"4g12hs" Merchant Interface

Version 1.1 (the 27h of July 2022)

Content

General Provisions

The Merchant Interface described in this document has been designed to facilitate online and offline payments on Merchants' websites using bank cards and electronic currencies.

The outgoing payments protocol gives an opportunity of making payments to external providers.

To be able to use the Interface, a Merchant must get registered with our Service and send a request from Merchant User Account to be provided with the opportunity to accept/make payments.

Payment Methods and Commission Calculation Rules

Payment methods supported by the Merchant Interface

Payment method	Currency code
VISA/MasterCard	MBC
WMR (WebMoney R)	WMR
Pay by mobile phone account	MobileCommerce
PromSvyazBank online bank	PsbInvoicing
Svyaznoy Stores	Svyaznoy
Elecsnet Terminals	Elecsnet

Payment method	Currency code
AliPay	AliPay
VTcom	VT
Installment PAYLATE	PayLate
Di-Pay	Dipay
QIWI	QIWI
Sberbank	Sberbank
PromSvyazBank branches	PSB-Cash
MKB Terminals (card payment)	MKB-Cards
CONTACT	Contact
MKB Terminals (cash payment)	MKB-Terminals
"Otkrytie" Cash desks / Online-bank	Otkrytie
Euroset Stores	Euroset
Quick Payments System	QuickPayments

Calculation and charging a commission

№	Case	Description	Notes
(1)	Increasing Merchant's invoice by the amount of commission fee	A Merchant receives the full amount specified on the invoice (e.g. if a Merchant has issued an invoice of RUB 50, a sum equivalent to RUB 50 will be deposited into Merchant's account; the commission fee is fully covered by a payer).	WMR
(2)	Commission fee deduction from the amount of invoice paid	In Case (2), the commission fee is deducted from the amount paid (e.g. if a Merchant has issued an invoice of RUB 50 and a payer has paid the invoice with a payment method of 3% commission fee, the sum of RUB 50 – 3% = RUB 48.50 will be deposited into Merchant's account).	MBC
(3)	A combination of (1) and (2)	In Case (3), a Merchant decides beforehand in what proportion a payer and a Merchant split the commission fee (e.g. when using a payment method of 3% commission fee, it is set to increase payer invoice by 1% while the Merchant will pay the remaining 2%. In this case, if the Merchant issues an invoice of RUB 50, the payer will have to pay an equivalent of RUB 50 + 1% = RUB 50.5 meanwhile the sum of RUB 50 – 2% = RUB 49 will be deposited into Merchant's account.)	WMR

ⓘ The list of available currencies and the commission rates are defined for each Merchant on a case-by-case basis.

When accepting bank card payments only the second option is available.

Merchant Interface Description

General operation procedure of the Merchant Interface is as follows:

- a Merchant issues an invoice (**with or without** redirecting to 4g12hs service webpage, including sending an invoice via email or SMS);
- a payer pays an invoice (provided by 4g12hs service);
- if needed a Merchant verifies that the payment has been made correctly by http(s) address specified in Merchant User Account (additionally in case of successful payment, a payment confirmation email is sent to Merchant's email address);
- a Merchant is notified of successful or unsuccessful invoice payment (incl. cancellation) by redirecting a payer to a specified page of Merchant's website;
- Afterwards a Merchant can send additional requests for: status clarification of a particular payment, authorised amounts deduction, refund/cancellation of successful payments (if the respective option is activated), receiving a statement to various criteria and also requests for accepted payments reimbursement (in cases where pay-out by individual requests is available on Merchant side).

Primary Payment Redirection Request$post = "account=$account&operator=$operator

Redirection with payment method selection/credit card details input on the service side

Data is transmitted to 4g12hs service with certain payment redirection parameters making a POST-call at address: https://fin.4g12hs.com/api/payment/start

The following parameters must be set correctly:

Name	Description	Examples	Notes
amount	product price denominated in payment currency (amountcurr)	100, 100.2, 100.25	Decimal separator is a dot (".")
amountcurr	payment currency used to denominate the payment amount (amount)	RUB/USD/EUR	Merchant can issue an invoice in only one preset currency

currency	payment method code used to make a payment (currency code)	MBC/WMR/WMZ/WME etc.	The parameter is optional. If the parameter currency passes an empty string, the System redirects to the payment methods selection form available for a specific Merchant.
number	Merchant's unique internal order number (a string of up to 32 characters); valid characters are: 0-9a-zA-Za-яA-Я, hyphen ("- "), dot (". "), slash ('"/") and space	Invoice5412	
trtype	transaction type	1	For all payment methods except bank cards this parameter should be equal to 1; for bank cards it can be equal to: 1 – for payments where it is necessary to charge an amount from a bank card, 2 – when only bank card authorisation hold on payment is required, 3 – carrying out a payment charging an amount from a bank card and obtaining additional information for making recurring payments, 4 – bank card authorisation hold and obtaining additional information for making recurring payments
recurringFrequency	minimum number of days between recurring payments (at least – 1), the parameter is required if trtype = 3 or 4 If payments are not supposed to be regular put 0 here	28	
recurringEndDate	end date before which recurring payments can be made (YYYYMMDD), the parameter is required if trtype = 3 or 4	20151231	
account	Merchant Account Number in 4g12hs System (is issued upon registration and displayed in Merchant User Account)		
paytoken	a token of a bank card that is to be charged (a Merchant should be preliminary allowed to use this parameter)		
lang	text language on 4g12hs service pages (ru – Russian; en – English); the parameter is not mandatory, when the value is absent or incorrect, ru is used	en	
email	payer's e-mail address (optional parameter)		
validity	time before the transaction processing is to be completed (optional parameter)	2017-03- 23T12:33:06+03:00	
backURL	the parameter allows to specify Merchant website's return URL other than the one specified in Merchant User Account		This parameter is optional. If the parameter backURL passes an empty string or is missing, the System redirects to Merchant's website specified in Merchant User Account.
cf1, cf2, cf3	user fields		
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters amount, amountcurr, currency, number, description, trtype, account, paytoken, backURL, cf1, cf2, cf3, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). If the parameters paytoken, backURL pass an empty string or are missing, they are not used to generate a digital signature and are not followed by a colon. If all the parameters cf1, cf2, cf3 pass an empty string or are missing, they are not used to generate a digital signature and are not followed by a colon. To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

All the parameters must be transmitted in UTF-8 encoding.

Invoice form template (PHP/HTML)

```
<?
    $amount = "10.23";
    $amountcurr = "RUB";
    $currency = "MBC";
    $number = "5412";
    $description = urlencode("Test payment of $amount $amountcurr");
    $trtype = "1";
    $account = "acc001002";
    $paytoken = "";
    $backURL = "";
    $signature = "$amount:$amountcurr:$currency:$number:$description:";
    $signature .= "$trtype:$account:";
    if ($paytoken != "") $signature .= "$paytoken:"; if ($backURL != "") $signature .= "$backURL:";
    $signature .= "secret_key_1:secret_key_2";
    $signature = strtoupper(md5($signature));
?>

<form action="https:// fin.4g12hs.com/api/payment/start" method=POST>
<input type="hidden" name="amount" value="<?print $amount?>">
<input type="hidden" name="amountcurr" value="<?print $amountcurr?>">
<input type="hidden" name="currency" value="<?print $currency?>">
<input type="hidden" name="number" value="<?print $number?>">
<input type="hidden" name="description" value="<?print $description?>">
<input type="hidden" name="trtype" value="<?print $trtype?>">
<input type="hidden" name="account" value="<?print $account?>">
<input type="hidden" name="signature" value="<?print $signature?>">
<input type="submit" value="Pay">
</form>
```

Redirection to payment with bank card details transmission

If Merchant's webpage complies with the PCI DSS standards (verified SAQ of Category D is available), then payer's bank card details can be filled in there. In this case data is transmitted to 4g12hs service with certain payment redirection parameters making a POST-call at address: **https://fin.4g12hs.com/api/payment/execute**

The following parameters must be set correctly:

Please note the absence of parameters ip_address, user_agent and accept_language in the request, which differs from the request in 4.1.3 (Request for making a payment without redirecting to 4g12hs webpage), due to the fact that this request is executed from the payer's browser, which itself provides the specified parameters in the HTTP headers.

Name	Description	Examples	Notes
amount	product price denominated in payment currency (amountcurr)	100, 100.2, 100.25	
amountcurr	payment currency used to denominate the payment amount (amount)	RUB/USD/EUR/GBP	Merchant can invoice in only one currency set for it.
number	Merchant's unique internal order number (a string of up to 32 characters); valid characters are: 0-9a-zA-Za-яA-Я, hyphen ("- "), dot (". "), slash ('"/") and space	Invoice5412	
description	text order description shown as URL-encoded string (6 characters minimum)	%37%31+%56%77	
trtype	transaction type	1	The trtype parameter can take the following values: 1 – for payments where charging an amount from a bank card needed, 2 – when only bank card authorisation hold on payment is required, 3 – carrying out a payment charging the amount from a bank card and obtaining additional information for making recurring payments, 4 – bank card authorisation hold and obtaining additional information for making recurring payments
recurringFrequency	minimum number of days between recurring payments (at least – 1), the parameter is required if trtype = 3 or 4 If payments are not supposed to be regular put 0 here	28	
recurringEndDate	end date before which recurring payments can be made (YYYYMMDD), the parameter is required if trtype = 3 or 4	20151231	
account	Merchant Account Number in 4g12hs System (is issued upon registration and displayed in Merchant User Account)		

PAN	bank card number	4000000000000000	This parameter is not mandatory if the payment is made via card token (paytoken parameter).
expmonth	expiry date month (01, 02, 03, ..., 12)	07	This parameter is not mandatory if the payment is made via card token (paytoken parameter).
expyear	expiry date year (4 digits)	2015	This parameter is not mandatory if the payment is made via card token (paytoken parameter).
cardholder	cardholder name	IVAN IVANOV	This parameter is not mandatory if the payment is made via card token (paytoken parameter). According to the rules of International Payment Systems only Latin symbols are allowed (in exact accordance with the spelling on the front side of the bank card).
securecode	CVV2/CVC2	112	
paytoken	a token of a bank card that is to be charged (a Merchant should be preliminary allowed to use this parameter)		
lang	text language on 4g12hs service pages (ru – russian; en – english); the parameter is not mandatory, when the value is absent or incorrect, ru is used	en	
email	payer's e-mail address (optional parameter)		
validity	time before the transaction processing is to be completed (optional parameter)	2017-03-23T12:33:06+03:00	
backURL	the parameter allows to specify Merchant website's return URL other than the one specified in Merchant User Account		This parameter is optional. If the parameter backURL passes an empty string or is missing, the System redirects to Merchant's website specified in Merchant User Account.
cf1, cf2, cf3	user fields		
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters amount, amountcurr, currency, number, description, trtype, account, paytoken, backURL, cf1, cf2, cf3, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). If the parameters PAN, expmonth, expyear, cardholder, paytoken, backURL pass an empty string or are missing, they are not used to generate a digital signature and are not followed by a colon. If all the parameters cf1, cf2, cf3 pass an empty string or are missing, they are not used to generate a digital signature and are not followed by a colon. To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

All the parameters must be transmitted in UTF-8 encoding.

Invoice form template (PHP/HTML)

```
<?
    $PAN = "4000000000000000";
    $expmonth = "07";
    $expyear = "2015";
    $cardholder = "IVAN IVANOV";
    $securecode = "112";
    $amount = "10.23";
    $amountcurr = "RUB";
    $currency = "MBC";
    $number = "5412";
    $description = urlencode("Test payment of $amount $amountcurr");
    $trtype = "1";
    $account = "acc001002";
    $paytoken = "";
    $backURL = "";
    $signature .= "$amount:$amountcurr:$number:$description:";
    $signature .= "$trtype:$account:";
```

```
    if ($paytoken != "") $signature .= "$paytoken:"; if ($backURL != "") $signature .= "$backURL:";
    $signature .= "secret_key_1:secret_key_2";
    $signature = strtoupper(md5($signature));
?>

<form action="https:// fin.4g12hs.com/api/payment/*****" method=POST>
<input type="hidden" name="PAN" value="<?print $PAN?>">
<input type="hidden" name="expmonth" value="<?print $expmonth?>">
<input type="hidden" name="expyear" value="<?print $expyear?>">
<input type="hidden" name="cardholder" value="<?print $cardholder?>">
<input type="hidden" name="securecode" value="<?print $securecode?>">
<input type="hidden" name="amount" value="<?print $amount?>">
<input type="hidden" name="amountcurr" value="<?print $amountcurr?>">
<input type="hidden" name="number" value="<?print $number?>">
<input type="hidden" name="description" value="<?print $description?>">
<input type="hidden" name="trtype" value="<?print $trtype?>">
<input type="hidden" name="account" value="<?print $account?>">
<input type="hidden" name="signature" value="<?print $signature?>">
<input type="submit" value="Pay">
</form>
```

Request for making a payment without redirecting to 4g12hs webpage

If Merchant's webpage complies with the PCI DSS standards (verified SAQ of Category D is available), and it is necessary to accept payments without switching to 4g12hs service webpage, then data is transmitted to 4g12hs service with certain payment redirection parameters making a POST-call at the address: https://fin.4g12hs.com/api/payment/execute

The following parameters must be set correctly:

Name	Description	Examples	Notes
amount	product price denominated in payment currency (amountcurr)	100, 100.2, 100.25	
amountcurr	payment currency used to denominate the payment amount (amount)	RUB/USD/EUR	Merchant can invoice in only one currency set for it
number	Merchant's unique internal order number (a string of up to 32 characters); valid characters are: 0-9a-zA-Za-яA-Я, hyphen ("- "), dot (". "), slash ('"/") and space	Invoice5412	
description	text order description shown as URL-encoded string (6 characters minimum)	%37%31+%56%77	
trtype	transaction type	1	The trtype parameter can take the following values: 1 – for payments where charging an amount from a bank card needed, 2 – when only bank card authorisation hold on payment is required, 3 – carrying out a payment, charging the amount from a bank card and obtaining additional information for making recurring payments, 4 – bank card authorisation hold and obtaining additional information for making recurring payments
recurringFrequency	minimum number of days between recurring payments (at least – 1), the parameter is required if trtype = 3 or 4 If payments are not supposed to be regular put 0 here	28	
recurringEndDate	end date before which recurring payments can be made (YYYYMMDD), the parameter is required if trtype = 3 or 4	20151231	
account	Merchant Account Number in 4g12hs System (is issued upon registration and displayed in Merchant User Account)		
PAN	bank card number	4000000000000000	This parameter is not mandatory if the payment is made via card token (paytoken parameter).
expmonth	expiry date month (01, 02, 03, ..., 12)	07	This parameter is not mandatory if the payment is made via card token (paytoken parameter).
expyear	expiry date year (4 digits)	2015	This parameter is not mandatory if the payment is made via card token (paytoken parameter).
cardholder	cardholder name	IVAN IVANOV	This parameter is not mandatory if the payment is made via card token (paytoken parameter). According to the rules of International Payment Systems only Latin symbols are allowed (in exact

			accordance with the spelling on the front side of the bank card).
securecode	CVV2/CVC2	112	
paytoken	a token of a bank card that is to be charged (a Merchant should be preliminary allowed to use this parameter)		
email	payer’s e-mail address (optional parameter)		
validity	time before the transaction processing is to be completed (optional parameter)	2017-03-23T12:33:06+03:00	
ip_address	payer’s IP-address ($_SERVER['REMOTE_ADDR'])	112	
user_agent	payer’s browser information ($_SERVER['HTTP_USER_AGENT'])	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/[...]	
accept_language	payer's current language settings ($_SERVER['HTTP_ACCEPT_LANGUAGE'])	de-DE,de;q=0.8,en-US;q=0.6,en;q=0.4,ru;q=0.2	
cf1, cf2, cf3	user fields		
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters amount, amountcurr, number, description, trtype, account, BIN, LAST4, expmonth, expyear, cardholder, paytoken, cf1, cf2, cf3, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). BIN parameter contains the first 6 digits of PAN parameter, LAST4 parameter contains the last 4 digits of PAN parameter. If the parameters PAN, expmonth, expyear, cardholder, paytoken pass an empty string or are missing, they are not used to generate a digital signature and are not followed by colons. If all the parameters cf1, cf2, cf3 pass an empty string or are missing, they are not used to generate a digital signature and are not followed by a colon. To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

All the parameters must be transmitted in UTF-8 encoding.

Request for making a payment without redirecting to 4g12hs webpage using secure card data transmission (cryptogram checkout)

If Merchant’s webpage complies with the PCI DSS standards (verified SAQ of Category D is available), and it is needed to accept payments without redirecting to 4g12hs Service webpage, data transmission to process a payment is done by a POST-call at address: https://fin.4g12hs.com/api/payment/execute

Along with that, the same parameters should be correctly set as when integrating **Request for making a payment without redirecting to 4g12hs webpage**, except for parameters **signature** and card's data **PAN, expmonth, expyear, securecode**. Instead of them, the request should contain **cryptogram** parameter, an encrypted line with the card data generated by the script.

All the parameters must be transmitted in UTF-8 encoding.

Instruction for using the script collecting and encypting card details

Form requirements

- Must operate via HTTPS connection with valid SSL certificate.
- Boxes shouldn't have "name" attribute - this prevents card data from reaching the server when sending a form.
- The input box of a card number must support 16 to 19 digits input.

Cryptogram Requirements

- Must be generated only by the original checkout script downloaded from the system addresses.
- The cryptogram cannot be stored after payment and cannot be used again.

Script Installation

The following script must be added to the payment form page code

```
<script src="https://fin.4g12hs.com/widget/payframe/distr/checkout/bundle.js"></script>
```

Important notes on use

The inputs shouldn't have "name" attribute in the card data entry form.

The card data input boxes must be marked with the attributes:

- **data-cp="cardNumber"** — card number box;
- **data-cp="expDateMonth"** — expiry month box;
- **data-cp="expDateYear"** — expiry year box;
- **data-cp="cvv"** — CVV code box;
- **data-cp="cardholder"** — cardholder name box.

Example form

```
<form id="cardDataForm" autocomplete="off">
    <input type="text" data-cp="cardNumber">
    <input type="text" data-cp="expDateMonth">
    <input type="text" data-cp="expDateYear">
    <input type="text" data-cp="cvv">
    <input type="text" data-cp="name">
    <button type="submit">PAY</button>
</form>
```

Implementation variant of cryptogram generation

```
data.cryptogram = function(formID, account) {
    var form = $(formID)[0];
    var checkout = new Pgw.Checkout(
        // account from Merchant User Account
        account,//"ACC001472",
        // tag containing card data fields
        form
    );
    var result = checkout.createCryptogramPacket();
    if (result.success) {
        // cryptogram is generated
        return result.packet;
    }
    else {
        // input errors are detected, object of `result.messages` format:
        // { cardholder: "There are too many characters in cardholder's name", cardNumber: "Wrong card number" }
        // where `cardholder`, `cardNumber` match the attributes `<input ... data-cp="cardNumber">`
        for (var msgName in result.messages) {
            alert(result.messages[msgName]);
        }
        return;
    }
}('#cardDataForm', data.account);
```

Apple Pay payment registration request

Data is transmitted to 4g12hs service making a POST-call at the address: https://fin.4g12hs.com/api/payment/applepayStart

The following parameters must be set correctly:

Name	Description	Examples	Notes
appId	App ID (app-store-id), where payment is made	284708449	
domainName	The domain from where payment is made in case of payment via web browser. Merchant's Apple Pay should be linked to this domain.	example.com	
validationURL	Apple Pay payment session initialization address obtained from the event ApplePaySession.onvalidatemerchant() when validating Merchant on a device	https://apple-pay- gateway-nc- pod3.apple.com/paymentservices/startSession	
account	Merchant Account Number in 4g12hs System (is issued upon registration and displayed in Merchant User Account)	ACC123456	

amount	product price denominated in payment currency (amountcurr)	100, 100.2, 100.25	
amountcurr	payment currency used to denominate the payment amount (amount)	RUB	Merchant can invoice in only one currency set for it
number	Merchant's unique internal order number (a string of up to 32 characters); valid characters are: 0-9a-zA-Za-яA-Я, hyphen ("- "), dot ("."), slash ("/") and space	Invoice5412	
description	text order description shown as URL-encoded string (6 characters minimum)	%37%31+%56%77	
trtype	transaction type	1, 2, 3, 4	For all payment methods except bank cards this parameter should be equal to 1; for bank cards it can be equal to: 1 – for payments where charging an amount from a bank card needed, 2 – when only bank card authorisation hold on payment is required, 3 – carrying out a payment, charging the amount from a bank card and obtaining additional information for making recurring payments, 4 – bank card authorisation hold and obtaining additional information for making recurring payments
recurringFrequency	minimum number of days between recurring payments (at least – 1), the parameter is required if trtype = 3 or 4 If payments are not supposed to be regular put 0 here	28	
recurringEndDate	end date before which recurring payments can be made (YYYYMMDD), the parameter is required if trtype = 3 or 4	20151231	
lang	text language on 4g12hs service pages (ru – russian; en – english); the parameter is not mandatory, when the value is absent or incorrect, ru is used	en	
email	payer's e-mail address (optional parameter)		
validity	time before the transaction processing is to be completed (optional parameter)	2017-03-23T12:33:06+03:00	
ip_address	payer's IP-address (optional parameter used for anti-fraud purposes)	112	
user_agent	payer's browser information (optional parameter used for anti-fraud purposes)	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/[...]	
accept_language	payer's current language settings information (optional parameter used for anti-fraud purposes)	de-DE,de;q=0.8,en- US;q=0.6,en;q=0.4,r u;q=0.2	
cf1, cf2, cf3	user fields		
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters amount, amountcurr, number, description, trtype, account, cf1, cf2, cf3, appId, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). If the parameter appId passes an empty string or is missing, it is not used to generate a digital signature and is not followed by a colon. If all the parameters cf1, cf2, cf3 pass an empty string or are missing, they are not used to generate a digital signature and are not followed by a colon. To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

All the parameters must be transmitted in UTF-8 encoding.

Apple Pay payment completion request

The result of the payment authorization process on payer's device is an Apple Pay payment token containing encrypted card token data and the payment data which are to be transmitted to 4g12hs Service making a POST-call at address: https://fin.4g12hs.com/api/payment/applepayProceed with the following parameters:

Name	Description	Examples	Notes
transID	Transaction number received during the payment initialization phase		
payment	Structure containing Apple Pay payment token		
payment[token]	Payment token received during Apple Pay authorization process		
payment[token][paymentData]			This and subsequent parameters are the parts of Apple Pay payment token structure
payment[token][paymentData][version]			
payment[token][paymentData][data]			
payment[token][paymentData][signat ure]			
payment[token][paymentData][header]			
payment[token][paymentData][header] [applicationData]			This parameter is optional
payment[token][paymentData][header] [ephemeralPublicKey]			This parameter is optional
payment[token][paymentData][header] [wrappedKey]			This parameter is optional
payment[token][paymentData][header] [publicKeyHash]			
payment[token][paymentData][header] [transactionId]			
payment[token][paymentMethod]			This parameter is optional
payment[token][paymentMethod] [displayName]		MasterCard 7248	This parameter is optional
payment[token][paymentMethod][network]		MasterCard, Visa	This parameter is optional
payment[token][paymentMethod][type]		credit	This parameter is optional
payment[token][transactionIdentifier]			This parameter is optional

Request for making one-stage payment using Apple Pay method

If Merchant's method of integration with Apple Pay provides for self-initialization of an Apple Pay session, prior payment registration with 4g12hs may not be necessary. In this case, payment data and Apple Pay payment token must be submitted to 4g12hs Service making a single POST request at the address https://fin.4g12hs.com/api/payment/applepayExecutecontaining the following parameters:

Name	Description	Examples	Notes
appId	App ID (app-store-id), where payment is made	284708449	
domainName	The domain from where payment is made in case of payment via web browser. Merchant's Apple Pay should be linked to this domain.	example.com	
account	Merchant Account Number in 4g12hs System (is issued upon registration and displayed in Merchant User Account)	ACC123456	
amount	product price denominated in payment currency (amountcurr)	100, 100.2, 100.25	
amountcurr	payment currency used to denominate the payment amount (amount)	RUB	Merchant can invoice in only one currency set for it
number	Merchant's unique internal order number (a string of up to 32 characters); valid characters are: 0-9a-zA-Za-яA-Я, hyphen ("- "), dot (". "), slash ("'/") and space	Invoice5412	

Name	Description	Examples	Notes
description	text order description shown as URL-encoded string (6 characters minimum)	%37%31+%56%77	
trtype	transaction type	1, 2, 3, 4	For all payment methods except bank cards this parameter should be equal to 1; for bank cards it can be equal to: 1 – for payments where charging an amount from a bank card needed, 2 – when only bank card authorisation hold on payment is required, 3 – carrying out a payment, charging the amount from a bank card and obtaining additional information for making recurring payments, 4 – bank card authorisation hold and obtaining additional information for making recurring payments
recurringFrequency	minimum number of days between recurring payments (at least – 1), the parameter is required if trtype = 3 or 4 If payments are not supposed to be regular put 0 here	28	
recurringEndDate	end date before which recurring payments can be made (YYYYMMDD), the parameter is required if trtype = 3 or 4	20151231	
lang	text language on 4g12hs service pages (ru – russian; en – english); the parameter is not mandatory, when the value is absent or incorrect, ru is used	en	
email	payer's e-mail address (optional parameter)		
validity	time before the transaction processing is to be completed (optional parameter)	2017-03-23T12:33:06+03:00	
ip_address	payer's IP-address (optional parameter used for anti-fraud purposes)	112	
user_agent	payer's browser information (optional parameter used for anti-fraud purposes)	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/[...]	
accept_language	payer's current language settings information (optional parameter used for anti-fraud purposes)	de-DE,de;q=0.8,en-US;q=0.6,en;q=0.4,ru;q=0.2	
cf1, cf2, cf3	user fields		
nonce	one-time (pseudo) random value in hex format, must be unique for each request		
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters nonce, amount, amountcurr, number, description, trtype, account, cf1, cf2, cf3, appId, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). If the parameters nonce and appId pass an empty string or are missing, the are not used to generate a digital signature and are not followed by a colon. If all the parameters cf1, cf2, cf3 pass an empty string or are missing, they are not used to generate a digital signature and are not followed by a colon. To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is

Name	Description	Examples	Notes
			subject to the corresponding setting in Merchant User Account.
payment	Structure containing Apple Pay payment token		
payment[token]	Payment token received during Apple Pay authorization process		
payment[token] [paymentData]	(similar to the Apple Pay payment completion request)		
payment[token] [paymentData] [version]			
payment[token] [paymentData][data]			
payment[token] [paymentData] [signature]			
payment[token] [paymentData] [header]			
payment[token] [paymentData] [header] [applicationData]			
payment[token] [paymentData] [header] [ephemeralPublicKey]			
payment[token] [paymentData] [header][wrappedKey]			
payment[token] [paymentData] [header] [publicKeyHash]			
payment[token] [paymentData] [header][transactionId]			
payment[token] [paymentMethod]			
payment[token] [paymentMethod] [displayName]		MasterCard 7248	
payment[token] [paymentMethod] [network]		MasterCard, Visa	
payment[token] [paymentMethod] [type]		credit	
payment[token] [transactionIdentifier]			

Google Pay payment registration request

Before you start integrating your app, please make sure that your solution complies with:

- developers documentation: https://developers.google.com/pay/api/android/
- brand guidelines: https://developers.google.com/pay/api/android/guides/brand-guidelines
- integration checklist: https://developers.google.com/pay/api/android/guides/test-and-deploy/integration-checklist

If you plan to connect payment on a site using your web page, please make sure that your solution complies with the following:

- developers documentation: https://developers.google.com/pay/api/web/
- brand guidelines: https://developers.google.com/pay/api/web/guides/brand-guidelines
- integration checklist: https://developers.google.com/pay/api/web/guides/test-and-deploy/integration-checklist

Necessary parameters for Google Pay integration

Gateway:system_identifier

GatewayMerchantId (is provided with company support)

Please note that Google Pay payment method is supported only for Visa and Mastercard cards

Data is transmitted to 4g12hs service making a POST-call at address:: https://fin.4g12hs.com/api/payment/googlepayStart

The following parameters must be set correctly:

Name	Description	Examples	Notes
appId	Google App identifier where payment is made	284708449	
domainName	The domain from where payment is made in case of payment via web browser. Merchant's Google Pay should be linked to this domain.	example.com	
account	Merchant Account Number in 4g12hs System (is issued upon registration and displayed in Merchant User Account)	ACC123456	
amount	product price denominated in payment currency (amountcurr)	100, 100.2, 100.25	
amountcurr	payment currency used to denominate the payment amount (amount)	RUB	Merchant can invoice in only one currency set for it
number	Merchant's unique internal order number (a string of up to 32 characters); valid characters are: 0-9a-zA-Za-яA-Я, hyphen ("- "), dot (". "), slash ('"/") and space	Invoice5412	
description	text order description shown as URL-encoded string (6 characters minimum)	%37%31+%56%77	
trtype	transaction type	1, 2, 3, 4	For all payment methods except bank cards this parameter should be equal to 1; for bank cards it can be equal to: 1 – for payments where it is necessary to charge an amount from a bank card, 2 – when only bank card authorisation hold on payment is required, 3 – carrying out a payment charging an amount from a bank card and obtaining additional information for making recurring payments, 4 – bank card authorisation hold and obtaining additional information for making recurring payments
recurringFrequency	minimum number of days between recurring payments (at least – 1), the parameter is required if trtype = 3 or 4 If payments are not supposed to be regular put 0 here	28	
recurringEndDate	end date before which recurring payments can be made (YYYYMMDD), the parameter is required if trtype = 3 or 4	20151231	
lang	text language on 4g12hs service pages (ru – russian; en – english); the parameter is not mandatory, when the value is absent or incorrect, ru is used	en	
email	payer's e-mail address (optional parameter)		
validity	time before the transaction processing is to be completed (optional parameter)	2017-03-23T12:33:06+03:00	
ip_address	payer's IP-address (optional parameter used for anti-fraud purposes)	112	
user_agent	payer's browser information (optional parameter used for anti-fraud purposes)	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/[...]	
accept_language	payer's current language settings information (optional parameter used for anti-fraud purposes)	de-DE,de;q=0.8,en-US;q=0.6,en;q=0.4,ru;q=0.2	
cf1, cf2, cf3	user fields		
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters amount, amountcurr, number, description, trtype, account, cf1, cf2, cf3, appId, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account).

Name	Description	Examples	Notes
			If the parameter **appId** passes an empty string or is missing, it is not used to generate a digital signature and is not followed by a colon. If all the parameters cf1, cf2, cf3 pass an empty string or are missing, they are not used to generate a digital signature and are not followed by a colon. To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

All the parameters must be transmitted in UTF-8 encoding.

Google Pay payment completion request

The result of a payment authorization process on payer's device is a Google Pay payment token containing encrypted card token data and payment data that must be transmitted to 4g12hs Service making a POST-call at the address https://fin.4g12hs.com/api/payment/googlepayProceed with the following parameters:

Name	Description	Examples
transID	Transaction number received during initialization stage	
payment	Structure containing Google Pay payment token	
payment[token]	Payment token received during Google Pay authorization process	
payment[token][apiVersion]		
payment[token][apiVersionMinor]		
payment[token][paymentMethodData]		
payment[token][paymentMethodData][description]		"Visa •••• 3189"
payment[token][paymentMethodData][info]		
payment[token][paymentMethodData][info][cardNetwork]		"VISA"
payment[token][paymentMethodData][info][cardDetails]		"3189"
payment[token][paymentMethodData][tokenizationData]		
payment[token][paymentMethodData][tokenizationData][token]		
payment[token][paymentMethodData][tokenizationData][type]		"PAYMENT_GATEWAY"
payment[token][paymentMethodData][type]		"CARD"

4g12hs request for transaction confirmation

In the cases listed below, 4g12hs Service performs a POST-call at a predetermined http(s) address of a Merchant to confirm the operation.

The call is made in the following cases:

– upon initial request for switching to payment provided all the request parameters of the online shop form are transmitted correctly

That said the following parameters are transmitted:

– to request to switch to a payment with the choice of payment methods /bank card data input on the Service side:

Name	Description	Examples	Notes
opertype	request mode	pay	
amount, amountcurr, currency, number, description, trtype, recurringFrequency, recurringEndDate, account, paytoken, backURL, cf1, cf2, cf3	contain the same values as those when the invoice is formed		
conversion_amount	payer invoice amount		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on Merchant's side. (amountcurr parameter).

			The corresponding option becomes available on activating *autoconversion* service (for merchants who receive compensation on accepted payments in a currency other than the one on payer invoice).
conversion_currency	payer invoice currency		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on Merchant's side. (amountcurr parameter). The corresponding option becomes available on activating *autoconversion* service (for merchants who receive compensation on accepted payments in a currency other than the one on payer invoice).
conversion_rate	currency conversion rate from currency to conversion_currency		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on Merchant's side. (amountcurr parameter). The corresponding option becomes available on activating *autoconversion* service (for merchants who receive compensation on accepted payments in a currency other than the one on payer invoice).
datetime	current date/time	2015-03-23 12:33:06.469763	
transID	transaction number	15431522	This number is used for all subsequent payment status clarification requests. To prevent a failure to obtain (e.g. due to connectivity issues) this number properly (by initial request response), it is recommended to save it on Merchant's server at this stage already
datetime	current date/time	2015-03-23 12:33:06.469763	
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters opertype, amount, amountcurr, currency, number, description, trtype, account, cf1, cf2, cf3, paytoken, backURL, transID, datetime, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). If the parameters paytoken and backURL pass an empty string or are missing, they are not used to generate a digital signature and are not followed by a colon. If all the parameters cf1, cf2, cf3 pass an empty string or are missing, they are not used to generate a digital signature and are not followed by a colon. To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

- to request to switch to a payment with bank card details transmission

Name	Description	Examples	Notes
opertype	request mode	pay	
PANmasked	bank card masked number transmitted in the original request	400000******0000	
cardholder, amount, amountcurr, number, description, trtype, account, paytoken, backURL, cf1, cf2, cf3	contain the same values as those when the invoice is formed		
conversion_amount	payer invoice amount		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on Merchant's side. (amountcurr parameter). The corresponding option becomes available on activating *autoconversion* service (for merchants who receive compensation on accepted payments in a currency other than the one on payer invoice).
conversion_currency	payer invoice currency		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on Merchant's side. (amountcurr parameter). The corresponding option becomes available on activating *autoconversion* service (for merchants who receive compensation on accepted payments in a currency other than the one on payer invoice).
conversion_rate	currency conversion rate from currency to conversion_currency		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on Merchant's side. (amountcurr parameter). The corresponding option becomes available on activating *autoconversion* service (for merchants who receive compensation on accepted payments in a currency other than the one on payer invoice).
transID	transaction number	15431522	This number is used for all subsequent payment status clarification requests.

			To prevent a failure to obtain (e.g. due to connectivity issues) this number properly (by initial request response), it is recommended to save it on Merchant's server at this stage already
datetime	current date/time	2015-03-23 12:33:06.469763	
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters PANmasked, cardholder, opertype, amount, amountcurr, number, description, trtype, account, cf1, cf2, cf3, paytoken, backURL, transID, datetime, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). If the parameters paytoken, backURL pass an empty string or are missing, they are not used to generate a digital signature and are not followed by a colon. If all the parameters cf1, cf2, cf3 pass an empty string or are missing, they are not used to generate a digital signature and are not followed by a colon. To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

- to request for payment execution without switching to the 4g12hs Service website and to request for payment registration when using Apple Pay method:

Name	Description	Examples	Notes
opertype	request mode	pay	
PANmasked	bank card masked number transmitted in the original request	400000******0000	
cardholder, amount, amountcurr, number, description, trtype, account, paytoken, cf1, cf2, cf3	contain the same values as those when the invoice is formed		
conversion_amount	payer invoice amount		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on Merchant's side. (amountcurr parameter). The corresponding option becomes available on activating *autoconversion* service (for merchants who receive compensation on accepted payments in a currency other than the one on payer invoice).
conversion_currency	payer invoice currency		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on Merchant's side. (amountcurr parameter). The corresponding option becomes available on activating *autoconversion* service (for merchants who receive compensation on accepted payments in a currency other than the one on payer invoice).
conversion_rate	currency conversion rate from currency to conversion_currency		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on Merchant's side. (amountcurr parameter). The corresponding option becomes available on activating *autoconversion* service (for merchants who receive compensation on accepted payments in a currency other than the one on payer invoice).
transID	transaction number	15431522	This number is used for all subsequent payment status clarification requests. To prevent a failure to obtain (e.g. due to connectivity issues) this number properly (by initial request response), it is recommended to save it on Merchant's server at this stage already
datetime	current date/time	2015-03-23 12:33:06.469763	
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters PANmasked, cardholder, opertype, amount, amountcurr, number, description, trtype, account, cf1, cf2, cf3, paytoken, transID, datetime, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). If the parameter paytoken, passes an empty string or is missing, it is not used to generate a digital signature and is not followed by a colon. If all the parameters cf1, cf2, cf3 pass an empty string or are missing, they are not used to generate a digital signature and are not followed by a colon. To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

- upon authorization hold release request:

Name	Description	Examples	Notes
opertype	request mode	unblock	
account	Merchant Account Number in 4g12hs System		
transID	transaction number	15431522	
datetime	current date/time	2015-03-23 12:33:06.469763	
signature	digital signatur		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters opertype, account, transID, datetime, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

- upon authorization hold charge request:

Name	Description	Examples	Notes
opertype	request mode	terminate	
amountterminate	charged amount denominated in merchant invoice currency	50.52	
conversion_amount	charged amount defined by payer invoice currency		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on merchant's side. (amountcurr parameter). The corresponding option becomes available on activating *autoconversion* service (for the merchants who receive compensation on accepted payments in a currency other than the one on payer invoice).
conversion_currency	payer invoice currency		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on merchant's side. (amountcurr parameter). The corresponding option becomes available on activating *autoconversion* service (for the merchants who receive compensation on accepted payments in a currency other than the one on payer invoice).
conversion_rate	conversion rate from merchant invoice currency to conversion_currency		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on merchant's side. (amountcurr parameter). The corresponding option becomes available on activating *autoconversion* service (for the merchants who receive compensation on accepted payments in a currency other than the one on payer invoice).
account	Merchant Account Number in 4g12hs System		
transID	transaction number	15431522	
datetime	current date/time	2015-03-23 12:33:06.469763	
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters opertype, amountterminate, account, transID, datetime, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

- upon partial or full transaction cancellation:

Name	Description	Examples	Notes
opertype	request mode	reversal	
amountreversal	refund amount defined by merchant invoice currency	50.52	
conversion_amount	refund amount defined by payer invoice currency		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on merchant's side. (amountcurr parameter).

			The corresponding option becomes available on activating *autoconversion* service (for the merchants who receive compensation on accepted payments in a currency other than the one on payer invoice).
conversion_currency	payer invoice currency		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on merchant's side. (amountcurr parameter). The corresponding option becomes available on activating *autoconversion* service (for the merchants who receive compensation on accepted payments in a currency other than the one in payer invoice).
conversion_rate	conversion rate from merchant invoice currency to conversion_currency		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on merchant's side. (amountcurr parameter). The corresponding option becomes available on activating *autoconversion* service (for the merchants who receive compensation on accepted payments in a currency other than the one on payer invoice).
account	Merchant Account Number in 4g12hs System		
transID	transaction number	15431522	
datetime	current date/time	2015-03-23 12:33:06.469763	
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters opertype, amountreversal, account, transID, datetime, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

When transaction confirmation received, a Merchant should send a transID value in response to each of the above requests. In case of any other response, the transaction will not be carried out, and 4g12hs will return the error of missing transaction confirmation.

- upon carrying out recurring payment the following parameters are transmitted:

Name	Description	Examples	Notes
opertype	request mode	recurrring	
amountrecurring	recurring payment amount	50.52	
account	Merchant Account Number in 4g12hs System		
transIDparent	ID number of transaction along with which recurring payment subscription was initiated	15431522	
recurringID	ID number for carrying out recurring payments	11311211312	
numberrecurring	recurring payment's number for Merchant's record purposes (if specified in Merchant's recurring payment request). *However, if the check-box "Unique Order ID" is checked in the Merchant's settings, this parameter is mandatory.*		54321
descriptionrecurring	recurring payment's text description shown as URL-encoded string (if specified in Merchant's recurring payment request)		%37%31+%56%77
cf1, cf2, cf3	user fields		
transIDrecurring	recurring payment transaction number		15431525
datetime	current date/time		2015-03-23 12:33:06.469763
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters opertype, amountrecurring, account, transIDparent, recurringID, numberrecurring, descriptionrecurring, cf1, cf2, cf3, transIDrecurring, datetime, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). If the parameters numberrecurring and descriptionrecurring pass an empty string or are missing, they are not used to generate a digital signature and are not followed by a colon.

			If all the parameters cf1, cf2, cf3 pass an empty string or are missing, they are not used to generate a digital signature and are not followed by a colon. To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

In case of operation approval, a Merchant should send a transIDrecurring value in response to this request. In case of any other response, the operation will not be carried out, and 4g12hs will return the error of missing operation confirmation.

Analysis of a request on Merchant's server (opertype=pay)

```
<?
   $opertype = $_POST["opertype"];
   switch($opertype)
   {
     case "pay":
                 $nonce = $_POST["nonce"];
                 $masked_pan = $_POST["masked_pan"];
                 $cardholder = $_POST["cardholder"];
                 $opertype = $_POST["opertype"];
                 $amount = $_POST["amount"];
                 $amountcurr = $_POST["amountcurr"];
                 $number = $_POST["number"];
                 $description = $_POST["description"];
                 $trtype = $_POST ["trtype"];
                 $account = $_POST["account"];
                 $paytoken = $_POST["paytoken"];
                 $backURL = $_POST["backURL"];
                 $transID = $_POST["transID"];
                 $datetime = $_POST["datetime"];
                 $cf1 = $_POST["cf1"];
                 $cf2 = $_POST["cf2"];
                 $cf3 = $_POST["cf3"];
                 $signature = $_POST["signature"];

       // Performing actions to determine correctness
       // transmitted parameters

       $testsig = "$nonce:$masked_pan:$cardholder:";
                 $testsig .= "$opertype:$amount:$amountcurr:";
                 $testsig .= "$number:$description:$trtype:";
                 $testsig .= "$account:";
                 if ($cf1 || $cf2 || $cf3) {
                     $testsig .= "$cf1:$cf2:$cf3:";
                 }
                 if ($paytoken) {
                     $testsig .= "$paytoken:";
                 }
                 if ($backURL) {
                     $testsig .= "$backURL:";
                 }
                 $testsig .= "$transID:$datetime:";
                 $testsig .= "секретный_ключ_1:секретный_ключ_2";
                 $testsig = strtoupper(md5($testsig));

                 if ($signature==$testsig)
       {
           if (Payment is to be carried out)
           {
               print $transID; exit(-1);
           }
       }
       print "No, thanks"; // for cancellation of making
                          // a payment any sequence of symbols
                          // can be returned
       break;
    case "terminate":
                ...
    case "reversal":
```

```
        ...
    }
?>
```

4g12hs response to a payment redirection request

For requests to switch to a payment with the choice of payment methods/bank card data input on the Service side, switching to payment with bank card details transmission and request for one-stage payment with Apple Pay method

If any parameters of the original request are not filled in or filled in incorrectly, as well as if no confirmation of payment has been received from a Merchant, redirection at Merchant's address indicated in backURL field (in User Account) turns on. That said the following (POST or GET, depending on the settings in User Account) parameters are transmitted:

Name	Description	Examples	Notes
errorcode	error code	101	Error codes list is provided in Appendix 1 of this document
errortext	error text message; with character indication as %XX	Product value specified incorrectly	
transID	transaction number	15431522	The value is returned if the error occurs after the transaction was assigned a number

To request for payment execution without redirecting to 4g12hs Service website

Request results in a json-response containing the following parameters:

status

transID

[additional parameters]

Parameter status may contain one of the following values:

- OK (operation successfully completed): this status is a terminal one on condition there are no refunds for the corresponding transaction; in case of making refunds, including partial ones, the transaction status will be changed to reversal
- authorise (blocked Amount); the status isn't terminal one; according to the rules of international payment systems, for transactions with this status a Merchant should send charge or release request: for VISA cards - within 5 days, for MasterCard - within 5 days
- error (operation execution error); the status can be terminal.
- wait (pending response from payment system); this status is non-terminal if 3 additional parameters are transmitted (ACSURL, PaReq, MD), 4g12hs service goes into standby mode waiting from a Merchant for the results of payment authorization on the side of a card's issuing bank.

Additional parameters:

- in case the transaction has one of the following statuses: OK, authorise:

Name	Description	Examples
time	operation completion time	2008-04-13T17:29:39+04:00
number	duplicates the value of the original request	1234
PAN	bank card masked number	400000******0000
cardholder	cardholder name (According to the rules of International Payment Systems only Latin symbols are allowed (in exact accordance with the spelling on the front side of the bank card)	CARDHOLDER NAME
paytoken	a token of a bank card that is charged (the parameter returns if the corresponding option is set for a Merchant)	
recurringID	ID number for carrying out recurring payments (returns if trtype = 3 or 4)	11311211312

- in case of an error (status = error):

Name	Description	Examples	Notes
errorcode	error code	312	Error codes list is provided in Appendix 2 of this document
errortext	error text message	payment amount specified incorrectly	
processing_code	payment denial code received from the bank (Response Code according to ISO 8583)		
processing_text	reason for payment denial		

If in the payment status query the appinfo was equal to 1, in the response to the request (when transaction status: OK, authorise, or error) *additional parameters* given in the table of Information on payment made are transmitted. In case the transaction status is equal to an error, transmission of additional parameters is carried out only if the transaction is rejected in accordance with anti-fraud policy rules.

- in case the final information about the payment has not been received from payment system or has been received additional information required to make a payment (status = wait):

Name	Description	Examples

number	duplicates the value of the original request	Invoice5412

When additional information required to make a payment has been received from the payment system, the following parameters are also transmitted:

Name	Description	Examples
ACSURL	the address to be switched at by a Merchant to authorize a payment on a website of a card's issuing bank	
PaReq	parameter to be sent at ACSURL address	
MD	Additional parameter for payment identification	

Having received such an answer, a Merchant should send a payer to the page specified in the parameter ASCURL. Redirection to the ASCURL must be done by a POST method transmitting the following parameters:

Name	Description	Examples
PaReq	PaReq parameter value from 4g12hs server’s response	
MD	MD parameter value from 4g12hs server’s response (If needed, additional information can be added to the value of this parameter for payment identification on Merchant’s side)	
TermUrl	merchant server's page address at which redirection will be done after a payment is processed on ACSURL	

The parameters PaRes and MD will be transmitted to the TermUrl page, MD will contain the same value that was transmitted in ACSURL request.

If necessary, the value of the original MD parameter that was received from the 4g12hs server must be restored from the MD value. After that, in order to complete payment processing on the payment system’s side it is necessary to make a POST call at the address: https://fin.4g12hs.com/api/payment/pares

The following parameters must be set correctly:

Name	Description	Examples	Notes
PaRes	parameter value PaRes, transmitted to TermUrl		
MD	MD parameter value from 4g12hs server’s response		
transID	transaction number	2015	
datetime	current date/time	2015-03-23 12:33:06.469763	
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters PaRes, MD, transID, datetime, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

The answer to this request is the same as the answer to the request for payment status.

Request for payment registration using Apple Pay method

Request results in a json-response containing the following parameters:

status

transID

[additional parameters]

Parameter status may contain one of the following values:

- error (operation execution error); the status can be terminal.
- wait (pending request for payment completion by Apple Pay method)

Additional parameters:

- in case of an error (status = error):

Name	Description	Examples	Notes
errorcode	error code	312	Error codes list is provided in Appendix 2 of this document
errortext	error text message	payment amount specified incorrectly	

Request for payment completion using Apple Pay method

Request results in a json-response containing the following parameters:

status

transID

[additional parameters]

Parameter status may contain one of the following values:

- error (operation execution error); the status can be either terminal or non-terminal, for example, in case the first payment attempt failed, but the client, staying in Merchant's payment system, made another (successful) payment attempt
- wait (waiting for payment system's response)

Additional parameters:

- in case of an error (status = error):

Name	Description	Examples	Notes
errorcode	error code	312	Error codes list is provided in Appendix 2 of this document
errortext	error text message	payment amount specified incorrectly	
processing_code	payment denial code received from a bank (Response Code according to ISO 8583)		
processing_text	reason for payment denial		

Information on payment made

It is necessary to process this information if payments are accepted online (for example, when selling electronic products/services to which a payer must get immediate access after payment).

If the field "payment status notification URL" (statusURL) is filled in Merchant User Account, after a successful payment is done a POST-call requests the address contained in it, with the following parameters:

Name	Description	Examples	Notes
amount, amountcurr, number, description, trtype, recurringFrequency, recurringEndDate, account, backURL	contain the same values as those when the invoice is formed		
currency	payment method code used to make a payment	MBC/WMR/WMZ/WME etc.	
payamount	amount paid by a customer (defined by the payment currency)	100, 100.2, 100.25	
percentplus	interest (commission) charged by the System in addition to invoice amount	2.0, 3.5	
percentminus	interest (commission) which will be deducted by the System from invoice amount	2.0, 3.5	
conversion_amount	payer invoice amount		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on Merchant's side. (amountcurr parameter). The corresponding option becomes available on activating *autoconversion* service (for the Merchants who receive compensation on accepted payments in a currency other than the one on payer invoice).
conversion_currency	payer invoice currency		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on Merchant's side. (amountcurr parameter). The corresponding option becomes available on activating *autoconversion* service (for the Merchants who receive compensation on accepted payments in a currency other than the payer invoice one).
conversion_rate	currency conversion rate from currency to conversion_currency		This parameter is transmitted only if the currency of an invoice paid by a customer differs from the currency specified in the primary payment request on Merchant's side. (amountcurr parameter). The corresponding option becomes available on activating *autoconversion* service (for the Merchants who receive compensation on accepted payments in a currency other than the payer invoice's one).
PAN	bank card masked number	400000******0000	PAN and cardholder parameters are returned only if the payment was made with a bank card
cardholder	cardholder name	CARDHOLDER NAME	PAN and cardholder parameters are returned only if the payment was made with a bank card

paytoken	a token of a bank card that is charged (the parameter returns if the corresponding option is set for a Merchant)		
transID	transaction number	15431522	
recurringID	ID number for carrying out recurring payments (returns if trtype = 3 or 4)	11311211312	
datetime	current date/time	2015-03-23 12:33:06.469763	
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters amount, amountcurr, currency, number, description, trtype, payamount, percentplus, percentminus, account, paytoken, backURL, transID, datetime, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). If the parameter paytoken, passes an empty string or is missing, it is not used to generate a digital signature and is not followed by a colon. If upon the original request the parameter backURL, passes an empty string or is missing, it is not used to generate a digital signature and is not followed by a colon either. To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

In case a payment is made with a bank card and the option to receive anti-fraud information is active in Merchant Acount, then *additional parameters* are returned:

Name	Description	Examples
binName	card issuer's name	MAX-BANK
binCountry	card's issuing bank country (two-character code according to ISO 3166)	RU
binPhone	card issuer's phone number	74950000000
binPrepaid	prepaid card indicator (Yes or No)	No
ipCountry	country of payer's IP address (two-character code according to ISO 3166, additional codes: A1 - anonymous proxy server, A2 - satellite internet, EU - Europe, AP - Asia Pacific region)	RU
ipHighRisk	indicator of a country with a high level of fraud activity (Yes or No)	No
ipRiskScore	payer IP address fraud risk rating indicator (up to 1: low; 1-2: medium; 2-3: high; more than 3: high)	0.0
mailFree	indication whether the e-mail address belongs to a free mail service (Yes or No)	Yes
riskScore	general rating of a transaction fraud-risk, fraud probability percentage (from 0.01 to 100)	1.12

As an additional check you can use IP address analysis - all 4g12hs calls are made from **XXX.XXX.XXX.XXX** address.

In response to this request, a Merchant should return "OK" symbols. In case of any other response, our server will repeat similar requests (subject to the choice of the appropriate option in Personal Account) in some time intervals within a few hours since the moment of successful payment until receiving "OK" response. In case of not receiving response "OK" within this period of time the corresponding message will be sent at Merchant's e-mail.

In order to prevent the situation when the info about successful payment isn't received by a Merchant (for example, in case of long-term unavailability of merchant's server), it is recommended to make payment status requests to the 4g12hs server for each payment initiated by a Merchant without successful status. These requests must be repeated until a payment acquires one of the terminal statuses.

If a Merchant is connected to the fiscal mode, then after successful payment 4g12hs Service will send a fiscal receipt to the client by e-mail. E-mail address for sending a fiscal receipt can be filled by a payer in the payment form on a webpage of our service or forwarded from a Merchant.

Checking invoice payment (PHP)

```php
<?
    $amount = $_POST["amount"];
    $amountcurr = $_POST["amountcurr"];
    $currency = $_POST["currency"];
    $number = $_POST["number"];
    $description = $_POST["description"];
    $trtype = $_POST["trtype"];
    $payamount = $_POST["payamount"];
    $percentplus = $_POST["percentplus"];
    $percentminus = $_POST["percentminus"];
    $account = $_POST["account"];
    $backURL = $_POST["backURL"];
```

```php
    $transID = $_POST["transID"];
    $datetime = $_POST["datetime"];
    $signature = $_POST["signature"];

    $testsig = "$amount:$amountcurr:$currency:$number:";
    $testsig .= "$description:$trtype:$payamount:$percentplus:";
    $testsig .= "$percentminus:$account";
    if ($backURL != "") $testsig .= "$backURL:";
    $testsig .= "$transID:$datetime:";
    $testsig .= "secret_key_1:secret_key_2";
    $testsig = strtoupper(md5($testsig));
    if ($signature==$testsig)
    {
        // The digital signature is correct, the invoice is paid,
        // change order status
    }
?>
```

Redirection to Merchant's website after payment

A return after a payment to Merchant's website (in case a Merchant supports the return) is made at the address specified in "URL for return after payment" (backURL) field in Merchant User Account.

The return is made with a POST or GET method (indicated by a Merchant in User Account) with following parameters transmission:

Name	Description	Examples
amount, amountcurr, account, number, description	contain the same values as those when the invoice is formed	
transID	transaction number	

In case of unsuccessful payment, two additional parameters are also transmitted:

Name	Description	Examples
errorcode	error code	2000
errortext	error text message; with character indication as %XX	"payment cancelled"

The fact of return page opening cannot be used as a proof of payment (even if there are no fields containing error information). Only the call at the statusURL address described in "Payment information" is a guarantee of payment.

Processing payment information (PHP/HTML)

```php
<?
    $amount = $_POST["amount"];
    $amountcurr = $_POST["amountcurr"];
    $account = $_POST["account"];
    $number = $_POST["number"];
    $description = $_POST["description"];
    $transID = $_POST["transID"];
    $errorcode = $_POST["errorcode"];
    $errortext = $_POST["errortext"];
?>

Amount: <b><?print $amount?></b><br>

Amountcurr: <b><?print $amountcurr?></b><br>

Account: <b><?print $account?></b><br>

Number: <b><?print $number?></b><br>

Description: <b><?print stripslashes(urldecode($description));?></b><br>

Errorcode: <b><?print $errorcode?></b><br>
```

```
Errortext: <b><?print urldecode($errortext)?></b><br>
```

Additional requests to 4g12hs server for a status of a payment made

If needed, a Merchant can send additional requests for the current transaction status.

The request is sent with a POST-call at the address: https://fin.4g12hs.com/api/payment/operate

That said the following parameters should be set correctly:

Name	Description	Examples	Notes
opertype	fixed value – check	check	
transID	transaction number, returned by 4g12hs server upon the initial request	15431522	This code for each transaction is also displayed when requesting the details of the account (including the Personal Account). The parameter is mandatory if the parameter number is missing.
number	value transmitted upon the initial switch/request	Invoice5412	The parameter is mandatory if the transID parameter is missing. When using this parameter, the correct information about the transaction will be returned only if there is only one transaction corresponding to the specified number value.
account	Merchant Account Number in 4g12hs System (is issued upon registration and displayed in Merchant User Account)		
appinfo	detaild information return: 0 – not needed (by default), 1 – needed	1	This parameter is used if the possibility of receiving anti-fraud information on transactions made with bank cards is set for the Merchan't account. When it is equal to 1, additional parameters are returned according to the table for Information on payment made.
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters opertype, account, transID, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

Operation result response returned by 4g12hs server to a request for executed payment status

Request results in a json-response containing the following parameters:

status

transID

amount

amountcurr

finalamount

datetime

[additional parameters]

Parameter status may contain one of the following values:

- OK (operation successfully completed): this status is a terminal one on condition that no returns will be made for the corresponding transaction; in case of making refunds, including partial ones, the transaction status will be changed to reversal
- reversal (the transaction is partially or completely cancelled); if the amount of a refund coincides with the amount of the original order, this status is a terminal one; otherwise, additional refunds may be done for this transaction (if multiple refunds are supported by the acquiring bank).
- authorise (blocked Amount); the status isn't terminal one; according to the rules of international payment systems, for transactions with this status a Merchant should send charge or release request: for VISA cards - within 5 days, for MasterCard - within 5 days
- unblocked (released amount); this status is a terminal one; the transaction acquires it after successful unlocking.
- error (operation execution error); the status can be terminal.
- wait (waiting for response from payment system); this status can be either terminal (for example, if a payer, having switched to payment system has closed the browser page and hasn't finished the payment), or non-terminal one, if the payment will be finished by a customer

Parameter finalamount contains the transaction amount including all partial refunds.

Parameter datetime contains the time of processing the incoming request in the format:

YYYY-MM-DDTHH:MM:SS+-HH:MM, for example: 2008-04-13T17:29:39+04:00.

Additional parameters:

- in case the transaction has one of the following statuses: OK, reversal, authorise, unblocked:

Name	Description	Examples	Notes
time	operation completion time	2008-04-13T17:29:39+04:00	
number	duplicates the value of the original request	1234	
PAN	bank card masked number	400000******0000	PAN and cardholder parameters are returned only if the payment was made with a bank card

cardholder	cardholder name	CARDHOLDER NAME	PAN and cardholder parameters are returned only if the payment was made with a bank card
paytoken	a token of a bank card that is charged (the parameter returns if the corresponding option is set for a Merchant)		
recurringID	ID number for carrying out recurring payments (returns if trtype = 3 or 4)	11311211312	

- if the transaction has the status: "wait" and the Merchant's account has an active checkbox «Provide step info in the response to payment status check», the step parameter will be passed as an additional parameter in the response body, which can contain one of the following values:

Name	Description
3ds	Payer filled Cardholder Data and got redirected to the issuing bank's page for 3DS auth procedure
init	Payment is initialized in the processor system; Cardholder Data hasn't been filled
proc	Payer has filled Cardholder Data and the Non-3DS operation is being processed
unknown	Current status of the operation is unknown, however, it hasn't been processed yet (terminal status – success or error – cannot be guaranteed by the system)

- in case the currency of an invoice paid by a customer differs from the currency specified in the initial request for payment by a Merchant (parameter amountcurr). The corresponding option becomes available on activating *autoconversion* service (for the Merchants who receive compensation on accepted payments in a currency other than the payer's invoice one):

Name	Description	Examples
conversion_amount	refund amount denominated in payer invoice currency	
conversion_currency	payer invoice currency	
conversion_rate	conversion rate from merchant invoice currency to conversion_currency	

If a Merchant is connected to the fiscal mode, then an additional parameter (data set) fiscal_data will be returned, each element of which consists of two parameters:

Name	Description	Examples
cash_rcp_text	string containing text ready to print receipt	
cash_rcp_data	fiscal receipt details	

Parameter cash_rcp_data, in its turn is a data set containing the following parameters:

Name	Description	Examples
cash_rcp_type	fiscal receipt type	pay *or* reversal
org	legal name of the entity receiving the payment (agent)	
fiscal_store	agent's fiscal number	
fiscal_inn	agent's Taxpayer Identification Number	
address	first line of agent address	
place	second line of agent address	
shop_name	name of the entity receiving the payment (online shop)	
shop_inn	Merchant Taxpayer Identification Number	
shop_site	Merchant's webpage	
number	order number generated by a Merchant	
email	payer's email address	
amount	transaction amount in rubles	
fee	transaction fee (in rubles)	
amount_final	transaction amount, including commission fee (in rubles)	
amount_total	total amount (in rubles)	
support	helpdesk contacts line	
reg_num	reg. number of a cash register	
fab_num	factory number of a cash register	
rcp_date	receipt date/time	

cash_rcp	document type	
sys	tax accounting system	
sess	shift number	
rcp_num	receipt number	
site	tax office webpage	
fiscal_doc	fiscal document	
fiscal_sign	fiscal signature	
device_num	terminal number	
qr	parameters line for QR code generating (to check the info on tax office webpage following the code link by mobile app)	

Information on each fiscal receipt may come after a while since the payment has obtained the appropriate status (OK, reversal, authorise, unblocked).

- in case of an error (status = error):

Name	Description	Examples	Notes
errorcode	error code	312	Error codes list is provided in Appendix 2 of this document
errortext	error text message	payment amount specified incorrectly	
processing_code	payment denial code received from the bank (Response Code according to ISO 8583)		
processing_text	reason for payment denial		

If appinfo parameter was equal to 1 in the payment status request and payment for the corresponding transaction was made with a bank card, in response to the request (in case of transaction status): OK, reversal, authorise, unblocked or error) transmission of additional parameters specified in the table for Information on payment made is performed. If the transaction status is equal to an error, transmission of additional parameters is performed only if the transaction is rejected due to anti-fraud policy rules.

- if no information on the payment status has been received from the payment system at the moment of the response generating (status = wait):

Name	Description	Examples
number	duplicates the value of the original request	Invoice5412

Examples. json-responses in each of the abovementioned cases:

when the operation is successful (OK):

```
{"status":"OK", "transID":"140000014", "finalamount":"418.20", "time": "2008-04-13T17:29:39+04:00", "number":"2217606",
"PAN":"400000******0000", "cardholder":"CARDHOLDER NAME"}
```

when the operation is successful (OK) and appinfo parameter (=1):

```
{"status":"OK", "transID":"140000014", "finalamount":"418.20", "time": "2008-04-13T17:29:39+04:00", "number":"2217606",
"PAN":"400000******0000", "cardholder":"CARDHOLDER NAME",

"binName":"MAX-BANK", "binCountry":"RU", "binPhone":"74950000000", "binPrepaid":"No", "ipCountry":"RU", "ipHighRisk":"No",

"ipRiskScore":"0.0", "mailFree":"Yes", "riskScore":"1.12"}
```

in case of an error (error):

```
{"status":"error", "errorcode":"113", "errortext": " The required amount is incorrect", "transID":"140000014",
"finalamount":"468.40"}
```

if no information on the payment status has been received from the payment system at the moment of the response generating (wait):

```
{"status":"wait", "transID":"140000014", "number":"2217606"}
```

Request for authorisation hold release

Request for authorisation hold release is done in 4g12hs Service making a POST-call at the address: https://fin.4g12hs.com/api/payment/operate

The following parameters must be set correctly:

Name	Description	Examples	Notes

opertype	fixed value – unblock	unblock	
account	Merchant Account Number in 4g12hs System		
transID	transaction number	15431522	
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters opertype, account, transID, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

Request results in a json-response containing the following parameters:

status

[additional parameters]

Parameter status may contain one of the following values:

- OK (operation successfully completed)
- error (operation execution error)

Additional parameters:

- when the operation is successful (status = OK):

Name	Description	Examples	Notes
PAN	bank card masked number	400000******0000	PAN and cardholder parameters are returned only if the payment was made with a bank card
cardholder	cardholder name	CARDHOLDER NAME	PAN and cardholder parameters are returned only if the payment was made with a bank card

- in case of an error (status = error):

Name	Description	Examples	Notes
errorcode	error code	331	Error codes list is provided in Appendix 2 of this document
errortext	error text message	charge amount specified incorrectly	
processing_code	payment denial code received from the bank (Response Code according to ISO 8583)		
processing_text	reason for payment denial		

If a Merchant is connected to the fiscal mode, then after successful payment 4g12hs Service will send a fiscal receipt to the client by e-mail. E-mail address for sending a fiscal receipt can be filled by a payer in the payment form on a webpage of our service or forwarded from a Merchant.

Examples. json-responses in each of the abovementioned cases:

when the operation is successful (OK):

```
{"status":"OK", "PAN":"400000******0000", "cardholder":"CARDHOLDER NAME"}
```

in case of an error (error):

```
{"status":"error", "errorcode":"135", "errortext": " Release of this transaction is not possible", "transID":"140000014"}
```

Request for authorization hold charge

Request for authorization hold charge is done in 4g12hs Service making a POST-call at the address: https://fin.4g12hs.com/api/payment/operate

The following parameters must be set correctly:

Name	Description	Examples	Notes
opertype	fixed value – terminate	terminate	
amountterminate	charge amount	150.20	The charge amount is indicated in the currency transmitted in the primary payment request sent by a Merchant (amountcurr parameter)
account	Merchant Account Number in 4g12hs System		
transID	transaction number	15431522	

signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters opertype, amountterminate, account, transID, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

Request results in a json-response containing the following parameters:

status

[additional parameters]

Parameter status may contain one of the following values:

- OK (operation successfully completed)
- error (operation execution error)

Additional parameters:

- when the operation is successful (status = OK):

Name	Description	Examples	Notes
PAN	bank card masked number	400000******0000	PAN and cardholder parameters are returned only if the payment was made with a bank card
cardholder	cardholder name	CARDHOLDER NAME	PAN and cardholder parameters are returned only if the payment was made with a bank card

- in case of an error (status = error):

Name	Description	Examples	Notes
errorcode	error code	331	Error codes list is provided in Appendix 2 of this document
errortext	error text message	charge amount specified incorrectly	
processing_code	payment denial code received from the bank (Response Code according to ISO 8583)		
processing_text	reason for payment denial		

If a Merchant is connected to the fiscal mode, then after successful payment 4g12hs Service will send a fiscal receipt to the client by e-mail. E-mail address for sending a fiscal receipt can be filled by a payer in the payment form on a webpage of our service or forwarded from a Merchant.

Examples. json-responses in each of the abovementioned cases:

when the operation is successful (OK):

```
{"status":"OK", "PAN":"400000******0000", "cardholder":"CARDHOLDER NAME"}
```

in case of an error (error):

```
{"status":"error", "errorcode":"120", "errortext": "Charge amount exceeds hold amount", "transID":"140000014"}
```

Request for full/partial refund

Full/partial refund request to the 4g12hs Service is made with POST-call at the address: https://fin.4g12hs.com/api/payment/operate

The following parameters must be set correctly:

Name	Description	Examples	Notes
opertype	fixed value – reversal	reversal	
amountreversal	refund amount	50.20	The refund amount is indicated in the currency transmitted in the primary payment request sent by a Merchant (amountcurr parameter)
account	Merchant Account Number in 4g12hs System		
transID	transaction number	15431522	
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters opertype, amountreversal, account, transID, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

Request results in a json-response containing the following parameters:

status

finalamount

[additional parameters]

Parameter status may contain one of the following values:

- OK (operation successfully completed)
- error (operation execution error)

Parameter finalamount contains the transaction amount including all partial refunds.

Additional parameters:

- when the operation is successful (status = OK):

Name	Description	Examples	Notes
PAN	bank card masked number	400000******0000	PAN and cardholder parameters are returned only if the payment was made with a bank card
cardholder	cardholder name	CARDHOLDER NAME	PAN and cardholder parameters are returned only if the payment was made with a bank card

- in case of an error (status = error):

Name	Description	Examples	Notes
errorcode	error code	335	Error codes list is provided in Appendix 2 of this document
errortext	error text message	refund amount specified incorrectly	
processing_code	payment denial code received from the bank (Response Code according to ISO 8583)		
processing_text	reason for payment denial		

If a Merchant is connected to the fiscal mode, then after successful payment 4g12hs Service will send a fiscal receipt to the client by e-mail. E-mail address for sending a fiscal receipt can be filled by a payer in the payment form on a webpage of our service or forwarded from a Merchant.

Examples. json-responses in each of the abovementioned cases:

when the operation is successful (OK):

```
{"status":"OK", "finalamount":"418.20", "PAN":"400000******0000", "cardholder":"CARDHOLDER NAME"}
```

in case of an error (error):

```
{"status":"error", "errorcode":"335", "errortext": "Refund amount specified incorrectly", "finalamount":"468.40",
"transID":"140000014"}
```

Recurring payment request

Recurring payment request to the 4g12hs Service is made by POST-call at the address: https://fin.4g12hs.com/api/payment/operate

The following parameters must be set correctly:

Name	Description	Examples	Notes
opertype	fixed value – recurring	recurring	
amountrecurring	recurring payment value	50.20	
account	Merchant Account Number in 4g12hs System		
transIDparent	ID number of transaction along with which recurring payment subscription was initiated	15431522	
recurringID	ID number for carrying out recurring payments (should be received when making a payment with trtype = 3 or 4)	11311211312	
numberrecurring	recurring payment's number for Merchant's record purposes (optional parameter)	54321	
descriptionrecurring	recurring payment's text description shown as URL-encoded string (optional parameter)	%37%31+%56%77	
cf1, cf2, cf3	user fields		

signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters opertype, amountrecurring, account, transIDparent, recurringID, numberrecurring, descriptionrecurring, cf1, cf2, cf3, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). If the parameters numberrecurring, descriptionrecurring pass empty string or are missing, they are not used to generate a digital signature and are not followed by a colon. If all the parameters cf1, cf2, cf3 pass an empty string or are missing, they are not used to generate a digital signature and are not followed by a colon. To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

Request results in a json-response containing the following parameters:

status

[additional parameters]

Parameter status may contain one of the following values:

- OK (operation successfully completed)
- error (operation execution error)

Additional parameters:

- when the operation is successful (status = OK):

Name	Description	Examples
PAN	bank card masked number	400000******0000
cardholder	cardholder name	CARDHOLDER NAME
numberrecurring	recurring payment's number for Merchant's record purposes (if transmitted in the original request)	54321
descriptionrecurring	recurring payment's text description shown as URL-encoded string (if transmitted in the original request)	%37%31+%56%77
transIDrecurring	recurring payment transaction number	15431525

- in case of an error (status = error):

Name	Description	Examples	Notes
errorcode	error code	344	Error codes list is provided in Appendix 2 of this document
errortext	error text message	making a recurring payment is not possible	
processing_code	payment denial code received from the bank (Response Code according to ISO 8583)		
processing_text	reason for payment denial		

Examples. json-responses in each of the abovementioned cases:

when the operation is successful (OK):

```
{"status":"OK", "PAN":"400000******0000", "cardholder":"CARDHOLDER NAME", "transIDrecurring":"15431525"}
```

in case of an error (error):

```
{"status":"error", "errorcode":"344", "errortext": "Making a recurring payment is not possible", "transID":"140000014"}
```

Request for billing a payer via Email/SMS

Information transmission to 4g12hs Service for billing by e-mail/SMS is done by a POST-call at the following address: https://fin.4g12hs.com/api/payment/invoice

That said the following parameters must be set correctly (the «+/–» column indicates whether this parameter is mandatory):

Name	Description	+/–	Examples	Notes
amount	product price in the payment currency (amountcurr)	+	100, 100.2, 100.25	
amountcurr	payment currency used to denominate the payment amount (amount)	+	RUB	

paysys	payment method code used to make a payment	+	MBC	
number	Merchant’s unique internal order number (a string of up to 32 characters); valid characters are: 0-9a-zA-Za-яA-Я, hyphen (“- “), dot (“.”), slash (‘”/”) and space	+	Invoice5412	
description	text order description shown as URL-encoded string (minimum - 6 characters)	+		
validity	date until which the invoice can be paid in the format of YYYY-MM-DDThh:mm:ss±hh:mm (in case the date is not set, Merchant's general settings are used)	–	2017-03-23T12:33:06+03:00	
first_name	payer’s first name	+	John, Customer	
last_name	payer’s last name	–		
middle_name	payer’s middle name	–		
email	payer’s email address	–		
notify_email	1 - send the invoice by e-mail; 0 - do not send it (if the email parameter is specified, then this one becomes mandatory)	–	1	
phone	payer's mobile phone in international format without spaces and "+" sign	–	79991111111	
notify_phone	1 - send the invoice by SMS; 0 - do not send it (if the phone parameter is specified, then this one becomes mandatory)	–	1	
backURL	the parameter allows to specify Merchant website's return URL other than the one specified in Merchant User Account	–		
account	Merchant Account Number in 4g12hs System (is issued upon registration and displayed in Merchant User Account)	+		
cf1, cf2, cf3	user fields	–		
signature	digital signature	+		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters amount, amountcurr, paysys, number, description, validity, first_name, last_name, middle_name, cf1, cf2, cf3, email, notify_email, phone, notify_phone, backURL, account, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). If the parameters email, phone pass an empty string or are missing, they as well as their corresponding parameters notify_email, notify_phone are not used to generate a digital signature and are not followed by a colon. If all the parameters cf1, cf2, cf3 pass an empty string or are missing, they are not used to generate a digital signature and are not followed by a colon. To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

All the parameters must be transmitted in UTF-8 encoding.

Request results in a json-response containing the following parameters:

status

[additional parameters]

Parameter status may contain one of the following values:

- wait (invoice issued successfully, waiting for payment)
- error (operation execution error)

Additional parameters:

- when the operation is successful (status = wait):

Name	Description	Examples	Notes
transID	transaction number	15431522	This number is used for all subsequent payment status clarification requests.
number	contains the value of this field sent in a request		
payURL	URL which a payer must follow to pay an invoice		

- in case of an error (status = error):

Name	Description	Examples	Notes
errorcode	error code	397	Error codes list is provided in Appendix 2 of this document
errortext	error text message	It is not possible to issue an invoice	

Examples. json-responses in each of the abovementioned cases:

when the operation is successful (wait):

```
{"status":"wait","transID":"180005801","number":"1542021333", "payURL":
"https://fin.4g12hs.com/#/payment/proceed/12345678- 1234-1234-1234-1234567890ab"}
```

in case of an error (error):

```
{"status":"error", "errorcode":"397", "errortext": "It is not possible to issue an invoice", "transID":"180005801"}
```

Outgoing payments protocol

General operation procedure of the protocol:

- a Merchant makes a request to 4g12hs server to make an outgoing payment;
- 4g12hs server verifies the request for its correctness and sends a payment confirmation request to Merchant's server (at a predefined http address);
- in case of confirmation from Merchant's server 4g12hs server makes a payment attempt, the result of which is sent back to a Merchant's server
- afterwards a Merchant can send additional requests for status clarification of a completed payment

Request to 4g12hs server for making a withdrawal

Data concerning executing payment is transmitted to 4g12hs server by a POST-call at address: https://fin.4g12hs.com/api/payout/execute

The following parameters must be set correctly:

Name	Description	Examples	Notes
account	Merchant Account Number in 4g12hs System		
operator	code of a provider which account is being funded	visamc	
params	beneficiary account number	4276....2135	
amount	transaction amount	10	
amountcurr	transaction currency	RUB	
nonce	one-time (pseudo) random value in hex format, must be unique for each request	1234567890abcdef	
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters nonce, account, operator, params, amount, amountcurr, number, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). If the parameter nonce is missing in a request, than it is not followed by a colon in digital signature. If bank card number appears in payment parameters (params field), it should be in the linked line as follows: 6 first digits, 6 '*' characters and 4 last digits, for example: 411111******1111, regardless of card number length (14-19). To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

Php code fragment of making a withdrawal request.

```
<?
    $params = "427600000000213500";
    $masked_params = "427600******3500";

    $account = "11111111111";
    $operator = "visamc";
    $amount = "10.00";
    $amountcurr = "RUB";
    $number = "Invoice1234";
    $nonce = bin2hex(openssl_random_pseudo_bytes(32));
```

```
    $post = "account=$account&operator=$operator&ms=$params&amount=$amount&amountcurr=$amountcurr&number=$number&nonce=$nonce";
    $signature = "$nonce:$account:$operator:$masked_params:$amount:$amountcurr:$number";
    $signature .= ":secret_key_1:secret_key_2";
    $signature = strtoupper(md5($signature));
    $post .= "&signature=$signature";

    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL,"___");
    curl_setopt($ch, CURLOPT_POST, 1);
    curl_setopt($ch, CURLOPT_POSTFIELDS, $post);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    $res = curl_exec($ch);
    curl_close($ch);
    print $res;
?>
```

Request from 4g12hs server's side for withdrawal confirmation

If all the parameters in a payment request from a Merchant are transmitted correctly, 4g12hs server makes a POST-call at a predetermined Merchant server's address to confirm a transaction.

That said the following parameters are transmitted:

Name	Description	Examples	Notes
account, operator, params, amount, amountcurr, number	duplicate the original request values		
transID	transaction number assigned to the payment on 4g12hs server	15431522	To prevent a failure to obtain (e.g. due to connectivity issues) this number properly (by initial request response), it is recommended to save it on merchant's server at this stage already
datetime	current date/time	2015-03-23 12:33:06.469763	
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters account, operator, params, amount, amountcurr, number, transID, datetime, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). If bank card number appears in payment parameters (params field), it should be in the linked line as follows: 6 first digits, 6 '*' characters and 4 last digits, for example: 411111******1111, regardless of card number length (14-19). To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

If the transaction is approved, Merchant's server in a response to this request must send a combination of characters "OK" (two capital Latin letters without quotes). In case of any other response, the operation will be denied.

Request's analysis on the server of an online store (php).

```
<?
$account = $_POST["account"];
$operator = $_POST["operator"];
$params = $_POST["params"];
$amount = $_POST["amount"];
$amountcurr= $_POST["amountcurr"];
$number = $_POST["number"];
$transId = $_POST["transId"];
$datetime = $_POST["datetime"];
$signature = $_POST["signature"];

// Performing actions to determine correctness
// of transmitted parameters

if (Payment must be made)
{
print "OK"; exit(-1);
}
```

```
else print "No, thanks";    // to cancel the payment
                            // any sequence of symbols
                            // can be returned
?>
```

Current balance request

Request is sent to 4g12hs server by a POST-call at address: /api/payout/balance:

Name	Description	Examples	Notes
account	Merchant Account Number in 4g12hs System	ACC123456	
nonce	one-time (pseudo) random value in hex format, must be unique for each request	1234567890abcdef	
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters nonce, account, secret_key_1, secret_key_2. To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm. The hash type is subject to the corresponding setting in Merchant User Account.

Php code fragment of making a current balance request

```
$nonce = bin2hex(openssl_random_pseudo_bytes(32));
$post = "account=$account&nonce=$nonce";
$signature = "$nonce:$account";
$signature .= ":secret_key_1:secret_key_2";
$signature = strtoupper(md5($signature));
$post .= "&signature=$signature";
```

Operation result sent by 4g12hs Server in a reply to withdrawal processing request

Request results in a json-response containing the following parameters:

status

[additional parameters]

Parameter status may contain one of the following values:

- OK (operation successfully completed): this status is a terminal one
- error (operation execution error); this status is a terminal one
- wait (pending confirmation from provider's server): this status is non-terminal

Additional parameters:

- when operation is successful (OK):

Name	Description	Examples
transID	transaction number assigned to the payment on 4g12hs server	15431522
time	operation completion time	2015-03-23 12:33:06.469763
number	duplicates the value of the original request	Invoice1234
amount	amount requested for withdrawal	100500.25
amountcurr	transaction currency	RUB
status	operation status	OK

- in case of an error (error):

Name	Description	Examples
errorcode	error code	312
errortext	error text message	Account number is specified incorrectly
transID	transaction number assigned to the payment on 4g12hs server	15431522
number	duplicates the value of the original request	1234
status	operation status	error

- in cases when at the moment of forming the response no information on payment status has been received (waiting):

Name	Description	Examples

transID	transaction number assigned to the payment on 4g12hs server	15431522
number	duplicates the value of the original request	1234
status	operation status	wait

Additional requests to 4g12hs server on a status of withdrawal made

If during the execution of a payment request no response has been received from 4g12hs server regarding successful or unsuccessful completion of payment, as well as in other cases, Merchant's server can send additional requests for current status of payment.

The request is transmitted with a POST-call at the address: https://fin.4g12hs.com/api/payout/status

That said the following parameters must be set correctly:

Name	Description	Examples	Notes
account	Merchant Account Number in 4g12hs System		
number	duplicates the value of the original request	1234	The parameter is optional, if transID parameter is transmitted
transID	transaction number assigned to the payment on 4g12hs server	15431522	The parameter is optional, if number parameter is transmitted
nonce	one-time (pseudo) random value in hex format, must be unique for each request	1234567890abcdef	
signature	digital signature		Digital signature is generated by the following rule: the operator *colon* is used to concatenate the parameters nonce, account, number, transID, secret_key_1 (is issued for a Merchant upon registration), and secret_key_2 (specified by a Merchant in User Account). The request may contain transID, number parameters together or individually (e.g. if transID was not received in case of network failure). If one of the parameters does not appear in the request, an empty value with a colon symbol should be anyway in its place in the digital signature. If the parameter nonce pass an empty string or is missing, it is not used to generate a digital signature and is not followed by a colon. To get a concatenated string one of the following hashes is calculated: 1) md5; 2) HMAC (sha256 algorithm) (to generate a hash the System uses a key formed by concatenating the keys: secret_key_1 and secret_key_2 without any additional characters in-between). The hash type is subject to the corresponding setting in Merchant User Account.

The format of 4g12hs server's responses is completely identical to the formats in the previous paragraph of this description, except that the transID parameter always comes back when an error occurs.

Appendix 1. Error codes returned by the script api/payment/*

Error code	Error description
-19	3DS authentication failed
05	Declined, contact card issuer
06	Suspected Fraud (Contact Acquirer)
14	Invalid Card Number
17	Cancelled by Customer
51	Insufficient Funds
54	Expired card
57	Restrictions on payment
61	Exceeds withdrawal limit
62	Restricted Card
63	Denial for security reasons
65	Exceeds transactions limit
68	Response Received Too Late / Timeout
92	Payment system error
96	System failure
130	Confirmation from a Merchant has not been received
131	Unsupported confirmation format from a Merchant
135	Manual status adjustment

137	Transaction execution timeout expired
221	Transaction amount does not match

The documentation lists only the main errors that are returned during operation. Other return codes may also appear.

Appendix 2. Error codes returned by the script api/payout/*

Error code	Error description
127	Payment declined
224	Currency is not allowed for the merchant
302	Translation with transmitted identifier is not found

The documentation lists only the main errors that are returned during operation. Other return codes may also appear.

Appendix 3. Possible Processing codes

Full list of error codes (ISO 8583):	
00	Successfully completed
01	Refer to card issuer
02	Refer to card issuer's special condition
03	Invalid merchant / source
04	PICK UP
05	Do not Honour
06	Error
07	Pick-up card, special condition
08	Honour with identification
09	Request in progress
10	Approved for partial amount
11	Approved (VIP)
12	Invalid transaction
13	Invalid amount
14	No such card
15	No such issuer
16	Approved, update track 3
17	Customer cancellation
18	Customer dispute
19	Re-enter transaction
20	Invalid response
21	No action taken
22	Suspected malfunction
23	Unacceptable transaction fee
24	File update not supported by receiver
25	No such record
26	Duplicate record update, old record replaced
27	File update field edit error
28	File locked out while update
29	File update error, contact acquirer

30	Format error
31	Issuer signed-off
32	Completed partially
33	Pick-up, expired card
34	Suspect Fraud
35	Pick-up, card acceptor contact acquirer
36	Pick up, card restricted
37	Pick up, call acquirer security
38	Pick up, Allowable PIN tries exceeded
39	No credit account
40	Requested function not supported
41	Pick up, lost card
42	No universal account
43	Pick up, stolen card
44	No investment account
50	Do not renew
51	Not sufficient funds
52	No chequing account
53	No savings account
54	Expired card / target
55	Incorrect PIN
56	No card record
57	Transaction not permitted to cardholder
58	Transaction not permitted to terminal
59	Suspected fraud
60	Card acceptor contact acquirer
61	Exceeds withdrawal amount limit
62	Restricted card
63	Security violation
64	Wrong original amount
65	Exceeds withdrawal frequency limit
66	Call acquirers security department
67	Card to be picked up at ATM
68	Response received too late
70	Invalid transaction; contact card issuer
71	Decline PIN not changed
75	Allowable number of PIN tries exceeded
76	Wrong PIN, number of PIN tries exceeded
77	Wrong Reference No.
78	Record Not Found
79	Already reversed
80	Network error
81	Foreign network error / PIN cryptographic error
82	Time-out at issuer system / Bad CVV (VISA)
83	Transaction failed
84	Pre-authorization timed out

85	No reason to decline
86	Unable to validate PIN
87	Purchase Approval Only
88	Cryptographic failure
89	Authentication failure
90	Time-out at issuer system / Bad CVV (VISA)
91	Issuer or switch is inoperative/Issuer unavailable
92	Unable to route at acquirer module
93	Cannot be completed, violation of law
94	Duplicate Transmission
95	Reconcile error / Auth Not found
96	System Malfunction
-2	Bad CGI request
-3	No or Invalid response received
-4	Server is not responding
-5	Connect failed
-6	Configuration error
-8	Error in card number field
-9	Error in card expiration date field
-10	Error in amount field
-11	Error in currency field
-12	System error
-12	Error in merchant terminal field
-15	Invalid Retrieval reference number
-16	Terminal is locked, please try again
-17	Access denied
-18	Error in CVC2 or CVC2 Description fields
-19	Authentication failed
-19	System error
-20	Expired transaction
-21	Duplicate transaction
-26	System error
-26	Invalid action BIN
-29	Invalid/duplicate authentication reference
-29	System error

Appendix 4. Test cards (for test environment!)

To make payments in the test environment, use the following test card details:

Card number	Valid thru	CVV	Description
4111111111111111	2030/12	123	successful payment with 3DS
4111111111100023	2030/12	123	successful payment without 3DS
4111111111111112	2030/12	123	recurring payment

Document revision history

Version	Date	Changes description
0.931	26.01.2015	–
0.932	22.03.2015	1. art. 4.2: unlock request information was added (unblock). 2. Hold amount release request was added 3. In sections. 4.9 and 4.10 the order of the parameters in generating of a digital signature was corrected (first account, after transID).
0.94	23.03.2015	Parameter datetime was added (current date/time) when 4g12hs sends confirmation transactions requests (section. 4.2) and transactions performed requests (section. 4.4). This parameter was also included into the values list used for digital signature generating (signature), before secret key values.
0.941	26.03.2015	1. A clarification was added that all the parameters must be transmitted in UTF-8 encoding. 2. In transmission of parameters description and trtype were added, these parameters are also included into the digital signature.
0.942	29.03.2015	In art. 4.7: – Parameters order of digital signature generating was corrected, when generating signature, a parameter transID goes after account; – unblocked status description was added – a clarification was added: multiple refunds should be supported by acquiring bank; – a clarification added: what additional parameters return upon the statuses reversal, authorise and unblocked.
0.943	25.07.2015	1.In art. 4.4: – Was added a parameters table regarding anti-fraud information about transactions – Information was added that repeated call statusURL (in case when the reply OK isn't received) is being carried out provided the respective option is turned on in Merchant User Account 2. In art. 4.6 appinfo parameter was added 3. In art. 4.7: – the information was added that if the parameter appinfo is set (=1) then additional parameters return provided a transaction has one of the following statuses: OK, reversal, authorise, unblocked, error; – an example of additional parameters waas given when the parameter appinfo is set (=1).
0.95	27.07.2015	1. In art. 4.1: – item 4.1.1 was highlighted; – item 4.1.2 was highlighted. 2. In art. 4.2: – the table of the parameters which are transmitted upon the request described in art. 4.1.1 was highlighted; – the table of the parameters which are transmitted upon the request described in в art. 4.1.2 was added.
0.962	21.10.2015	1. In subparagraphs 4.1.1, 4.1.2 values 3 and 4 of a parameter trtype were described. 2. In subparagraphs 4.1.1, 4.1.2, 4.2, 4.4 parameters recurringFrequency and recurringEndDate were added. 3. In section 4.2 a confirmation request for recurring payment was added. 4. In subparagraphs 4.4, 4.7 a parameter recurringID was added. 5. In section 4.5 a parameter account was added to the parameters list and to the example. 6. Section. 4.11 was added. 7. Information from art. 3 was corrected.
0.963	16.11.2015	1. The parameters PAN, expmonth, expyear, cardholder, securecode. were excluded from signature generating rule in section 4.1.2 2. The wording of the first sentences is corrected in subparagraphs. 4.8, 4.9, 4.10, 4.11.
0.964	14.06.2016	Possibility of parameter cardkey usage was added in subparagraphs 4.1.1, 4.1.2, 4.2, 4.4, 4.7. An note on optionality of the parameters PAN, expmonth, expyear, cardholder was added in art. 4.1.2
0.965	29.06.2016	Digital values when calculating commissions in cases (2) and (3) were corrected in art. 3 A clarification on acceptable symbols into the field number was added in subparagraph. 4.1.1-4.1.2 In subparagraphs. 4.2 (request for carrying out a recurring payment), 4.11 parameters numberrecurring, descriptionrecurring were added; rules of parameter signature were corrected. Information that a value of the parameter transIDrecurring must be returned when requesting for confirmation of making a recurring payment was added in section 4.2 Description of statusURL was added in section 4.4 Field's time format was corrected in art section 4.7 A parameter finalamount was added in subparagraphs 4.7 и 4.10. Parameters were corrected.
0.966	12.07.2016	Parameter's name cardkey was changed to paytoken in subparagraphs 4.1.1, 4.1.2, 4.2, 4.4, 4.7 A parameter lang was added in subparagraphs. 4.1.1, 4.1.2; a rule of digital signature generating was corrected.
0.967	22.08.2016	The description and the list of acceptable parameters of the lang parameter were corrected in subparagraphs 4.1.1-4.1.2; also, this parameter was excluded from the digital signature.

0.968	27.09.2016	Item 4.1.3 was added. Request description when making a call described in art. 4.1.3 was added in art. 4.2 Subparagraphs 4.3.1 and 4.3.2 were highlighted in 4.3
0.969	09.10.2016	Subparagraph 4.1.1-4.1.3: an optional parameter email was added to the list of transmitted parameters sent in the request. Subparagraph. 4.1.3: the parameters ip_address, user_agent, accept_language were added into the parameters list transmitted in the request. Subparagraph. 4.3.2: the parameter PARes was changed to PaRes. Section. 4.7: parameters amount and amountcurr were added into the returned parameters list.
0.970	27.06.2017	Description of status authorize was corrected in subparagraph 4.3.2. section. 4.4: – A recommendation was added to perform a payment status request for each payment initiated by a Merchant that does not have a successful status. – Information was added on sending a fiscal receipt to a payer if a Merchant is connected to the fiscal mode. – Text of the example was corrected section. 4.7: – Descriptions of statuses authorise and – unblocked were corrected; – parameters list returned to a Merchant in case a transaction has one of these statuses OK, reversal, authorise, unblocked, was added provided a Merchnat has fiscal mode connected. Art. 4.8: Was added an information on sending a new fiscal receipt to a payer if a Merchant is connected to the fiscal mode. Art. 4.9: Was added an information on sending a new fiscal receipt to a payer in case a Merchant is connected to the fiscal mode and the charge amount is other than the authorised one. Art. 4.10: Was added an information on sending a new fiscal receipt to a payer if a Merchant is connected to the fiscal mode.
0.971	30.08.2017	Text of the examples from sections. 4.1.1, 4.1.2, 4.2 was corrected.
0.973	26.07.2018	In subparagraphs. 4.1.1-4.1.3: a clarification was added that a Merchant can issue invoices only in one of the currencies previously specified for it (amountcurr parameter). Information about parameters conversion_amount, conversion_currency and conversion_rate was added in the section III.2 when making the calls described in subparagraphs. 4.1.1-4.1.3, 4.9, 4.10. Additional parameters list (conversion_amount, conversion_currency, conversion_rate) and information about their transmission were added in the section 4.7 In section 4.9: was added a clarification that charge currency is indicated in the currency transmitted in the initial payment request transmitted from a Merchant (amountcurr parameter). In section 4.10 was specified that refund amount shall be indicated in the currency transmitted in the initial payment request from a Merchant (amountcurr parameter).
0.974	13.11.2018	In art. 4 clarification was added that an invoice may be issued via email/SMS. Was added art. 4.12.
0.975	23.03.2019	In sections 4.1.1-4.1.3, 4.11, 4.12 and also in section 4.2 (for the requests described in sections. 4.1.1-4.1.3, 4.11) was added the information on possibility of parameters cf1, cf2, cf3 transmission and their inclusion to digital signature (signature parameter). Addresses for redirecting/sending a request were corrected in sections 4.1.2-4.1.3 Information that the minimum length of description filed shouldn't be less than 6 symbols was added in the sections 4.1.1-4.1.3 и 4.12 Sections 4.1.5 и 4.1.6 were added In section 4.2 information was added that the confirmation of the request 4.1.5 is similar to the confirmation of the request 4.1.3. Other minor corrections were also made. Sections 4.3.3 и 4.3.4 were added In sections 4.3.2, 4.7-11 parameters processing_code and processing_text were added to the list of additional parameters returned in case of an error.
0.976	05.08.2019	In point 2, information about the protocol for making outgoing payments were added. A missing paytoken parameter was added to the digital signature generation rule in section 4.4. Added art 5 (Protocol for making outgoing payments); to the numbers of subsequent items (except the art. 6) one more unit added.
0.977	30.01.2020	Items of registration 4.1.8 and payment completion 4.1.9 requests for Google Pay method were added Appendix 3 with card data for making payments in a test environment was added Description of the parameter 'recurringFrequency' was added into paragraph 4.1 (information about the value of the parameter in case of irregular charges)
0.978	06.03.2020	The list of payment methods supported by the merchant interface was added art. 3.1 Section 4.1.4 is added. The description of the request on payment execution without switching to a site of 4g12hs Service using the protected data transmission of a card (cryptogram checkout). In item 4.1.5 a description of the request to register a payment by ApplePay method was added
0.979	24.04.2020	Paragraph 5 has been amended on protocol parameters for making payments Appendix 1 and Appendix 2 - tables with error codes were completed
0.980	11.02.2021	In section 4.1.2 address for POST-call is corrected; Notes on signature are revised, too - backURL parameter is added.

		In section 4.2 example of a request for transaction confirmation is updated; descriptions of authorize and error values are revised. In section 4.6 descriptions of authorize and error values are revised; Notes on number are updated. In section 4.7 status: "wait" and additional parameter step with description of values are added. In section 4.11 parameter numberrecurring now described. In section 5 description of current balance request is added.
0.981	11.02.2021	Appendix 3 Test cards renamed into Appendix 4. Appendix 3 Possible Processing codes was added.

Нет меток