address with the following parameters:

- **Order_ID**—Order ID
- **Signature**— digital signature (uppercase(md5(Order_ID + Status + password)))
- **Status** — status (authorized, paid, cancelled)
Status 'authorized' is sent in case of successful preauthorization, 'paid' – is sent in case of successful **Complete** command (when the corresponding information is received from a bank-acquirer), 'canceled' – is sent when the preauthorization is successfully cancelled or the "Refund" command is successfully sent.

4.2.3 Verification of the payment with preauthorization

To send the verification for the earlier made preauthorization, the **POST** or **GET** request with the parameters specified in Tables 6 and 7 below must be sent to <https://wpay.uniteller.ru/confirm/>. The Response will contain the values specified in the **S_FIELDS** parameter (see Section 7.1 "Possible fields of S_FIELDS parameter", page 50).

The response format will depend on the **Format** parameter sent:

- 1 - response in CSV format (";" is used as a delimiter)
- 2 – response in WDDX format
- 3 - response in XML format

If the **Format** parameter is not specified, the response will be in CSV format.

Table 6 - Obligatory parameters of the verification request for the payment with preauthorization

No	Parameter	Type	Description
1	Billnumber	12 digits	The transaction number in the Uniteller system.
2	Shop_ID	String up to 64 symbols	The e-shop ID in the Uniteller system. This ID is visible to the Merchant on the Back-office in the "e-Shops" menu item, Uniteller Point_ID column.

No	Parameter	Type	Description
3	Login	String up to 64 symbols	The login assigned to the Merchant during the account creation in the Uniteller system.
4	Password	80 symbols	The password assigned to the Merchant during the account creation in the Uniteller system.

Table 7 - Optional parameters of the verification request for the payment with preauthorization

No	Parameter	Type	Default value	Description
1	Subtotal_P	Amount		The changed amount of the transaction. This amount must not exceed the initial payment amount and is transferred only in case of necessity to change the payment amount.
2	Currency	3-symbols	Authorization currency code	The currency code. Only the authorization currency code can be used.
3	Language	2 symbols	'ru'	Result language
4	Format	1 (CSV), 2 (WDDX), 3 (XML)	1	The result format. In format 1 the fields are delimited with semicolon.
5	S_FIELDS		* (all fields)	<p>Headlines and names of the displayed fields.</p> <p>Form: Fird1;Fields2;...;FeldK, where Field1 is a fields name of the available ones (see below); or FieldName1=Field1; FieldName2=Field2;...; FieldNameK=FieldK, where FieldName1 is a headline to be used, for example, in CSV for the column with the value of the Field1.</p> <p>Fields sequence in S_FIELDS determines the fields sequence in the result.</p> <p>If S_FIELDS is not determined, the result will contain all fields.</p> <p>(Section 7.1 "Possible fields of S_FIELDS parameter", page 50)</p>

If any error occurs, two parameters will be returned: **firstcode** and **secondcode**. The values of these parameters are given in Table 8, page 28.

Table 8 - Possible error types during the verification request of the payment with preauthorization

Code (firstcode)	Message (secondcode)	Description
1	Authentication error	Wrong authorization data (Login, Password)
3	Mandatory parameter '%fieldName%' is not present in the request	Obligatory parameter is not specified (%fieldName% - parameter name)
4	Bill not found	Transaction is not found
5	Field %fieldName% has bad format	Wrong value format or the value is not acceptable (%fieldname% - parameter name)
10	S_FIELDS contains field '%name%' which is not allowed	S_FIELDS field contains the parameter which is not supported. %name% - parameter code
15	The operation failed	Something went wrong and the operation has been interrupted. Please, try next time.
18	Authorization reversal is not allowed	Verification is not possible.

Sending the verification request does not result the immediate sending of the command to complete the order payment. The commands to complete the payment are sent automatically for the preauthorizations verified by the Merchant before the end of the operational day (at 8:30 pm).

If during the specified preauthorization period the Merchant's software does not send any verification for the orders waiting to be verified, such preauthorizations will be cancelled (no additional actions are required) and the earlier funds reservations for such orders will be returned to the Purchasers' accounts.

If the Merchant's software sends an order verification request and the response is successful, any further verification request under this order will return an error code and its description.

If the Merchant's software sends an order verification request and it returns an error and its description, the Merchant must analyze the error description and make necessary corrections to the verification request to get the successful response.

If the Merchant's software sends a verification request for a stale (cancelled) order and the response is successful, the attempt to send the payment complete command for such order will result in a response from a Bank-acquirer with an error.

4.3 Recurring payments

4.3.1 General

The Uniteller payment system allows performing the recurring payments.

Recurring payments mean the payments executed without a Cardholder (in automatic mode), but upon his/her earlier agreement to it and as to the agreed schedule (including dates of some definite events).

Examples of the recurring payments:

- Monthly charge for Internet services;
- Definite amount charge-off basing on the invoice for mobile phone services during a month (in case of credit payment conditions);

- Automatic payment of the specified amount to the account of a mobile phone, if the balance is lower than specified;
- Definite amount charge-off basing on the conditions specified. For example, if a balance in an on-line game account is 10 rub., the payment will be 1000 rub., and if 50 rub. – 500 rub.

4.3.2 Recurring payments peculiarities and principles of their arrangement in the Uniteller system

Recurring payments have the following peculiarities:

- Recurring payment is initialized without a Cardholder's participation, so it is impossible to obtain the CVV2 (CVC2) code of the credit card.
- Recurring payment execution requires the data of its "parent" transaction executed by a Cardholder. This "parent" transaction is the "template" for other recurring payments of the same kind.
- Recurring payment does not differ from a single payment by a credit card. Its peculiarity is in that some part of the data, required for its execution, is not entered by the Purchaser but is taken from a "parent" payment.
- Taking in to account that the recurring payment is executed without a Cardholder, it is impossible to provide 3D-Secure support to this transaction (but "parent" transaction can be executed with 3D-Secure support). The Merchant is responsible for all risks in this case.

When executing the recurring payments, Uniteller adheres the following principles:

- The Merchant works with the Purchaser (Cardholder). Uniteller works with the Merchant.
- The Merchant is responsible for all necessary legal agreements and procedures with the Purchaser as regards to the recurring payments, and also for arrangement and support of the recurring payments schedule.

Note: to activate the recurring payments, the Merchant must obligatory obtain the Cardholder's certain agreement to it. This agreement can be made in different ways – confirmation of the charge-off rules on the Merchant's website by clicking [OK] button or with a check mark, etc. Signed printed agreement is not required. The frequency of the charge is set either by the Cardholder by him/herself or by the Merchant, to avoid any misunderstandings. It is recommended keeping this information to avoid any possible claims.

- To activate the mechanism of the recurring payments, the Merchant must sign the corresponding supplementary agreement with an acquiring bank.
- In the process of the recurring payments execution, Uniteller is responsible for the payment requests processing received from the Merchant. All payment requests received from the Merchant are considered by Uniteller as legal and meet the Purchaser and Merchant's demands.
- Recurring payment amount can differ from the amount of its "parent" transaction.
- Any recurring payment can become a "parent" transaction for the future recurring payments of the same kind.
- Only Uniteller employees have the right to activate the support of the recurring payments for the Merchant's e-shop.
- The period between the recurring payments cannot be longer than 180 days.

4.3.3 Recurring payments execution

To enable the recurring payment, it is necessary to send POST or GET request to <https://wpay.uniteller.ru/recurrent/> with the parameters specified in Table 9 below.

Table 9 - Obligatory parameters of the request to execute the recurring payment

No	Parameters	Description
1	Shop_IDP	The e-shop identifier in the Uniteller system. Due to the made changes in the Uniteller system the e-shop identifier was renamed to Uniteller Point ID in the Back-office. This identifier is visible to the Merchant in his/her Back-office in “e-Shops” menu item, Uniteller Point ID column on the ‘ Merchant’s e-shops ’ page.
2	Order_IDP	The order number in the e-shop settlement system, which corresponds to the transaction. It can be of any not empty string up to 127 symbols long and cannot contain blanks only.
3	Subtotal_P	The purchase amount in the currency, specified in the Agreement with an Acquirer. A dot is used as a decimal delimiter. For example, 12.34.
4	Parent_Order_IDP	The “parent” transaction number (Order_IDP) in the e-shop settlement system. It can be of any not empty string up to 127 symbols long and cannot contain blanks only.
5	Signature	<p>The signature which ensures transaction critical data invariability (amounts, Order_IDP) (see Section 7.5 ‘Payment page signing’, page 64).</p> <p>Signature is calculated using the following algorithm:</p> <pre>Signature = uppercase(md5(md5(Shop_IDP) + & + md5(Order_IDP) + & + md5(Subtotal_P) + & + md5(Parent_Order_IDP) + & + md5(password)))</pre> <p>where:</p> <ul style="list-style-type: none"> • password – password from the “Authorization results” Section on the Uniteller system Back-office • '+' – text lines concatenation operation (all lines are converted to bytes in ASCII encoding) • '&' – ‘fields delimiter’ symbol • md5 – cryptographic hash-function • uppercase – uppercase function

The response will be sent in CSV format (“;” as a delimiter).

The response format is similar to the payment cancellation response, but contains **Signature** parameter value.

The response format to the recurring payment request is specified in Section 7.3.3 “Recurring payment request”, page 62.

If any error occurs, two parameters will be returned: **firstcode** and **secondcode**. The values for these parameters are given in Table 10 below.

Table 10 - Possible error messages for the request to execute the recurring payment

Code (firstcode)	Message (secondcode)	Description
2	Invalid signature	The request contains invalid signature
3	Mandatory parameter '%fieldName%' is not present in the request	Obligatory parameter is not specified (%fieldName% - parameter name)
5	Field %fieldName% has bad format	Wrong value format or the value is not available (%fieldname% - parameter name)
15	The operation failed	Something went wrong and the operation has been interrupted. Please, try next time.
22	Recurrent payment not allowed	Recurring payment function is not supported by this e-shop.
23	Incorrect Parent_Order_IDP	There is no link to the "parent" transaction or refers to unsuccessful transaction.
24	Order_IDP already exists	Such Order_IDP already exists.
25	Shop_IDP not found	Shop_IDP is not found.

4.4 Credit cards registration for the repeated payments

4.4.1 General information about the credit cards registration

To simplify the credit card payment process for the e-shop customers, the Uniteller system provides the ability of the credit cards registration, saving only the main data to be used for the repeated payments with these cards.

To pay with a credit card which had been earlier registered in the Uniteller payment system, the Purchaser must not enter all credit card data in the payment form, it is necessary to enter CVV2/CVC2 code only and, in some cases, pass 3-D Secure authorization. The Purchaser can have several registered credit cards and select the one the order will be paid with directly on the Uniteller payment page or the e-shop website.

It is at the e-shop discretion to use the mechanism of the credit cards registration during the payment process in the e-shop.

4.4.2 The necessity of the credit cards registration and general binding procedures

There are various scenarios for the e-shop to use credit cards binding procedure. The most popular are:

- Saving the credit card information (except CVV2/CVC2 code) after the first payment on condition that the Purchaser agrees to it. For the further payments in this e-shop the Purchaser will be able to select the registered credit card in the list and not enter full credit card information.
- Binding the credit card is also used to reduce the number of fraudulent operations of the illegal credit card use. The credit card binding process is separated from the further payments. The e-shop can set the option to pay only with the registered cards and the Purchaser selects the registered credit card on the e-shop website.
- The credit cards issued by a bank are bound to the specified e-shop automatically (without e-shop and Purchaser's participation) and are connected to the corresponding Purchasers' identifiers in the e-shop. This variant is used, for example, for co-branding cards between the bank and the e-shop that allows the Cardholders, being the customers of the e-shop, to obtain the simplified payment procedure using these cards in the e-shop at once.

There are two basic procedures of the credit cards binding:

- **The binding with the successful payment** – the credit card is registered, if, during the usual payment process when the full credit card data are entered, the Purchaser confirms the intention to save the credit card data and selects the **“Save the credit card data”** check box, and the transaction is successful (see section 4.4.4.2 “First credit card payment after authorization in the e-shop”, page 33).
- **The binding with the random amount** – the credit card is registered, if after the random amount authorization the Purchaser confirms it correctly (see Section 4.4.4.5 “The registration of the credit card with the random amount”, page 35).

4.4.3 Security and division of responsibility

4.4.3.1 Credit card data, “mask” and its statuses

The registered card means the main credit card data (except CVV2/CVC2 code) stored in the Uniteller processing center. The credit card data are never sent neither to e-shop nor the Purchaser (through the payment form or otherwise).

Each registered credit card belongs to a definite registered e-shop customer. Several credit cards can be registered for one customer. The same credit card can be registered for several customers of the same or different e-shops.

Each registered credit card has a unique **Card_IDP** identifier, ‘mask’ and status.

The credit card ‘mask’ is used for the e-shop visitor to see the registered credit cards for him/her and at the same time not to show the credit card data, according to the security requirements. The card ‘mask’ contains the information of the credit card type (VISA, MasterCard, JCB, Diners Club) and four last digits of the card number. The ‘mask’ is visible to the Purchaser and can be transferred to the e-shop.

There are three statuses for the credit card:

- **«Not verified»** — the Purchaser had started the credit card registration procedure, but has not confirmed it with the specified random amount yet.
- **«Active»** — the payment can be done with the registered credit card with ‘Active’ status only.

- «**Blocked**» — the active credit card is blocked to temporary prevent payments with it.

4.4.3.2 Customer_IDP - the Purchaser's unique identifier

The e-shop must assign a unique **Customer_IDP** identifier to each of the registered customers. Such identifier can be the customer's name in the e-shop system (phone, e-mail, etc.). The Uniteller processing center recognizes a Purchaser basing on the **Customer_IDP** parameter transferred from the e-shop when the Purchaser is redirected to the payment page. The e-shop must prevent the **Customer_IDP** parameter to be used not by the Purchaser it was assigned to. The e-shop is responsible for the correct authentication and customers' authorization.

The payment with the credit card, which data are stored in the processing center, is possible only when the card CVV2/CVC2 code is specified correctly. If the credit card supports 3-D Secure authorization, the Purchaser must pass this authorization each time paying with this credit card.

4.4.4 Routine usage scenarios

4.4.4.1 Credit card payment without authorization in the e-shop

The steps for the credit card payment without authorization in the e-shop are the following:

1. If the Purchaser has not passed the authorization on the e-shop website (also in case when the Purchaser passed the authorization, but the e-shop has not sent his/her **Customer_IDP** identifier to the Uniteller website), he/she is redirected to the standard credit card payment page on the Uniteller website where it is necessary to specify full credit card information.
2. The Purchaser enters the required credit card information the payment is done with.
3. If the specified credit card information is correct, the payment is processed and the credit card data are not saved.
4. For further payments the Purchaser will have to enter the credit card information again.

4.4.4.2 First payment with the credit card after the authorization in the e-shop

The steps for the first credit card payment after the authorization in the e-shop are the following:

1. The Purchaser passes the authorization on the e-shop website, and the e-shop assigns him/her the corresponding unique **Customer_IDP** identifier.
2. When the e-shop sends the order payment page request for this Purchaser, the Purchaser's **Customer_IDP** identifier must be sent together with other parameters.
3. When the Purchaser is redirected to the credit card payment page on the Uniteller website, the processing center identifies that neither credit card is registered for this Purchaser.
4. The standard credit card payment page the full credit card information must be entered on is displayed to the Purchaser.
5. Also the standard credit card payment page contains the "**Save credit card information**" check box and the text that informs the Purchaser the meaning of this field and also the confidentiality warranty information. By default, the check-box is not selected.
6. If the Purchaser does not select the check box for the "**Save credit card information**" field, further behavior of the payment page and the processing center will be the same as it is described in the Section 4.4.4.1 "Credit card payment without authorization in the e-shop", page 33.
7. If the check mark is selected and the transaction is successful, the credit card will be registered

for this Purchaser in this e-shop in the processing center. An unique **Card_IDP** identifier is assigned to the credit card data and the corresponding displaying 'mask' is created. The 'Active' status is assigned to the credit card.

8. No additional information about the fact of the credit card registration for the Purchaser is sent to the e-shop.

4.4.4.3 Further payments with the registered credit card

The steps for the further payments with the registered credit card are the following:

1. The Purchaser (visitor) passes the authorization on the e-shop website and the e-shop assigns him/her the corresponding unique **Customer_IDP** identifier.
2. When the e-shop sends the order payment page request for this Purchaser, the Purchaser's **Customer_IDP** identifier must be sent together with other parameters.
3. When the Purchaser is redirected to the credit card payment page on the Uniteller website, the processing center identifies that a credit card is registered for this Purchaser.
4. The simplified payment form is displayed to the Purchaser on the credit card payment page with the corresponding information text and the list of the credit cards to pay with.
5. The list of the credit cards contains the 'mask' of the registered credit card and "**Pay with another credit card**" menu item.
6. The Purchaser is offered the following options: pay the order with the specified credit card, pay the order with another credit card, or delete the credit card registration (delete the data of the registered credit card).
7. If the first option is selected, the Purchaser enters CVV2/CVC2 code of the credit card on the payment page and, if necessary, passes 3-D Secure authorization.
8. If the second option is selected, the Purchaser is redirected to the standard payment page and enters all information of a new credit card. If the data of the new credit card fully correspond the data of the registered credit card, the new credit card will not be registered. If the "**Save credit card information**" check-box is selected, the status of the credit card will be changed to "Active" and if the check box is not selected, the status will not be changed correspondingly.
9. If the third option is selected, the processing center deletes the connection of the registered credit card with the Purchaser. The Purchaser is redirected to the standard credit card payment page the full credit card information must be entered on. See also Section 4.4.4.7 "Deleting the credit card registration", page 37.

4.4.4.4 Selecting the registered credit card on the Uniteller web-site during the payment process

The steps of the credit card selection from the list of the registered cards on the Uniteller website are the following:

1. The Purchaser (visitor) passes the authorization on the e-shop website, and the e-shop assigns him/her the corresponding unique **Customer_IDP** identifier.
2. When the e-shop sends the order payment page request for this Purchaser, the Purchaser's **Customer_IDP** identifier must be sent together with other parameters.
3. When the Purchaser is redirected to the credit card payment page on the Uniteller website, the processing center identifies that several credit cards are registered for this Purchaser.
4. The simplified payment form is displayed to the Purchaser on the credit card payment page with

the corresponding information text and the list of the credit cards to pay with.

5. The list of the credit cards contains the 'masks' of all active credit cards registered for this Purchaser in the e-shop and "Pay with another credit card" menu item.
6. The Purchaser can select any credit card for the payment in the list or select "Pay with another credit card" menu item.
7. In the first case, the Purchaser enters CVV2/CVC2 code of the credit card on the payment page and, if necessary, passes 3-D Secure authorization.
8. In the second case, the Purchaser is redirected to the standard payment page and enters full information of a new credit card. If the data of the new credit card fully correspond the data of any registered credit card, the new credit card will not be registered. If the "Save credit card information" check box is selected, the status of the credit card will be changed to "Active" and if the check box and not selected, the status will not be changed correspondingly.
9. The Purchaser is also able to delete any credit card in the list of the registered one (see Section 4.4.4.7 "Deleing the credit card registration", page 37).
10. If the Purchaser deletes the last registered credit card, he/she will be automatically redirected to the standard payment page and further credit card payment process will be performed according to the scenario described in the Section 4.4.4.2 "First credit card payment after the authorization in the e-shop", page 33. The Purchaser is also able to register a new credit card.

4.4.4.5 The registration of the credit card with a random amount

To provide the ability to register credit cards with a random amount, the e-shop must add the corresponding application form onto its website which redirects to the credit card registration page. The application form template is provided below:

The HTML-template sample of the form which redirects to the registration page of the credit cards with the random amount:

```
<FORM ACTION="https://wpay.uniteller.ru/pay/" METHOD="POST">
<INPUT TYPE="HIDDEN" NAME="Shop_IDP" VALUE="Your Shop_ID">
<INPUT TYPE="HIDDEN" NAME="Order_IDP" VALUE="Your Order_ID">
<INPUT TYPE="HIDDEN" NAME="Lifetime" VALUE="The form lifetime">
<INPUT TYPE="HIDDEN" NAME="Customer_IDP" VALUE="Customer's identifier">
<INPUT TYPE="HIDDEN" NAME="Signature" VALUE="Form signature">
<INPUT TYPE="SUBMIT" NAME="Submit" VALUE="Register">
<INPUT TYPE="HIDDEN" NAME="Card_Registration" VALUE="1">
<INPUT TYPE="HIDDEN" NAME="URL_RETURN_OK" VALUE="http://example.com/pay/ok/">
<INPUT TYPE="HIDDEN" NAME="URL_RETURN_NO" VALUE="http://example.com/pay/fail/">
</FORM>
```

where:

- **Shop_IDP** — the e-shop identifier. This identifier is visible to the Merchant on his/her Back-office in "e-Shops" menu item, **Uniteller Point_ID** column on the "Merchant's e-shops" page.
- **Order_IDP** — an order number in the e-shop settlement system or any unique identifier, using which the e-shop will send an order authorization request in the future. It can be of any string up to 127 symbols long.
Lifetime — the form lifetime in seconds, starting from the moment it was displayed. It must be in the form of integer positive number. If the Purchaser works with the form longer than it is determined, the form will be considered stale and payment will not be accepted. In this case the Purchaser will be offered to return to the Merchant's website for reordering.
- **Customer_IDP** — the Purchaser's unique identifier.

- **Card_Registration** — the identifier of display the credit card registration form with the random amount. To display the form, the identifier must be equal to '1'. If this identifier does not present or has other value, the credit card payment form will be displayed on the Uniteller website.
- **Signature** — the signature that ensures the form critical data invariability. Signature is calculated using the following algorithm:

```
Signature = uppercase(md5(md5(Shop_IDP) + & + md5(Order_IDP) + & + md5(Lifetime) + & + md5(Customer_IDP) + & + md5(password)))
```

where:

- **password** – password from “**Authorization results**” Section on the Uniteller system Back-office.
- '+' – text lines concatenation operation (all lines are converted to bytes in ASCII encoding).
- '&' – 'fields delimiter' symbol. If optional parameter is not sent in the form, the '&' symbol which corresponds to this field (following it) is saved in the string to calculate the **Signature**.
- **md5** – cryptographic hash-function (lower case symbols)
- **uppercase** – uppercase function
- **Lifetime** - the form lifetime in seconds. If **Lifetime** is not sent in the form, it must be received as an empty string (md5 value of the empty string — d41d8cd98f00b204e9800998ecf8427e – is placed into the calculation formula).

The main steps for the registration of the credit card with the random amount are the following:

1. The Purchaser (visitor) passes the authorization on the e-shop website, and the e-shop assigns him/her the corresponding unique **Customer_IDP** identifier.
2. On the e-shop website the Purchaser is offered to register his/her credit card with a random amount. If the Purchaser accepts this offer, the form which redirects to the registration page of a credit card with random amount is generated on the e-shop website. The form contains **Shop_IDP** – the e-shop identifier, **Customer_IDP** – the Purchaser's identifier and **Card_Registration='1'** parameter (see the form sample above). The request that includes the form parameters is sent to Uniteller website.
3. On the Uniteller website the credit card registration page, the full credit card information must be entered on, is displayed to the Purchaser. The payment amount is generated automatically from 0,01 to 9.99 rubles, regardless of the value sent in the form. The payment is always processed with the **Preauth** status (payment with preauthorization, see Section 4.2 «Payment preauthorization **Ошибка! Источник ссылки не найден.**», page 25). Unlike on the payment page, on the registration page the payment amount is not displayed to the Purchaser and is not sent via e-mail. The registration page also contains the corresponding information text.
4. If the payment attempt is successful the credit card is registered in the processing center to this Purchaser and this e-shop. An unique **Card_IDP** identifier is assigned to the credit card data and the corresponding displaying 'mask' is created. The “Not verified” status is assigned to the credit card.
5. In the result of the successful payment attempt, to register a credit card, the generated random amount is reserved on the Purchaser's credit card. The Purchaser must him/herself check the random amount reserved on the credit card through the tools provided by the issuing bank (SMS-message, Back-office on the bank website, the support service call, etc.). The corresponding information page is displayed to the Purchaser.
6. The e-shop is not reported of any additional information about the fact of the credit card registration for this Purchaser, but the status of the payment attempt (see Section 4.2.2 “Payment preauthorization process”, page 26).

7. If the payment attempt is successful, the e-shop can obtain the information about the financial operation that includes the payment amount (**Subtotal_P**) and the value of the **Card_IDP** parameter – the identifier of the registered credit card, by sending the “Authorization results verification” request (see Section 4.6 “Authorization results verification”, page 44). The **Card_IDP** field is present only for the successful registration operations with the random amount.
8. To confirm the credit card registration, the Purchaser must enter the reserved amount on the credit card on the e-shop website. The e-shop verifies the accuracy of the entered amount for the corresponding credit card itself and also limits the number of attempts (the recommended limit is 5 attempts maximum).
9. If the Purchaser successfully passes the verification, the e-shop must send the request to change the credit card status from “Not verified” to “Active” (see Section 4.4.4.10 “Changing the status of the registered credit card”, page 38).
10. If the verification for the Purchaser failed (the attempts limit or time is over), the e-shop must send the request to delete the credit card registration (see Section 4.4.4.10 “Changing the status of the registered credit card”, page 38).
11. Once the credit card registration is verified or not by the Purchaser or when the time limit is over (the recommended limit is 6 hours maximum), the e-shop must cancel the payment (see Section 4.5 “Payment cancellation and refund”, page 41 and Section 4.5.2 “Cancellation of the payment with preauthorization”, page 43).

4.4.4.6 Selecting the registered credit card on the e-shop website during the payment process

The steps of the credit card selection from the list of the registered cards on the e-shop website are the following:

1. The Purchaser (visitor) passes the authorization on the e-shop website, and the e-shop assigns him/her the corresponding unique **Customer_IDP** identifier.
2. The list of the registered active credit cards is displayed to the Purchaser where he/she must select the credit card to pay with. The credit cards are displayed in the form of ‘masks’. On the payment page for this Purchaser the e-shop must specify **Shop_IDP** – the e-shop identifier, **Customer_IDP** – the Purchaser’s identifier and **Card_IDP** – the card identifier, selected by the Purchaser.
3. When the Purchaser is redirected to the Uniteller website, the simplified payment form, the ‘mask’ of the selected credit card and the corresponding information are displayed to the Purchaser on credit card payment page.
4. On the payment page the Purchaser enters CVV2/CVC2 code of the credit card and, if necessary, passes 3-D Secure authorization.

4.4.4.7 Deleting the credit card registration

When the Purchaser selects the option to delete the earlier registered credit card, the e-shop must send the corresponding request to Uniteller with the specified **Card_IDP** for the credit card which registration needs to be deleted (see 4.4.4.10 “Changing the status of the registered credit card”, page 38). The result of the operation can be successful or failed.

4.4.4.8 Blocking the registered credit card

When the Purchaser selects the option to block the earlier registered credit card, the e-shop must send the corresponding request to Uniteller with the specified **Card_IDP** for the credit card which needs to be

blocked (see 4.4.4.10 “Changing the status of the registered credit card”, page 38). If the operation is successful the credit card status will be changed to “Blocked”. Only one active credit card can be blocked.

4.4.4.9 Unblocking the registered credit card

When the Purchaser selects the option to unblock the earlier registered credit card, the e-shop must send the corresponding request to Uniteller with the specified **Card_IDP** for the credit card which needs to be unblocked (see 4.4.4.10 “Changing the status of the registered credit card”, page 38). If the operation is successful the credit card status will be changed to “Active”.

4.4.4.10 Changing the status of the registered credit card

To cancel the credit card registration or change its status (verify, block, unblock) the e-shop must send **POST** or **GET** request to <https://wpay.uniteller.ru/card/> with the parameters specified in Tables 11 and 12 below.

Table 11 — Obligatory parameters of the request to change the status of the registered credit card

No	Parameter	Type	Description
1	Shop_IDP	String up to 64 symbols	The e-shop identifier in the Uniteller system.
2	Login	String up to 64 symbols	Login assigned to the Merchant during the account creation in the Uniteller system.
3	Password	80 symbols	Password assigned to the Merchant during the account creation in the Uniteller system.
4	Card_IDP	String up to 128 symbols	The registered credit card identifier.
5	Customer_IDP	Can be of any line maximum 64 digits long	The Purchaser’s identifier used by some e-shops.
6	Action	Possible values: 1 – confirm registration; 2 – delete registration; 3 – block the credit card; 4 – block the credit card.	The operation assigned to the credit card.

Table 12 — Optional parameters of the request to change the status of the the registered credit card

No	Parameter	Type	Default meaning	Description
1	Format	Possible values: 1 (CSV); 2 (WDDX); 3 (XML).	1	The result format. The fields in format 1 are delimited with semicolon.

The response will contain the fields specified in Table 13.

Table 13 — The fields of the response to the request of changing the registered credit card status

No	Field	Type	Value
1	ErrorCode	Number (integer, non-negative)	0 – is case of success or an error number
2	ErrorMessage	String	Error description

If any error occurs, two parameters will be returned: **firstcode** and **secondcode**. The values of these parameters are given in Table 14, page 39.

Table 14 – Possible error messages for the request of changing the registered credit card status

Code (firstcode)	Message (secondcode)	Description
1	Authentication error	Wrong authorization data (Login, Password).
3	Mandatory parameter '%fieldName%' is not present in the request	Obligatory parameter is not specified (%fieldName% — parameter name).
5	Field %fieldName% has bad format	Wrong value format or the value is not acceptable. (%fieldname% - parameter name)
15	The operation failed	Something went wrong and the operation has been interrupted. Please, try next time.
30	Card not found	The credit card is not found.
31	Card can't be activated because it's blocked	The credit card cannot be activated as it is blocked.
32	Card can't be blocked because it's not confirmed	The credit card cannot be blocked as it is not verified.
33	Card can't be unblocked because it's not confirmed	The credit card cannot be unblocked as it is not verified.
34	TempCard not found	The credit card with such TempCard_IDP data (for the Shop_IDP specified) is not found

4.4.4.11 Obtaining the list of the registered credit cards

To obtain the list of the registered credit cards for the definite Purchaser (specified **Customer_IDP**), the e-shop must send the corresponding request to the Uniteller website, the response to which will contain the list of the registered cards (**Card_IDP**) with the 'mask' for each card (credit card type and masked number), issuing bank name (there can be names in English and errors due to symbols encoding) and the credit card status.

To obtain the list of the registered credit cards, it is necessary to send **POST** or **GET** request to <https://wpay.uniteller.ru/card/> with the parameters specified in Tables 15 and 16 below.

Table 15 — Obligatory parameters of the request to obtain the list of the registered credit cards

No	Parameter	Type	Description
1	Shop_IDP	String up to 64 symbols	The e-shop identifier in the Uniteller system.
2	Login	String up to 64 symbols	Login assigned to the Merchant during the account creation in the Uniteller system.
3	Password	80 symbols	Password assigned to the Merchant during the account creation in the Uniteller system.
4	Customer_IDP	Can be of any line maximum 64 digits long	The Purchaser's identifier used by some e-shops.

Table 16 — Optional parameters of the request to obtain the list of the registered credit cards

No	Parameter	Type	Default meaning	Description
1	Format	Possible values: 1 (CSV); 2 (WDDX); 3 (XML).	1	The result format. The fields in format 1 are delimited with semicolon.

If the request is successful, the record with 5 fields, specified in the Table 17 below, will be returned for each credit card.

Table 17 — The fields of the response on the request to obtain the registered credit cards list, if successful

No	Field	Type	Description
1	Card_IDP	String up to 128 symbols	The identifier of the registered credit card.
2	CardType	String	Credit card type (Visa, MasterCard, DinnersClub, JCB).
3	CardNumber	String of 4 symbols	Four last PAN symbols.
4	CardStatus	Number (integer, non-negative)	The card status: (0 — not verified, 1 — active, 2 — blocked).
5	BankName	String	Issuing bank name.

If any error occurs, the response will contain the fields specified in Table 18 below.

Table 18 — The fields of the response on the request to obtain the registered credit cards list, if failed

No	Field	Type	Description
1	ErrorCode	Number (integer, non-negative)	Error number.
2	ErrorMessage	String	Error message description.

Possible error messages corresponds the ones specified in the Table 14, page 39.

4.5 Payment cancellation and refund

4.5.1 Payment cancellation request and possible response formats

To cancel the executed transaction, it is necessary to send **POST** or **GET** request to <https://wpay.uniteller.ru/unblock/> with the parameters specified in Tables 19 and 20 below.

For such acquirers as TransCreditBank, Bank of Moscow and UCS² the partial payment cancellation is supported - the cancellations on the amount which is less the initial transaction amount (or the initial amount with the already made cancellations (current balance)). For all other acquirers only full payment amount cancellations are supported.

For the TransCreditBank and UCS acquirers multiple cancellations for one initial payment are supported, for other acquirers only one cancellation is allowed.

For AK BARS Bank acquirer the cancellation for the last payment is supported only.

The response to this request will contain the values listed in **S_FIELDS** parameter (see Section 7.1 "Possible fields of S_FIELDS parameter", page 50).

Response format will depend on the **Format** parameter sent:

- 1 – Response in CSV format. Semicolon ";" is used as a delimiter.
- 2 – Response in WDDX format.
- 3 – Response in XML format.
- 4 – Response in SOAP format

If the **Format** parameter is not determined, the response will be in CSV format.

Table 19 - Obligatory parameters of the payment cancellation request

No	Parameter	Type	Description
1	Bill number	12 digits	The payment number in the Uniteller system.
2	Shop_ID	String up to 64 symbols	The e-shop identifier in the Uniteller system. This identifier is visible to the Merchant on its Back-office in "e-Shops" menu item, Uniteller Point_ID column.
3	Login	String up to 64 symbols	Login assigned to the Merchant during the account creation in the Uniteller system.
4	Password	80 symbols	Password assigned to the Merchant during the account creation in the Uniteller system.

² For the moment of the current Integration manual release, there is an error for the UCS acquirer in the status of the payment purpose for partial cancellation process till the operation when the funds are charged from an account — a transaction has the «Successful charge-off» instead of «Successful authorization» status. A transaction can keep this wrong status from one hour to one day. The real status of the transaction is visible on the «Detailed transaction information» page of the Uniteller Back office — if the «Requests to the processing center» section contains some notes of the funds charge operations, the funds have been charged. This status error will be corrected in the nearest versions of the system. Should you have any questions, please, contact Uniteller Technical support.

Table 20 - Optional parameters of the payment cancellation request

No	Parameter	Type	Default value	Description
1	Subtotal_P	Amount	Authorization amount	The refund amount. The refund amount must be in the range from 0,01 rubles to the payment amount inclusive. A dot is used as a decimal delimiter.
2	Currency	3-symbols	Authorization currency code	Cancellation or refund currency code. Only authorization currency code can be used.
3	RVR Reason	1 (operation cancellation by e-shop), 2 (operation cancellation by the Cardholder), 3 (fraud operation)	1	The reason of the operation cancellation.
4	Language	2 symbols	'u	Result language.
5	Format	1 (CSV), 2 (WDDX), 3 (XML) 4 (SOAP)	1	Result form. The fields in the format 1 are delimited with semicolon.
	S_FIELDS		* (all fields)	Headlines and names of the fields displayed. Form: Fird1;Fields2;...;FeldK, where Field1 is a fields name of the available ones (see below); or FieldName1=Field1; FieldName2=Field2;...; FieldNameK=FieldK, where FieldName1 is a headline to be used, for example, in CSV for the column with the value of Field1. Fields sequence in S_FIELDS determines the fields sequence is the result. If S_FIELDS is not determined, the result will contain all fields. (see Section 7.1 "Possible fields of S_FIELDS parameter", page 50)

If any error occurs, two parameters will be returned: **firstcode** and **secondcode**. The values of these parameters are given in Table 21 below.

Table 21 - Possible error messages of the payment cancellation request

Code (firstcode)	Message (secondcode)	Description
1	Authentication error	Wrong authorization data (Login, Password).
3	Mandatory parameter '%fieldName%' is not present in the request	Obligatory parameter is not specified (%fieldName% - parameter name).
4	Bill not found	Transaction is not found.
5	Field %fieldName% has bad format	Wrong value format or the value is specified as available. (%fieldname% - parameter name)
10	S_FIELDS contains field '%name%' which is not allowed	S_FIELDS contains the parameter which is not supported. (%name% - parameter code)
15	The operation failed	Something went wrong and the operation has been interrupted. Please, try next time.
16	The order has been already cancelled	Transaction has been cancelled earlier.
17	Authorization reversal is not allowed	Cancellation is not possible.
35	Partial return is not supported	Partial refund is not supported.

4.5.2 Cancellation of the payment with preauthorization

The Merchant can cancel an order at any time using the “Cancel the payment” operation (on the Back-Office or send the request to the definite URL). If the Merchant cancels the operation with the sent verification but without the payment complete command sent, this operation will be cancelled and the payment complete command will not be sent. If the Merchant cancels the operation the payment complete command had been sent for, the refund command will be applied.

4.5.3 Refund

In case of necessity to return the definite amount to the Cardholder, the Uniteller system allows performing the “Refund” operation. The refund operation is executed only to the definite payment operation.

The “Refund” operation must be performed by the Merchant’s authorized employee with the authorized access to the Back-office and being informed of all security points as regards to any operations with the Cardholder’s data.

For the transactions processed by the TansCreditBank, Bank of Moscow and UCS acquirers the partial refund is available (the refund of the amount which is less the initial transaction amount). For all other acquirers full refund is possible only (the refund amount must equal the transaction amount).

For the TransCreditBank and UCS acquirers multiple refunds for one initial payment are supported, for

other acquirers a single refund is allowed only.

For AK BARS Bank acquirer the refund for the last payment is supported only.

The refund operation can be initiated either by sending the request to <https://wpay.uniteller.ru/unblock/> or in the Uniteller system Back-office.

The refund request is the same as the payment cancellation request (see Section 4.5.1 " Payment cancellation request and possible response formats", page 41). If for the moment this request is processed the transaction amount has not been charged, the payment cancellation operation will be started, and if the transaction amount has been charged the refund operation will be initiated.

The "Refund" operation order in the Uniteller system Back-office is described in the Section 5 "Back-office", page 49.

4.6 Authorization results verification

4.6.1 Authorization results request

To obtain the authorization verification result, a request with GET-parameters or POST-parameters, given in the Tables 22 and 23 below, must be sent to <https://wpay.uniteller.ru/results/>. The response format to this request depends on a value of the **Format** parameter sent (see Table 23, page 45).

Possible response formats:

- CSV
- «In brackets»
- WDDX
- XML
- SOAP

The detailed description of the response format is given in Section 7.3 "Response formats", page 52).

Table 22 - Obligatory parameters of the authorization result request

No	Parameter	Description
1	Shop_ID	The e-shop identifier (is assigned upon the Service agreement signing with Uniteller).
2	Login	Login. Login is available for a Merchant at the Back-office, " Authorization parameters " menu.
3	Password	Password. Password is available for a Merchant at the Back-office, " Authorization parameters " menu.

Table 23 - Optional parameters of the authorization results request

#	Parameter	Description	
1	ShopOrderNumber	The order number in the e-shop settlement system. If this parameter is indicated, the response contains authorization result for the specified order. If the operations period (Start... and End... parameters, see below) is not specified in the authorization result request basing on the order number, the response will include all operations history with this order number.	
2	Success (0 – unsuccessful, 1 – successful, 2 – all)	The operations to be included to the response. 2 is set by default.	
3	StartDay	Start... (...Day, ...Month, etc.) and End... parameters determine start/end of the period (inclusive) the transactions will be included into the report for. The limitations for the authorization results request are given in the Section 4.6.2 “Restrictions to the authorization results request”, page 47. If Start... and End... parameters are not specified, the request for the last 24 hours will be performed, by default. If the period for the requested transactions (via Start... and End... parameters) is specified and, at the same time, the order number (ShopOrderNumber) is sent, these two conditions are processed basing on “And” order, so the response will be sent to the operations which correspond to the specified order number and performed within the specified period of time.	
4	StartMonth		
5	StartYear		
6	StartHour		
7	StartMin		
8	EndDay		
9	EndMonth		
10	EndYear		
11	EndHour		
12	EndMin		
13	MeanType (0 - any, 1 – VISA, 2 – MasterCard, 3 – Diners Club, 4 – JCB, 5 – AMEX)		Operations with a kind of a payment method to be included to the report.
14	EMoneyType (see the value at the Table 3, page 14)		Operations with a kind of an electronic payment method to be included to the report.
15	Format (1 – CSV, 2 – WDDX, 3 – «in brackets», 4 – XML, 5 – SOAP)	Result format. Fields in format 1 are separated by a delimiter specified in the Delimiter field (see below). Each field in format 3 is enclosed in delimiters, specified in OpenDelimiter and CloseDelimiter fields (see below). Detailed information for each format is given in Section 7.3 “Response formats”, page 52.	

#	Parameter	Description
16	ZipFlag (0 – browser, 1 – file, 2 – archive)	Result mode. 0 is set by default. In the mode 2 the result is archived into *.zip format.
17	Header (0 – no, 1 - yes)	Whether the request parameters should be added into the response. 0 is set by default
18	Header1 (0 – no, 1 - yes)	Where fields headlines should be added into the response. 0 is set by default
19	Delimiter (';', ':', ' ', '/')	Fields delimiter in CVS-format. If another symbol is indicated, the default ';' symbol will be used.
20	OpenDelimiter ('[', '{', '(')	Opening delimiter of the fields in "in brackets" format. If other symbol is given, the default '[' symbol will be used.
21	CloseDelimiter (']', '}', ')')	Closing delimiter of the fields in "in brackets" format. If other symbol is given, the default ']' symbol will be used.
22	RowDelimiter (',', '10', '13,10', '10,13')	Row delimiter. '13,10' is set by default.
23	S_FIELDS	Headlines and names of the displayed fields. Form: Field1;Fields2;...;FieldK, where Field1 is a field name of the available ones (see below); or FieldName1=Field1; FieldName2=Field2;...; FieldNameK=FieldK, where FieldName1 is a headline to be used, for example, in CSV for the column with the value of Field1. Fields sequence in S_FIELDS determines the fields sequence in the result. If S_FIELDS is not determined, the result will contain all fields specified in Section 7.1 "Possible fields of S_FIELDS parameter, page 50.

The values of the **MeanType** and **EMoneyType** parameters define the data sets in the response to the request (see Table 24 below).

Table 24 – The data sets in the response to the authorization verification request, according to the values of MeanType and EMoneyType parameters

#	The value of MeanType parameter	The value of EMoneyType parameter	Data set
1	Not sent	Not sent	The list of all operations on credit cards and electronic currencies.
2	0	Not sent	The list of all operations on credit cards only.

#	The value of MeanType parameter	The value of EMoneyType parameter	Data set
3	N (an integer identifier)	Not sent	The list of all operations on the specified credit card type.
4	Not sent	0	The list of all operation on electronic currencies only.
5	Not sent	N (an integer identifier)	The list of all operations on the specified type of electronic currency.
6	0	0	The list of all operations on credit cards and electronic currencies.
7	N (an integer identifier)	0	The list of all operations on electronic currencies and the specified credit card type.
	0	N (an integer identifier)	The list of all operations on credit cards and the specified type of electronic currency.
	N (an integer identifier)	N (an integer identifier)	The list of all operations on the specified credit cards type and the type of electronic currency.

4.6.2 Restrictions for the authorization results request

The authorization results request has the following restrictions:

- Request frequency must not exceed 1 request per 5 seconds.
- In the authorization results request with the specified period, operations for which will be included into the report for (**Start...** and **End...** parameters), the duration of the specified period must not exceed 7 days, otherwise the request will not be executed and an error message will be returned.

If the **Start...** and **End...** parameters are not specified, the request for the last 24 hours till the request is received will be performed on default.

4.6.3 e-Shop server notification about the transaction status

In case of a successful transaction with the Purchaser's credit card, the Uniteller system sends notification about the changed order status to '**authorized**' to the Merchant's e-shop server. The notification is also sent in the cases of:

- Performing the transaction of cancellation the funds reservation;
- Performing the operation of the refund on the funds charged;
- Funds charging;
- Order payment in an electronic payment system.

The notification is performed by sending the **HTTP POST** request to the address specified by the Merchant in the Uniteller system Back-office for "**URL notification address**" parameter on "**Edit e-shop**"

page (“Documents and e-shops” menu item). This request contains the parameters specified in Table 25 below.

Table 25 - The parameters of the e-shop server notification request about the transaction status

№	Parameter:	Description:
1	Order_ID	The order number in the e-shop settlement system.
2	Status	<p>The order status.</p> <p>The order status can take the following values:</p> <ul style="list-style-type: none"> • authorized – funds have been successfully reserved (authorization transaction is performed). • paid – paid (financial transaction is performed or the order is paid in an electronic payment system). • cancelled – cancelled (the transaction of the cancellation of the reserved funds is executed or the refund operation is executed for the transaction, the financial transaction had been already done for)
3	Signature	<p>Digital signature which is calculated as to the algorithm:</p> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;"> $\text{Signature} = \text{uppercase}(\text{md5}(\text{Order_ID} + \text{Status} + \text{password})),$ </div> <p>where:</p> <ul style="list-style-type: none"> • password – password from the “Authorization parameters” Section in the Uniteller system Back-office • '+' – operation of text strings catenation (all strings are transformed into bytes in ASCII encoding). • md5 – cryptographic hash-function. • uppercase – uppercase function

If, for some reasons, the notification is not received by the e-shop server (for example, when the notification was sent the server was not available), the Uniteller system will perform additional attempts to send the notification. In general there will be 10 notification attempts (the first failed notification inclusive) sent to the e-shop server for the period of approximately 6,5 minutes or more (real intervals between the e-shop notifications depend on the Uniteller system workload and the size of the operations queue).

If all 10 attempts of sending the notification to the e-shop server about the changed transaction (payment) status are not accepted, there will be no further attempts and the e-shop must send the request for the status of the required transaction itself, as it is described in the Section 4.6.1 “Authorization results request”, page 44.

5 Uniteller Back-office

5.1 Browsing the operations list

The Uniteller Back-office allows Merchant's employees to monitor the credit card transactions and also obtain the general financial statements.

The Uniteller Back Office is a dedicated website with a set of pages and on-line forms which allow the registered and logged in user to obtain general or requested information and also use other system functional according to the rights assigned.

Back-office login details are given to the Merchant during the first e-shop activation.

Authorized access to the Back-office is performed with login and password. The access to any credit card operation data is available only after registration.

Information about the operations is available in the "**Card operations**" menu. When this menu is selected, the "**Card operations**" report page is displayed. The interface of this report page contains an area with the criteria fields (filters) of the request and a table with the results of the executed request, which contains operations information according to the specified criteria.

More details about Back Office are provided in "**The Uniteller payment system Back-office. Merchant's employee guide**".

5.2 Refund operation in the Uniteller Back-office

The refund to a credit card is available for the successful transactions, which were not cancelled.

To perform the refund for a definite transaction it is necessary to click the [**Refund**] button for the required transaction in the row of the table with the request results on the "**Credit card operations**" page of the Back-office. In the result, the operation will change its status, its record in the request result table will change its color and a new message will appear in the "**Operation Description**" column.

More details about the refund are provided in "Uniteller payment system. Merchant's employee guide".

The time of the refund operation is not predetermined and can take several days. In case of a failed automatic **Refund** operation, the Merchant's authorized employee must contact the Uniteller technical support for manual refund.

6 Technical support

General information about Uniteller company is available at the company's official website <http://uniteller.ru/> or over the phone +7 (495) 987-19-60.

Uniteller Technical Support is available round-the-clock over the phone +7 (495) 987-19-60 or e-mail support@uniteller.ru.

In case of any errors and/or inaccuracies found in this document, and also for any improvement offers to this Integration manual, please, contact Uniteller Technical Support.

7 Help information

7.1 Possible fields of S_FIELDS parameters

#	Field:	Description:
1	OderNumber	Order ID in Merchant's e-shop
2	Response_Code	Response code (see below)
3	Recommendation	Response code description
4	Message	Error message (with description, if any)
5	Comment	Payment comment (is sent with the payment request)
6	Date	Payment date and time in dd.mm.yyyy format
7	Total	Total amount paid for one order. A dot is used as a decimal delimiter.
8	Currency	Currency code
9	CardType	Credit card type. Possible values: Visa, MasterCard, Diners Club, JCB
10	CardNumber	PAN last 4 digits
11	LastName	Cardholder's Last name
12	FirstName	Cardholder's First name
13	MiddleName	Cardholder's Middle name
14	Address	Cardholder's address
15	Email	Cardholder's e-mail
16	ApprovalCode	Transaction verification code received from the processing center
17	CVC2	CVC2/CVV2/4DBC availability (0 – authorization without CVC2, 1 – authorization with CVC2)
18	IPAddress	Purchaser's IP-address
19	BillNumber	Payment ID in Uniteller system

#	Field:	Description:
20	BankName	Issuing bank name
21	Status	Order status
22	Error_Code	Response code from the processing center
23	Error_Comment	Description of the response code received from the processing center
24	PacketDate	Request date and time in dd.mm.yyyy hh:mm:ss format
25	PaymentType	"1" - credit card payment; "3" – electronic currency payment
26	EMoneyType	Electronic currency type. Possible values are given in Table 3, page 14.
27	EOrderData	The data for an order submitted in electronic payment system. In "title1=value1, title2=value2, ..." format.
28	Card_IDP	Identifier of the registered credit card
29	PT_Code	Transaction (payment) types

7.2 'Response_code' field value

№	Value:	Comments:
1	AS000	SUCCESSFULAUTHORIZATION
2	AS100	AUTHORIZATION DENIAL
3	AS101	AUTHORIZATION DENIAL. Invalid card number
4	AS102	AUTHORIZATION DENIAL. Not enough funds
5	AS104	AUTHORIZATION DENIAL. Wrong expiration date
6	AS105	AUTHORIZATION DENIAL. Limit is exceeded
7	AS107	AUTHORIZATION DENIAL. Data receive error
8	AS108	AUTHORIZATION DENIAL. Fraud suspicion
9	AS109	AUTHORIZATION DENIAL. The limit for Uniteller operations is exceeded
10	AS200	REPEAT AUTHORIZATION
11	AS998	SYSTEM ERROR. Please, contact Uniteller.



7.3 Response formats

7.3.1 Transaction status request

7.3.1.1. Error message format

If any error occurs, all types, except SOAP, will get the following response:

```
ERROR: <error text>
```

7.3.1.2 CSV

If a response contains **Header=1**, the reply will include:

```
ZipFlag;ShopOrderNumber;Shop_ID;Format;Delimiter;OpenDelimiter;CloseDelimiter;RowDelimit
er;MeanType;StartDate;EndDate;Success;PaymentType;
value ZipFlag;value ShopOrderNumber;valueShop_ID;valueFormat;valueDelimiter;value
OpenDelimiter;value CloseDelimiter;value RowDelimiter;value MeanType;value
StartDate;value EndDate;value Success;value PaymentType;
```

If a response contains **Header1=1**, the reply will include:

```
Fieldname;.....FieldM name;
```

The rows with the specific authorization requests data are given further:

```
Field1 value;.....FieldM value;
```

7.3.1.3. "In brackets"

If a response contains **Header=1**, the reply will include:

```
[ZipFlag][ShopOrderNumber][Shop_ID][Format][Delimiter][OpenDelimiter][CloseDelimiter]
[RowDelimiter][MeanType][StartDate][EndDate][Success][PaymentType]
[ZipFlag value][ShopOrderNumber value][Shop_ID value][Format value][Delimiter
value][OpenDelimiter value][CloseDelimiter value][RowDelimiter value][MeanType
value][StartDate value][EndDate value][Success value][PaymentType value]
```

If a response contains **Header1=1**, the reply will include:

```
[Field1name].....[FieldM name]
```

The rows with the specific authorization requests data are given further:

```
[Field1 value].....[FieldM value]
```

7.3.1.4. WDDX

```

<wddxPacket version='1.0'>
<header></header>
<data>
  <struct>
    <var name='FIELD'>
      <array length='1'>
        <array length='Enter fields amount'>
          <string>Field1 name</string>
          <string>.....</string>
          <string>FieldM name</string>
        </array>
      </array>
    </var>
    <var name='COUNT'><number>Objects number</number></var>
    <var name='FIRSTCODE'><string>First code</string></var>
    <var name='SECONDCODE'><string>Second code</string></var>
    <var name='ORDERS'>
      <array length='Objects amount'>
        <array length='Enter fields amount'>
          <string>Field1 value</string>
          <string>.....</string>
          <string>FieldM value</string>
        </array>
      </array>
    </var>
    <var name='REQUEST'>
      <array length='13'>
        <array length='2'>
          <string>ZipFlag</string>
          <string>ZIPFLAG value</string>
        </array>
        <array length='2'>
          <string>ShopOrderNumber</string>
          <string>SHOPORDERNUMBER value</string>
        </array>
        <array length='2'>
          <string>Shop_ID</string>
          <string>SHOP_ID value</string>
        </array>
        <array length='2'>
          <string>Format</string>
          <string>FORMAT value</string>
        </array>
        <array length='2'>
          <string>Delimiter</string>
          <number>DELIMITER value</number>
        </array>
        <array length='2'>
          <string>OpenDelimiter</string>
          <number>OPENDELIMITER value</number>
        </array>
        <array length='2'>
          <string>CloseDelimiter</string>
          <number>CLOSEDELIMITER value</number>
        </array>
        <array length='2'>
          <string>RowDelimiter</string>
          <string>nROWDELIMITER value</string>
        </array>
      </array>
    </var>
  </struct>
</data>
</wddxPacket>

```



```

        <array length='2'>
            <string>MeanType</string>
            <string>MEANTYPE value</string>
        </array>
        <array length='2'>
            <string>PaymentType</string>
            <string>PAYMENTTYPE value</string>
        </array>
        <array length='2'>
            <string>StartDate</string>
            <string>STARTMONTH/STARTDAY/STARTYEAR value</string>
        </array>
        <array length='2'>
            <string>EndDate</string>
            <string>ENDDAY/ENDDAY/ENDYEAR value</string>
        </array>
        <array length='2'>
            <string>Success</string>
            <string>SUCCESS value</string>
        </array>
    </array>
</var>
</struct>
</data>
</wddxPacket>

```

7.3.1.5 XML

```

<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<unitellerresult firstcode='First code' secondcode='Second code' count='Objects
number'>
<request>
<zipflag>ZIPFLAGvalue</zipflag>
<shopordernumber>SHOPORDERNUMBER value</shopordernumber>
<shop_id>SHOP_IDvalue</shop_id>
<format>FORMATvalue</format>
<delimiter>DELIMITER value</delimiter>
<opendelimiter>OPENDELIMITER value</opendelimiter>
<closeddelimiter>CLOSEDELIMITER value</closeddelimiter>
<rowdelimiter>ROWDELIMITER value</rowdelimiter>
<meantype>MEANTYPE value</meantype>
<paymenttype>PAYMENTTYPE value</paymenttype>
<startdate>STARTMONTH/STARTDAY/STARTYEAR value</startdate>
<enddate>ENDDAY/ENDDAY/ENDYEAR value</enddate>
<success>SUCCES value</success>
</request>
<orders>
<field>
<ordernumber>Field name</ordernumber>
<response_code>Field name</response_code>
<recommendation>Field name</recommendation>
<message>Field name</message>
<comment>Field name</comment>
<date>Field name</date>
<total>Field name</total>
<currency>Field name</currency>
<cardtype>Field name</cardtype>
<cardnumber>Field name</cardnumber>
<lastname>Field name</lastname>
<firstname>Field name</firstname>

```



uniteller

self @ online & onlife

```

<middlename>Field name</middlename>
<address>Field name</address>
<email>Field name</email>
<country>Field name</country>
<rate>Field name</rate>
<approvalcode>Field name</approvalcode>
<cardsubtype>Field name</cardsubtype>
<cvc2>Field name</cvc2>
<cardholder>Field name</cardholder>
<ipaddress>Field name</ipaddress>
<protocoltypename>Field name</protocoltypename>
<billnumber>Field name</billnumber>
<bankname>Field name</bankname>
<status>Field name</status>
<error_code>Field name</error_code>
<error_comment>Field name</error_comment>
<packetdate>Field name</packetdate>
<signature>Field name</signature>
<processingname>Field name</processingname>
<paymenttransactiontype_id>Field name</paymenttransactiontype_id>
</field>
<order>
<ordernumber>Order number</ordernumber>
<response_code>Response code</response_code>
<recommendation>Recomendations</recommendation>
<message>Message</message>
<comment>Comment</comment>
<date>Date</date>
<total>Total</total>
<currency>Currency code</currency>
<cardtype>Card type</cardtype>
<cardnumber>Card number</cardnumber>
<lastname>Last name</lastname>
<firstname>First name</firstname>
<middlename>Middle name</middlename>
<address>Address</address>
<email>E-mail</email>
<country>Issuing bank country code</country>
<rate>Currency rate (0.00)</rate>
<approvalcode>Authorization code</approvalcode>
<cardsubtype>Card subtype</cardsubtype>
<cvc2>Using flag</cvc2>
<cardholder>Cardholder</cardholder>
<ipaddress>Purchaser's IP-address</ipaddress>
<protocoltypename>Protocol type</protocoltypename>
<billnumber>Transaction number</billnumber>
<bankname>Issuing bank name</bankname>
<status>Order status</status>
<error_code>Processing center response code</error_code>
<error_comment>Processing center decryption code</error_comment>
<packetdate>Packet receiving date</packetdate>
<processingname>Processing</processingname>
<paymenttransactiontype_id>Transaction type</paymenttransactiontype_id>
</order>
<order>.....</order>
</orders>
</unitellerresult>

```



uniteller

self @ online & onlife

7.3.1.6. SOAP

WSDL: <https://wpay.uniteller.ru/results/wSDL/>

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<SOAP-ENV:Body SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<ASS-NS:GetPaymentsResultResponse xmlns:ASS-NS="http://www.uniteller.ru/message/">
<return xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xsi:type="SOAP-ENC:Array" xmlns:si="http://www.uniteller.ru/type/"
SOAP-ENC:arrayType="si:SOAPStruct[Objects number]">
<payment xmlns:si=" http://www.uniteller.ru/type/" xsi:type="si:SOAPStruct">
<ordernumber xsi:type="xsd:string">Order number</ordernumber>
<response_code xsi:type="xsd:string">Response code</response_code>
<recommendation xsi:type="xsd:string">Recommendations</recommendation>
<message xsi:type="xsd:string">Message</message>
<comment xsi:type="xsd:string">Comment</comment>
<date xsi:type="xsd:string">Date</date>
<total xsi:type="xsd:string">Totaol</total>
<currency xsi:type="xsd:string">Currency code</currency>
<cardtype xsi:type="xsd:string">Card type</cardtype>
<cardnumber xsi:type="xsd:string">Card number</cardnumber>
<lastname xsi:type="xsd:string">Last name</lastname>
<firstname xsi:type="xsd:string">First name</firstname>
<middlename xsi:type="xsd:string">Middle name</middlename>
<address xsi:type="xsd:string">Address</address>
<email xsi:type="xsd:string">E-mail</email>
<country xsi:type="xsd:string">Issuing bank country code</country>
<rate xsi:type="xsd:string">Currency rate</rate>
<approvalcode xsi:type="xsd:string">Authorization code</approvalcode>
<cardsubtype xsi:type="xsd:string">Card subtype</cardsubtype>
<cvc2 xsi:type="xsd:string">Using flag</cvc2>
<cardholder xsi:type="xsd:string">Cardholder</cardholder>
<ipaddress xsi:type="xsd:string">Purchaser's IP-address</ipaddress>
<protocoltypename xsi:type="xsd:string">Protocol type</protocoltypename>
<billnumber xsi:type="xsd:string">Transaction number</billnumber>
<bankname xsi:type="xsd:string">Issuing bank name</bankname>
<status xsi:type="xsd:string">Order status</status>
<error_code xsi:type="xsd:string">Processing center response code</error_code>
<error_comment xsi:type="xsd:string">Processing center decryption
code</error_comment>
<packetdate xsi:type="xsd:string">Packet receiving date</packetdate>
<signature xsi:type="xsd:string">Electronic signature</signature>
<processingname xsi:type="xsd:string">Processing</processingname>
<paymenttransactiontype_id xsi:type="xsd:string">Тип
транзакции</paymenttransactiontype_id>
</payment>
<payment>.....</payment>
</return>
</ASS-NS:GetPaymentResultResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```



uniteller

self @ online & onlife

In case of an error:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<SOAP-ENV:Body SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<SOAP-ENV:Fault>
<faultcode>First code</faultcode>
<faultstring>Second code</faultstring>
<detail />
</SOAP-ENV:Fault>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

7.3.2 Transaction cancellation request

7.3.2.1 CSV

7.3.2.1.1. Successful result

```
OrderNumber;Response_Code;Recommendation;Message;Comment;Date;Total;Currency;CardType
;CardNumber;LastName;FirstName;MiddleName;Address;Email;ApprovalCode;CVC2;CardHolder;
IPAddress;BillNumber;BankName;Status;Error_Code;Error_Comment;PacketDate;PaymentType;
Phone;
OrderNumber value;Response_Code value;Recommendation value;Message value;Comment
value;Date value;Total value;Currency value;CardType value;CardNumber value;LastName
value;FirstName value;MiddleName value;Address value;Email value;ApprovalCode
value;whether CVC2 is specified;CardHolder value;IPAddress value;BillNumber
value;BankName value;Status value;Error_Code value;Error_Comment value;PacketDate
value;PaymentType value;Phone value;
```

7.3.2.1.2. Error message

```
ErrorCode;ErrorMessage;
Error code;Error message;
```

7.3.2.2 WDDX

7.3.2.2.1. Successful result

```
<?xmlversion="1.0"encoding="utf-8"?>
<wddxPacketversion="1.0">
<header/>
<data>
<struct>
<var name="ordernumber"><string>Ordernumber value</string></var>
<var name="response_code"><string>Response_code value</string></var>
<var name="recommendation"><string>Recommendation value</string></var>
<var name="message"><string>Message value</string></var>
<var name="comment"><string>Comment value</string></var>
<var name="date"><string>Date value</string></var>
<var name="total"><string>Total value</string></var>
<var name="currency"><string>Currency value</string></var>
<var name="cardtype"><string>Cardtype value</string></var>
<var name="cardnumber"><string>Cardnumber value</string></var>
<var name="lastname"><string>Lastname value</string></var>
<var name="firstname"><string>Firstname value</string></var>
<var name="middlename"><string>Middlename value</string></var>
```



uniteller

self @ online & onlife

```

<var name="address"><string>Address value</string></var>
<var name="email"><string>Email value</string></var>
<var name="approvalcode"><string>Approvalcode value</string></var>
<var name="cvc2"><string>CVC2 value</string></var>
<var name="cardholder"><string>Cardholder value</string></var>
<var name="ipaddress"><string>IPaddress value</string></var>
<var name="billnumber"><string>Billnumber value</string></var>
<var name="bankname"><string>Bankname value</string></var>
<var name="status"><string>Status value</string></var>
<var name="error_code"><string>Error_code value</string></var>
<var name="error_comment"><string>Error_comment value</string></var>
<var name="packetdate"><string>Packetdate value</string></var>
<var name="paymenttype"><string>Paymenttype value</string></var>
<var name="phone"><string>Phone value</string></var>
</struct>
</data>
</wddxPacket>

```

7.3.2.2.2. Error message

```

<?xmlversion="1.0"encoding="utf-8"?>
<wddxPacketversion="1.0">
<header/>
<data>
<struct>
<varname="error_code"><string>Error code</string></var>
<varname="error_message"><string>Error message</string></var>
</struct>
</data>
</wddxPacket>

```

7.3.2.3 XML

7.3.2.3.1. Successful result

```

<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<!DOCTYPE unitellerresult [
  <!ATTLIST unitellerresult
    firstcode CDATA #REQUIRED
    secondcode CDATA #REQUIRED
    count CDATA #REQUIRED
  >
  <!ELEMENT result (orders?)>
  <!ELEMENT orders (order)>
  <!ELEMENT order (ordernumber?, response_code?, recommendation?, message?, comment?,
    date?, total?, currency?, cardtype?, cardnumber?,
    lastname?, firstname?, middlename?, address?, email?,
    approvalcode?, cvc2?, cardholder?, ipaddress?, billnumber?,
    bankname?, status?, error_code?, error_comment?, packetdate?,
    paymenttype?, phone?)>
  <!ELEMENT ordernumber (#PCDATA)>
  <!ELEMENT response_code (#PCDATA)>
  <!ELEMENT recommendation (#PCDATA)>
  <!ELEMENT message (#PCDATA)>
  <!ELEMENT comment (#PCDATA)>
  <!ELEMENT date (#PCDATA)>
  <!ELEMENT total (#PCDATA)>
  <!ELEMENT currency (#PCDATA)>
  <!ELEMENT cardtype (#PCDATA)>

```



```

<!ELEMENT cardnumber (#PCDATA)>
<!ELEMENT lastname (#PCDATA)>
<!ELEMENT firstname (#PCDATA)>
<!ELEMENT middlename (#PCDATA)>
<!ELEMENT address (#PCDATA)>
<!ELEMENT email (#PCDATA)>
<!ELEMENT approvalcode (#PCDATA)>
<!ELEMENT cvc2 (#PCDATA)>
<!ELEMENT cardholder (#PCDATA)>
<!ELEMENT ipaddress (#PCDATA)>
<!ELEMENT billnumber (#PCDATA)>
<!ELEMENT bankname (#PCDATA)>
<!ELEMENT status (#PCDATA)>
<!ELEMENT error_code (#PCDATA)>
<!ELEMENT error_comment (#PCDATA)>
<!ELEMENT packetdate (#PCDATA)>
<!ELEMENT paymenttype (#PCDATA)>
<!ELEMENT phone (#PCDATA)>
]>
<unitellerresult firstcode="" secondcode="" count="1">
  <orders>
    <order>
      <ordernumber>Ordernumber value</ordernumber>
      <response_code>Response_code value</response_code>
      <recommendation>Recommendation value</recommendation>
      <message>Message value</message>
      <comment>Comment value</comment>
      <date>Date value</date>
      <total>Total value</total>
      <currency>Currency value</currency>
      <cardtype>Cardtype value</cardtype>
      <cardnumber>Cardnumber value</cardnumber>
      <lastname>Lastname value</lastname>
      <firstname>Firstname value</firstname>
      <middlename>Middlename value</middlename>
      <address>Address value</address>
      <email>Email value</email>
      <approvalcode>Approvalcode value</approvalcode>
      <cvc2>Значение cvc2</cvc2>
      <cardholder>Cardholder value</cardholder>
      <ipaddress>IPaddress value</ipaddress>
      <billnumber>Billnumber value</billnumber>
      <bankname>Bankname value</bankname>
      <status>Status value</status>
      <error_code>Error_code value</error_code>
      <error_comment>Error_comment value</error_comment>
      <packetdate>Packetdate value</packetdate>
      <paymenttype>Paymenttype value</paymenttype>
      <phone>Phone value</phone>
    </order>
  </orders>
</unitellerresult>

```



uniteller

self @ online & onlife

7.3.2.4 SOAP

WSDL: <https://wpay.uniteller.ru/unblock/wSDL/>

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<SOAP-ENV:Body SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<ASS-NS:MakeReversalResponse xmlns:ASS-NS="http://www.uniteller.ru/message/">
<return xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xsi:type="SOAP-ENC:Array" xmlns:si="http://www.uniteller.ru/type/"
SOAP-ENC:arrayType="si:SOAPStruct[Objects amount]">
<payment xmlns:si=" http://www.uniteller.ru/type/" xsi:type="si:SOAPStruct">
<ordernumber xsi:type="xsd:string">Order ID</ordernumber>
<response_code xsi:type="xsd:string">Response Code</response_code>
<recommendation xsi:type="xsd:string">Recommendation</recommendation>
<message xsi:type="xsd:string">Message</message>
<comment xsi:type="xsd:string">Comment</comment>
<date xsi:type="xsd:string">Date</date>
<total xsi:type="xsd:string">Total</total>
<currency xsi:type="xsd:string">Currency code</currency>
<cardtype xsi:type="xsd:string">Card Type</cardtype>
<cardnumber xsi:type="xsd:string">Card number</cardnumber>
<lastname xsi:type="xsd:string">Last name</lastname>
<firstname xsi:type="xsd:string">Name</firstname>
<middlename xsi:type="xsd:string">Middle name</middlename>
<address xsi:type="xsd:string">Address</address>
<email xsi:type="xsd:string">E-mail</email>
<country xsi:type="xsd:string">Issuing bank county code</country>
<rate xsi:type="xsd:string">Currency rate</rate>
<approvalcode xsi:type="xsd:string">Authorization code</approvalcode>
<cardsubtype xsi:type="xsd:string">Card subtype</cardsubtype>
<cvc2 xsi:type="xsd:string">Use flag</cvc2>
<cardholder xsi:type="xsd:string">Cardholder</cardholder>
<ipaddress xsi:type="xsd:string">Purchaser's IP-address</ipaddress>
<protocoltypename xsi:type="xsd:string">Protocol type</protocoltypename>
<billnumber xsi:type="xsd:string">Payment ID</billnumber>
<bankname xsi:type="xsd:string">Issuing bank name</bankname>
<status xsi:type="xsd:string">Order status</status>
<error_code xsi:type="xsd:string">Processing center response code</error_code>
<error_comment xsi:type="xsd:string">Response code description from the processing
center</error_comment>
<packetdate xsi:type="xsd:string">Packet receiving date</packetdate>
<signature xsi:type="xsd:string">Electronic digital signature</signature>
<processingname xsi:type="xsd:string">Processing</processingname>
<paymenttransactiontype_id xsi:type="xsd:string">Transaction
type</paymenttransactiontype_id>
<phone xsi:type="xsd:string">Phone</phone>
<idata xsi:type="xsd:string">"Long record"</idata>
</payment>
<payment>.....</payment>
</return>
</ASS-NS:MakeReversalResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```



uniteller

self @ online & onlife

In case of an error:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<SOAP-ENV:Body SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<SOAP-ENV:Fault>
<faultcode>First code</faultcode>
<faultstring>Seconf code</faultstring>
<detail />
</SOAP-ENV:Fault>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Error message

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<!DOCTYPE unitellerresult [
  <!ATTLIST unitellerresult
    firstcode CDATA #REQUIRED
    secondcode CDATA #REQUIRED
    count CDATA #REQUIRED
  >
  <!ELEMENT result (orders?)>
  <!ELEMENT orders (order)>
  <!ELEMENT order (ordernumber?, response_code?, recommendation?, message?, com-
ment?,
    date?, total?, currency?, cardtype?, cardnumber?,
    lastname?, firstname?, middlename?, address?, email?,
    approvalcode?, cvc2?, cardholder?, ipaddress?, billnumber?,
    bankname?, status?, error_code?, error_comment?, packetdate?,
    paymenttype?, phone?)>
  <!ELEMENT ordernumber (#PCDATA)>
  <!ELEMENT response_code (#PCDATA)>
  <!ELEMENT recommendation (#PCDATA)>
  <!ELEMENT message (#PCDATA)>
  <!ELEMENT comment (#PCDATA)>
  <!ELEMENT date (#PCDATA)>
  <!ELEMENT total (#PCDATA)>
  <!ELEMENT currency (#PCDATA)>
  <!ELEMENT cardtype (#PCDATA)>
  <!ELEMENT cardnumber (#PCDATA)>
  <!ELEMENT lastname (#PCDATA)>
  <!ELEMENT firstname (#PCDATA)>
  <!ELEMENT middlename (#PCDATA)>
  <!ELEMENT address (#PCDATA)>
  <!ELEMENT email (#PCDATA)>
  <!ELEMENT approvalcode (#PCDATA)>
  <!ELEMENT cvc2 (#PCDATA)>
  <!ELEMENT cardholder (#PCDATA)>
  <!ELEMENT ipaddress (#PCDATA)>
  <!ELEMENT billnumber (#PCDATA)>
  <!ELEMENT bankname (#PCDATA)>
  <!ELEMENT status (#PCDATA)>
  <!ELEMENT error_code (#PCDATA)>
  <!ELEMENT error_comment (#PCDATA)>
  <!ELEMENT packetdate (#PCDATA)>
  <!ELEMENT paymenttype (#PCDATA)>
  <!ELEMENT phone (#PCDATA)>
```



uniteller

self @ online & onlife

```
]>
<unitellerresult firstcode="Error code" secondcode="Error message" count="0">
  <orders></orders>
</unitellerresult>
```

7.3.3 Recurring payment request

7.3.3.1 CSV

7.3.3.1.1. Result receiving

In the received response, the **Response_Code** field contains the response code (see Section 7.2 “Response_code field value”, page 52).

```
OrderNumber;Response_Code;Recommendation;Message;Comment;Date;Total;Currency;CardType
;CardNumber;LastName;FirstName;MiddleName;Address;Email;ApprovalCode;CVC2;CardHolder;
IPAddress;BillNumber;BankName;Status;Error_Code;Error_Comment;PacketDate;PaymentType;
Phone;Signature;
OrderNumber value;Response_Code value;Recommendation value;Message value;Comment
value;Date value;Total value;Currency value;CardType value;CardNumber value;LastName
value;FirstName value;MiddleName value;Address value;Email value;ApprovalCode
value;whether CVC2 is specified;CardHolder value;IPAddress value;BillNumber
value;BankName value;Status value;Error_Code value;Error_Comment value;PacketDate
value;PaymentType value;Phone value;Signature value;
```

Signature value = uppercase(md5(**OrderNumber** + **Total** value + **Password**))

7.3.3.1.2. Error message

```
ErrorCode;ErrorMessage;
Error code;Error message;
```



7.4 PHP code samples

7.4.1 Obtaining the executed transaction report via SOAP

PHP SOAP module is used.

In order to get the confirmation of the successful transaction with **Order_ID**:

```
ini_set('soap.wsdl_cache_enabled', '0');
ini_set('soap.wsdl_cache_ttl', '0');

$client = new SoapClient("https://wpay.uniteller.ru/results/wsdl/",
array(
    'trace'      => 0,
    'exceptions' => 1,
)
);

// Order settings
$Order_ID = "Replace this string with Order_ID";
// e-Shop settings
$Shop_ID = "Replace this string with Shop_ID";
$login = "Replace this string with AuthorizationLogin";
$password = "Replace this string withAuthorizationPassword";

$result = $client->GetPaymentsResult(
    $Shop_ID
    , $login
    , $password
    , $Order_ID
    , $success = 1
    , $startmin = null
    , $starthour = null
    , $startday = null
    , $startmonth = null
    , $startyear = null
    , $endmin = null
    , $endhour = null
    , $endday = null
    , $endmonth = null
    , $endyear = null
    , $meantype = null
    , $paymenttype = null
    , $english = null
);

// check if the transaction data corresponds to the transaction amount,
// which was indicated on the "Basket" page
if (count($result) == 1) {
    // The transaction is executed
}
else {
    // The transaction is not executed
}
```



uniteller

self @ online & onlife

7.5 Payment page signing

Absence of the payment form signing on the Merchant's e-shop website makes the payment page open to fraud attacks.

The Signature allows protecting from any fraud even on the stage of the payment page loading.

The payment form signature is the value of the **Signature** parameter which copulation algorithm is specified in the table 1, page 12 (see Section 6.2.2 "Payment form on the Merchant's e-shop website and its parameters", page 12).

If the signature is incorrect (for example, an attacker has changed one or several fields on the payment page on the e-shop website), the Purchaser will be displayed an error message instead the payment page and the payment process will not start.

