

Payment Center API
WEBFORM/GATEWAY MODE
v2.6.2

Content

Introduction	3
WebPay (webform)	4
WebBlock (webform)	6
Pay (gateway)	4
Block (gateway)	6
Token (gateway)	6
Charge (webform/gateway)	7
Cancel (webform/gateway)	8
Refund (webform/gateway)	9
Rebill (webform/gateway)	10
Ack3DS (gateway)	11
Status (webform/gateway)	12
Unsubscribe (webform/gateway)	13
Check (webform/gateway)	13
3D-Secure authentication	14
Webhooks	15
Payment	15
Fail	16
Refund	16
Void	17
Receipt	17
Repeating of webhook notifications	18
Signature	18

Introduction

Payment Center API enables to perform the basic set of operation with payments by providing bank card details on the merchant's page.

- **WebPay (webform)** – one-step payment operation – funds are deducted from the card immediately after execution.
- **WebBlock (webform)** – two-step payment operation – funds are blocked on the card.
- **Pay (gateway)** – one-step payment operation – funds are deducted from the card immediately after execution.
- **Block (gateway)** – two-step payment operation – funds are blocked on the card.
- **Token (gateway)** – token generation for the payment operation via the link.
- **Charge (webform/gateway)** – funds deduction from the card within the two-step payment operation executed earlier.
- **Cancel (webform/gateway)** – unblock funds on the card (partial or full).
- **Refund (webform/gateway)** – funds refund operation to the card (partial or full), is possible only after funds deducting.
- **Rebill (webform/gateway)** – the operation of automatic funds deduction from a previously "linked" card.
- **Ack3DS (gateway)** – is used by one-step / two-step payment operation in case if the operation is performed using 3D Secure.
- **Status (webform/gateway)** – an operation for getting the payment status.
- **Unsubscribe (webform/gateway)** – unsubscribe from a recurring payment.
- **Check (webform/gateway)** – checking of a subscription to a recurring payment.

WebPay (webform)

One-step payment operation - funds are deducted from the card immediately after the operation is carried out. There is a possibility to specify a **rebillFlag** to pre-authorize a recurring payment.

The **WebPay** request format is: [https:// secured.payment.center/v2/webpay](https://secured.payment.center/v2/webpay) (POST-request).

Description of the **WebPay** request parameters:

Parameter	Format	Required	Description
serviceld	Int(12)	Yes	Partner service ID. 1 to 12 digits with no spaces or delimiters.
orderId	String(100)	Yes	Unique order identifier in the Partner system.
amount	Int(12), symbol '.'	Yes	Amount to be paid. From 1 to 12 digits, can contain a decimal separator in the form of a dot '.'.
currency	String(3)	Yes	Currency in ISO format (USD, EUR, RUB...). Characters (a-zA-Z).
description	String(250)	Yes	Transaction description.
email	String	No*	Email of the customer. Required for recurring payments. This email should not be sent to the bank. This email is to notify the Customer only. It is saved in the transaction.
phone	String(10-20), ahead '+'	No*	Phone of the customer. In the international format +79991231212 (with no spaces).
lang	String(2)	No	Language designation in ISO format (for example, en, ru...).
customFields	String(8096)	No	Additional transaction fields.
extra	String(2000)	No	Additional parameters. JSON array. It can contain parameters (the first 3 are required): success_url – the URL redirecting from the 'success' page; decline_url – the URL redirecting from the 'error' page; cancel_url – the URL to return back (button 'Back'); account_id – to return directly to the client's personal area. Example: {"success_url": "http://server1.com/", "decline_url":

			"http://server2.com/", "cancel_url": "http://server3.com/", "account_id": "1122aass112"}
rebillFlag	Bit	No	A flag of a recurring payment. The possible values are 0 or 1.
address	String(200)	No	Address of the cardholder, indicated by registration of the card in bank. Can be present if verification of the cardholder's address is supported.
town	String(200)	No	City of the cardholder, indicated by registration of the card in bank. Can be present if verification of the cardholder's address is supported.
zip	String(20)	No	Zip code of the cardholder, indicated by registration of the card in bank. Can be present if verification of the cardholder's address is supported.
country	Int(3)	No	Country code in ISO format, specified by a card registration.

* parameter is required depending on the gate (contact your manager for more information).

WebBlock (webform)

The two-step payment operation – funds are blocked on the card. There is a possibility to specify a **rebillFlag** to pre-authorize a recurring payment.

The format of **WebBlock** request is: <https://secured.payment.center/v2/webblock> (POST request).

The list of parameters in a request is identical to the one in **WebPay** operation.

Pay (gateway)

One-step payment operation – funds are deducted from the card immediately after execution. In addition, there is a possibility to specify a **rebillFlag** for pre-authorize of a recurring payment.

The **Pay** request format is: <https://secured.payment.center/v2/pay> (POST-request with the parameter **signature** in the header - digital signature, required parameter).

Description of **Pay** request parameters:

Parameter	Format	Required	Description
serviceld	Int(12)	Yes	Partner service ID. From 1 to 12 digits with no spaces and delimiters.
cardNumber	Int(12-19)	Yes	Card number. From 12 to 19 digits without spaces.
expMonth	Int(2)	Yes	Month of card expiration. 2 digits with leading zero.
expYear	Int(2)	Yes	Year of card expiration. The last 2 digits of the year.
cardHolder	String(30)	Yes	The cardholder's name (on the front side of the card). Valid characters are [a-Z., -].
cvc	Int(3)	Yes	CVC2/CVV2. 3 digits.
orderId	String(100)	Yes	Unique order identifier in the Partner system.
amount	Int(12), symbol '.'	Yes	Amount to be paid. From 1 to 12 digits, can contain a decimal separator in the form of a dot '.'.
currency	String(3)	Yes	Currency in ISO format (USD, EUR, RUB). Letters (a-zA-Z).
description	String(250)	Yes	Transaction description.
email	String	No*	Email of the customer. Required for recurring payments. This email should not be sent to the bank. This email is to notify the Customer only. It is saved in the transaction.
phone	Int(10-20), ahead '+'	No*	Phone of the customer. In the international format +79991231212 (with no spaces).

lang	String(2)	No	Language designation in ISO format (for example, en, ru...).
customFields	String(8096)	No	Additional transaction fields.
rebillFlag	Bit	No	A sign of a recurring payment. The possible values are 0 or 1.
address	String(200)	No	Address of the cardholder, indicated by registration of the card in bank. Can be present if verification of the cardholder's address is supported.
town	String(200)	No	City of the cardholder, indicated by registration of the card in bank. Can be present if verification of the cardholder's address is supported.
zip	String(20)	No	Zip code of the cardholder, indicated by registration of the card in bank. Can be present if verification of the cardholder's address is supported.
country	Int(3)	No	Code of the country indicated by registration of the card in bank, in the ISO format.

* parameter is required depending on the gate (contact your manager for more information).

The response format to the **Pay** request is: XML string with a node **<v2PayResponse>** (in the header the parameter **signature** – digital signature, required parameter).

Description of the response parameters to the **Pay** request:

Parameter	Format	Required	Description
success	Reserved values	Yes	Flag of the operation success: true – if the operation succeeds, false – if an error occurs, 3DS – 3DS operation, REDIRECT – the response from the bank for a redirecting to the specified URL.
orderId	String(100)	Yes	Unique transaction ID in the Partner system.
tranId	Int(20)	Yes, in case of success=true	Transaction ID in the system.
amount	Int(12), symbol ‘.’	Yes, in case of success=true	Amount of payment. Is equal to the one sent in the request.
currency	String(3)	Yes, in case of success=true	The currency code in which the transaction was conducted in the bank.
gateAmount	Int(12), symbol ‘.’	Yes, in case of success=true	The amount of payment in the currency in which the transaction was conducted in the bank.
gateCurrency	String(3)	Yes, in case of success=true	The currency code in which the transaction was conducted in the bank.
tranStatus	Reserved values	Yes, in case of success=true	The current status of the transaction. The possible values are: new (open) – a new payment for which no transactions have been made, trusted – a new payment, checking with AntiFraud is passed, filtered – a new payment, that noted by AntiFraud as a fraud, preAuthorized3DS – the payment is waiting for the completion of 3DS authorization, preAuthorizedAF – the payment is waiting for confirmation from the cardholder, authorized – funds are blocked, voided – funds are unlocked, charged – funds are charged, refunded – refund is completed, rejected – payment is failed, error – the payment was completed with an error.
errCode	Reserved	Yes, in case of	Error code.

	values	success=false	
errMessage	Reserved values	Yes, in case of success=false	Error description.
rebillId	Int(20)	Her	The transaction ID for which the money will be re-deducted.
acsUrl	String	Yes, in case of success=3DS	URL for redirect.
paRes	String	Yes, in case of success=3DS	Encrypted request.
threeDSKey	String	Yes, in case of success=3DS	Special attribute.
redirectUrl	String	Yes, in case of success=REDIRECT	URL for redirect.
redirectParams	String	Yes, in case of success=REDIRECT	A string of parameters to redirect. The string format is 'parameter_name_1 = parameter_value_1 & parameter_name_2 = value_of_parameter_2 & ...'
redirectTransId	String	Yes, in case of success=REDIRECT	Transaction ID in the bank system.

Attention! By using **3D-Secure** authentication the operation format will change as it is described in the paragraph **3D-Secure Authentication**.

Block (gateway)

The two-step payment operation – funds are blocked on the card. There is a possibility to specify a **rebillFlag** to pre-authorize a recurring payment.

The format of **Block** request is: <https://secured.payment.center/v2/block> (POST-request with the parameter **signature** in the header - digital signature, required parameter).

The list of parameters in a request is identical to the one in **Pay** operation.

The format of the response to **Block** query is: xml string with node **<v2BlockResponse>** (in the header the parameter **signature** - digital signature, required parameter).

The list of parameters in the response is identical to **Pay** operation.

Attention! By using **3D-Secure** authentication the operation format will change as it is described in the paragraph **3D-Secure Authentication**.

Token (gateway)

Generating a **token** for processing payments through the link.

The format of **Token** request is: <https://secured.payment.center/v2/token> (POST-request with the parameter **signature** in the header - digital signature, required parameter).

The list of parameters in a request is identical to the one in **WebPay** operation.

The format of the response to **Token** request is: xml string with node **<v2TokenResponse>** (in the header the parameter signature - digital signature, required parameter).

Description of response parameters to the **Token** request:

Parameter	Format	Required	Description
success	Reserved values	Yes	Flag of the operation success: true – if the operation succeeds,

			false – if an error occurs.
token	String(32)	Yes, in case of success=true	Unique ID.
errCode	Reserved values	Yes, in case of success=false	Error code.
errMessage	Reserved values	Yes, in case of success=false	Error description.

Examples:

```
<v2TokenResponse><success>true</success><token>948b81dc18d296b25622a016bfe25a0</token></v2TokenResponse>
```

```
<v2TokenResponse><success>false</success><errcode>1</errcode><errmessage>Wrong parameters</errmessage></v2TokenResponse>
```

Using:

<https://secured.payment.center/v2/webpay/?token=948b81dc18d296b25622a016bfe25a0>

<https://secured.payment.center/v2/webblock/?token=948b81dc18d296b25622a016bfe25a0>

Charge (webform/gateway)

Deduction of funds from the card during the two-step payment operation executed earlier.

The format of the **Charge** request is: <https://secured.payment.center/v2/charge> (POST- request with the signature parameter in the header - digital signature, required parameter).

Description of **Charge** request parameters:

Parameter	Format	Required	Description
serviceld	Int(12)	Yes	Partner service ID. 1 to 12 digits with no spaces or delimiters.
tranId	Int(20)	Yes	Transaction ID in the system.
amount	Int(12), symbol '.'	No	Payment confirmation amount. The parameter does not exist when the full amount is confirmed.
currency	String(3)	No	Currency in ISO format (USD, EUR, RUB...). Characters (a-zA-Z).

The response format to **Charge** request is: xml string with node **<v2ChargeResponse>** (in the header the parameter **signature** - digital signature, required parameter).

Description of response parameters to the **Charge** request:

Parameter	Format	Required	Description
success	Reserved values	Yes	Flag of the operation success: true – if the operation succeeds, false – if an error occurs.
tranId	Int(20)	Yes	Transaction ID in the system.
amount	Int(12), symbol '.'	Yes, in case of success=true	Payment amount. Corresponds to the one sent in the request.
newAmount	Int(12), symbol '.'	Yes, in case of success=true	Remaining amount. With full confirmation, it will be equal to 0.
currency	String(3)	Yes, in case of success=true	Currency code of the transaction that was processed by the bank.
gateAmount	Int(12), symbol '.'	Yes, in case of	The payment amount in the currency of the transaction

		success=true	that was processed by the bank.
gateCurrency	String(3)	Yes, in case of success=true	Currency code of the transaction that was processed by the bank.
tranStatus	Reserved values	Yes, in case of success=true	The current status of transaction. The possible values are: new (open) — new payment with no transactions conducted yet, trusted — new payment that Antifraud check is passed, filtered — new payment that was marked as a fraud by AntiFraud, preAuthorized3DS — the payment is waiting on the completion of 3DS authorization, preAuthorizedAF — the payment is waiting for confirmation from the cardholder, authorized — funds are blocked, voided — funds are unlocked, charged — funds are charged, refunded — refund completed, rejected — payment failed, error — payment transaction was completed with an error.
errCode	Reserved values	Yes, in case of success=false	Error code.
errMessage	Reserved values	Yes, in case of success=false	Error description.
rebillId	Int(20)	No	The identifier of a recurring payment. It represents a transaction ID in the system.

Cancel (webform/gateway)

Unblocking funds on card (partial or full).

The format of the **Cancel** request: <https://secured.payment.center/v2/cancel> (POST- request with the **signature** parameter in the header - digital signature, required parameter)

Description of **Cancel** request parameters:

Parameter	Format	Required	Description
serviceld	Int(12)	Yes	Partner service ID. 1 to 12 digits with no spaces or delimiters.
tranId	Int(20)	Yes	Transaction ID in the system.
amount	Int(12), symbol '.'	Yes	Payment amount.
currency	String(3)	Yes	Currency in ISO format (USD, EUR, RUB...). Characters (a-zA-Z).

The format of the response to the **Cancel** request is: xml a string with the node **<v2CancelResponse>** (in the header the parameter **signature** - digital signature, a required parameter).

Description of response parameters to the **Cancel** request:

Parameter	Format	Required	Description
success	Reserved values	Yes	Flag of the operation success: true – if the operation succeeds, false – if an error occurs.
tranId	Int(20)	Yes	Transaction ID in the system.
amount	Int(12), symbol '.'	Yes, in case of success=true	Payment amount. Corresponds to the one sent in the request.
currency	String(3)	Yes, in case of	Currency code of the transaction that was processed by the bank.

		success=true	
gateAmount	Int(12), symbol '.'	Yes, in case of success=true	The payment amount in the currency of the transaction that was processed by the bank.
gateCurrency	String(3)	Yes, in case of success=true	Currency code of the transaction that was processed by the bank.
tranStatus	Reserved values	Yes, in case of success=true	The current status of transaction. The possible values are: new (open) — new payment with no transactions conducted yet, trusted — new payment that Antifraud check is passed, filtered — new payment that was marked as a fraud by AntiFraud, preAuthorized3DS — the payment is waiting on the completion of 3DS authorization, preAuthorizedAF — the payment is waiting for confirmation from the cardholder, authorized — funds are blocked, voided — funds are unlocked, charged — funds are charged, refunded — refund completed, rejected — payment failed, error — payment transaction was completed with an error.
errCode	Reserved values	Yes, in case of success=false	Error code.
errMessage	Reserved values	Yes, in case of success=false	Error description.

Refund (webform/gateway)

Funds get refunded to the card (partial or full), is possible only after the funds get deducted.

The format of the **Refund** request is: <https://secured.payment.center/v2/Refund> (POST-request with the **signature** parameter in the header - digital signature, required parameter).

Description of **Refund** request parameters:

Parameter	Format	Required	Description
serviceld	Int(12)	Yes	Partner service ID. 1 to 12 digits with no spaces or delimiters.
tranId	Int(20)	Yes	Transaction ID in the system.
amount	Int(12), symbol '.'	Yes	Refund amount.
currency	String(3)	Yes	Currency in ISO format (USD, EUR, RUB...). Characters (a-zA-Z).

The format of response to the **Refund** request is: xml string with node **<v2RefundResponse>** (in the header the parameter **signature** - digital signature, required parameter).

Description of response parameters to the **Refund** request:

Parameter	Format	Required	Description
success	Reserved values	Yes	Flag of the operation success: true – if the operation succeeds, false – if an error occurs.
tranId	Int(20)	Yes	Transaction ID in the system.
amount	Int(12), symbol '.'	Yes, in case of	Payment amount. Corresponds to the one sent in the

		success=true	request.
currency	String(3)	Yes, in case of success=true	Currency code of the transaction that was processed by the bank.
gateAmount	Int(12), symbol '.'	Yes, in case of success=true	The payment amount in the currency of the transaction that was processed by the bank.
gateCurrency	String(3)	Yes, in case of success=true	Currency code of the transaction that was processed by the bank.
newAmount	Int(12), symbol '.'	Yes, in case of success=true	Remaining amount.
tranStatus	Reserved values	Yes, in case of success=true	The current status of transaction. The possible values are: new (open) — new payment with no transactions conducted yet, trusted — new payment that Antifraud check is passed, filtered — new payment that was marked as a fraud by AntiFraud, preAuthorized3DS — the payment is waiting on the completion of 3DS authorization, preAuthorizedAF — the payment is waiting for confirmation from the cardholder, authorized — funds are blocked, voided — funds are unlocked, charged — funds are charged, refunded — refund completed, rejected — payment failed, error — payment transaction was completed with an error.
errCode	Reserved values	Yes, in case of success=false	Error code.
errMessage	Reserved values	Yes, in case of success=false	Error description.

Rebill (webform/gateway)

An operation of automatic funds deduction from a previously "linked" card.

The format of the **Rebill** request is: <https://secured.payment.center/v2/Rebill> (POST-request with the **signature** parameter in the header - digital signature, required parameter).

Description of **Rebill** request parameters:

Parameter	Format	Required	Description
serviceld	Int(12)	Yes	Partner service ID. 1 to 12 digits with no spaces or delimiters.
orderId	String(100)	Yes	Unique order identifier in the Partner system.
amount	Int(12), symbol '.'	Yes	Payment amount.
currency	String(3)	Yes	Currency in ISO format (USD, EUR, RUB...). Characters (a-zA-Z).
description	String(250)	No	Transaction description.
rebillId	Int(20)	Yes	The identifier of a recurring payment. It represents a transaction ID in the system.
usePaymentType	Bit	No	Flag of using a payment type of the parent transaction. The possible values are (by default is '0'): '1' — use a payment type of the parent transaction (BLOCK/PAY), '0' — don't use a payment type of the parent transaction (always PAY).

The format of response to the **Rebill** request is: xml string with node **<v2RebillResponse>** (in the header the parameter **signature** - digital signature, required parameter).

Description of response parameters to the **Rebill** request:

Parameter	Format	Required	Description
success	Reserved values	Yes	Flag of the operation success: true – if the operation succeeds, false – if an error occurs.
tranId	Int(20)	Yes	Transaction ID in the system.
amount	Int(12), symbol ‘.’	Yes, in case of success=true	Payment amount. Corresponds to the one sent in the request.
currency	String(3)	Yes, in case of success=true	Currency code of the transaction that was processed by the bank.
gateAmount	Int(12), symbol ‘.’	Yes, in case of success=true	The payment amount in the currency of the transaction that was processed by the bank.
gateCurrency	String(3)	Yes, in case of success=true	Currency code of the transaction that was processed by the bank.
tranStatus	Reserved values	Yes, in case of success=true	The current status of transaction. The possible values are: new (open) – new payment with no transactions conducted yet, trusted – new payment that Antifraud check is passed, filtered – new payment that was marked as a fraud by AntiFraud, preAuthorized3DS – the payment is waiting on the completion of 3DS authorization, preAuthorizedAF – the payment is waiting for confirmation from the cardholder, authorized – funds are blocked, voided – funds are unlocked, charged – funds are charged, refunded – refund completed, rejected – payment failed, error – payment transaction was completed with an error.
errCode	Reserved values	Yes, in case of success=false	Error code.
errMessage	Reserved values	Yes, in case of success=false	Error description.
rebillId	Int(20)	No	The identifier of a recurring payment. It represents a transaction ID in the system.

Ack3DS (gateway)

Is used by **Pay** or **Block** operations with 3DS Secure after receiving the results of authentication from the bank to complete a one-step\two-step payment operation.

The format of the **Ack3DS** request is: <https://secured.payment.center/v2/ack3ds> (POST-request with the signature parameter in the header - digital signature, required parameter).

Description of **Ack3DS** request parameters:

Parameter	Format	Required	Description
serviceld	Int(12)	Yes	Partner service ID. 1 to 12 digits with no spaces or delimiters.
tranId	Int(20)	Yes	Transaction ID in the system.
orderId	String(100)	Yes	Unique order identifier in the Partner system.

emitentResponse	String	Yes	All parameters received from the issuing bank, packed in JSON as an associative array. Parameter's names received from the issuer bank should be kept as they are. The parameter must be passed <i>urlencoded</i> .
------------------------	--------	-----	---

The response format for the **Ack3DS** request is fully consistent with the response format for **Block** or **Pay** requests when using a non-3D Secure card.

Status (*webform/gateway*)

An operation for getting the status of the payment.

The format of the **Status** request is: <https://secured.payment.center/v2/status> (POST-request with the **signature** parameter in the header - digital signature, required parameter).

Description of **Status** request parameters:

Parameter	Format	Required	Description
serviceld	Int(12)	Yes	Partner service ID. 1 to 12 digits with no spaces or delimiters.
tranId	Int(20)	Yes	Transaction ID in the system.

The format of response to the **Status** request is: xml string with node **<v2StatusResponse>** (in the header the parameter **signature** - digital signature, required parameter).

Description of response parameters to the **Status** request:

Parameter	Format	Required	Description
success	Reserved values	Yes	Flag of the operation success: true – if the operation succeeds, false – if an error occurs.
tranId	Int(20)	Yes	Transaction ID in the system.
orderId	String(100)	Yes, in case of success=true	Unique order identifier in the Partner system.
amount	Int(12), symbol '.'	Yes, in case of success=true	Payment amount. Corresponds to the one sent in the request.
currency	String(3)	Yes, in case of success=true	Currency code of the transaction that was processed by the bank.
gateAmount	Int(12), symbol '.'	Yes, in case of success=true	The payment amount in the currency of the transaction that was processed by the bank.
gateCurrency	String(3)	Yes, in case of success=true	Currency code of the transaction that was processed by the bank.
tranStatus	Reserved values	Yes, in case of success=true	The current status of transaction. The possible values are: new (open) – new payment with no transactions conducted yet, trusted – new payment that Antifraud check is passed, filtered – new payment that was marked as a fraud by AntiFraud, preAuthorized3DS – the payment is waiting on the completion of 3DS authorization, preAuthorizedAF – the payment is waiting for confirmation from the cardholder, authorized – funds are blocked, voided – funds are unlocked, charged – funds are charged, refunded – refund completed, rejected – payment failed, error – payment transaction was completed with an error.

errCode	Reserved values	Yes, in case of success=false	Error code.
errMessage	Reserved values	Yes, in case of success=false	Error description.

Unsubscribe (*webform/gateway*)

Unsubscribe from a recurring payment.

The format of response to the **Unsubscribe** request is: <https://secured.payment.center/v2/unsubscribe> (POST-request with the **signature** parameter in the header - digital signature, required parameter).

Description of **Unsubscribe** request parameters:

Parameter	Format	Required	Description
serviceld	Int(12)	Yes	Partner service ID. 1 to 12 digits with no spaces or delimiters.
rebillId	Int(20)	Yes	The identifier of a recurring payment. It represents a transaction ID in the system.

The format of response to the **Unsubscribe**: xml string with node **<v2UnsubscribeResponse>** (in the header the parameter **signature** - digital signature, required parameter).

Description of response parameters to the **Unsubscribe** request:

Parameter	Format	Required	Description
success	Reserved values	Yes	Flag of the operation success: true – if the operation succeeds, false – if an error occurs.
errCode	Reserved values	Yes, in case of success=false	Error code.
errMessage	Reserved values	Yes, in case of success=false	Error description.

Check (*webform/gateway*)

Checking of a subscription to a recurring payment.

The format of response to the **Check** request is: <https://secured.payment.center/v2/check> (POST-request with the **signature** parameter in the header - digital signature, required parameter).

Description of **Check** request parameters:

Parameter	Format	Required	Description
serviceld	Int(12)	Yes	Partner service ID. 1 to 12 digits with no spaces or delimiters.
rebillId	Int(20)	Yes	The identifier of a recurring payment. It represents a transaction ID in the system.

The format of response to the **Check**: xml string with node **<v2CheckResponse>** (in the header the parameter **signature** - digital signature, required parameter).

Description of response parameters to the **Check** request:

Parameter	Format	Required	Description
success	Reserved values	Yes	Flag of the operation success: true – if the operation succeeds, false – if an error occurs.
errCode	Reserved values	Yes, in case of success=false	Error code.

errMessage	Reserved values	Yes, in case of success=false	Error description.
Status	Reserved values	Yes, in case of success=true	Recurrent payment status. Possible values are: ACTIVE , CANCELLED , NOT_EXISTS .

3D-Secure authentication

Applied for **3D-Secure**. Processing order - cardholder authentication by the issuing bank and communicating results to the gateway service.

Step 1. When receiving a request for payment in one or two-step operation, the acquirer bank verifies that the card has participated in 3D-Secure authentication. If 3D-Secure is active for the card both **Block** and **Pay** methods will contain '3DS' value in 'success' attribute of the response XML. You should expect **ACSUrl**, **PaReq** and **ThreeDSKey** attributes in the response as well.

The Response – xml-format string with a **v2PayResponse/v2BlockResponse** node.

Node attributes:

#	Parameter	Format	Required	Description
1	success	Reserved value	Yes	Flag of the operation success: 3DS - 3DS operation.
2	orderId	String(100)	Yes	Unique order identifier in the Partner system.
3	tranId	Int(20)	Yes	Transaction ID in the system.
4	acsUrl	String	Yes	URL for redirect.
5	paReq	String	Yes	Encrypted request.
6	threeDSKey	String	Yes	Special attribute.

Step 2. After receiving the response from the system, the Partner redirects the user to the site of the issuing bank, for additional authentication.

Redirect format – POST-request to an address, specified in the value of **ACSUrl** attribute.

Request parameters:

#	Parameter	Format	Required	Description
1	PaReq	String	Yes	Значение атрибута PaReq (необходимо обязательно сделать <i>urldecode</i> перед отправкой на ACSUrl).
2	TermUrl	String	Yes	The user will be returned to this address after passing the authentication on the website of the issuing bank.
3	MD	String	Yes	The value of the ThreeDSKey attribute.

Step 3. . After passing the authentication on issuing bank's side, user will get redirected to the **TermUrl** address.

Redirect format – POST-request to an address, specified in the value of **TermUrl** attribute.

Request parameters:

#	Parameter	Format	Required	Description
1	PaRes	String	Yes	The value of the PaRes attribute.
2	MD	String	Yes	The value of the ThreeDSKey attribute, received from the payment gateway during initial request Block или Pay .

Step 4. After receiving authentication results from the issuing bank to complete the blockage or process a payment, Merchant should execute a request **Ack3DS**.

The format of the **Ack3DS** request is: <https://secured.payment.center/v2/ack3ds> (POST-request with the **signature** parameter in the header - digital signature, required parameter)

Request parameters:

Parameter	Format	Required	Description
serviceld	Int(12)	Yes	Partner service ID. 1 to 12 digits with no spaces or delimiters.
tranId	Int(20)	Yes	Transaction ID in the system.
orderId	String(100)	Yes	Unique order identifier in the Partner system.
emitentResponse	String	Yes	All parameters received from the issuing bank, packed in JSON as an associative array. Parameter's names received from the issuer bank should be kept as they are. The parameter must be passed <i>urlencoded</i> .

Step 5. Merchant receives a response with the results of the payment operation. The result of the **Ack3DS** request matches the results of **Block** or **Pay** requests when non-3D Secure card is using.

Webhooks

HTTP POST-request from the system to the site (service) of a merchant is formed when certain events occur, if the partner has a URL configured and the sending of notifications is activated. All types of notifications contain in HTTP header parameter **signature** in which the verification value of the request is located, being calculated using the HMAC algorithm (an example of a signature formation can be viewed in the self-titled section).

Depending on the configuration of the service, data is being sent in a different format:

- JSON (application/json) - *is not wrapped in the Request.*
- XML (application/xml) - *wrapped in the Request.*

Payment

Is performed after a payment was successfully - issuer authorization was received. Provides information on the payment: the system is sending the request with payment information to the merchant's address, and the merchant service has to process this information.

Parameters are passed in the body of the request, the list is presented in the table below:

Parameter	Format	Required	Description
Event	Reserved value	Yes	Payment
Transaction_Id	Int(20)	Yes	Transaction ID in the system.
Order_Id	String(100)	Yes	Unique order identifier in the Partner system.
Service_Id	Int(12)	Yes	Partner service ID. 1 to 12 digits with no spaces or delimiters.
Amount	Int(12), symbol '.'	Yes	Payment amount. Corresponds to the one sent in the request.
Currency	String(3)	Yes	Currency in ISO format (USD, EUR, RUB...).
DateTime	DD.MM.YYYY hh24.mi.ss	Yes	Created date of the payment.
CardMasked	String(12-19)	Yes	Masked card number.
IsTest	Bit(0 или 1)	Yes	1 - test; 0 – production.
Status	String	Yes	The payment status after the authorization: CHARGED — for one-step payment operation, BLOCKED — for two-step payment operation.
Cardholder	String(30)	No	Cardholder name.
Email	String	No	Email of the customer.
Phone	String(10-20), ahead '+'	No	Phone of the customer.
RebillId	Int(20)	No	The identifier of a recurring payment. It represents a transaction ID in the system.
Masked_PAN	String(12-19)	No	Masked card number.
Description	String(250)	No	Transaction description in the request.

Token	String	No	'Token' of a recurring payment.
ExpirationDate	String	No	Expired date of the card in format MM/YY.
RRN	String	No	Registration number of the transaction in the bank.

Fail

Performed if the payment was rejected and used for analyze the number and reasons of failures. It is worth considering that the fact of refusal to pay is not final - the user can pay from the second time. Also this notification is applied in the absence of 3DS authorization (DECLINED_BY_TIMEOUT).

Parameters are passed in the body of the request, the list is presented in the table below:

Parameter	Format	Required	Description
Event	Reserved value	Yes	Fail
Transaction_Id	Int(20)	Yes	Transaction ID in the system.
Order_Id	String(100)	Yes	Unique order identifier in the Partner system.
Service_Id	Int(12)	Yes	Partner service ID. 1 to 12 digits with no spaces or delimiters.
Amount	Int(12), symbol '.'	Yes	Payment amount. Corresponds to the one sent in the request.
Currency	String(3)	Yes	Currency in ISO format (USD, EUR, RUB...).
DateTime	DD.MM.YYYY hh24.mi.ss	Yes	Created date of the payment.
CardMasked	String(12-19)	Yes	Masked card number.
IsTest	Bit(0 или 1)	Yes	1 - test; 0 – production.
ErrorMessage	String	Yes	Причина отказа.
Cardholder	String(30)	No	Cardholder name.
Email	String	No	Email of the customer.
Phone	String(10-20), ahead '+'	No	Phone of the customer.
Description	String(250)	No	Transaction description in the request.
ExpirationDate	String	No	Expired date of the card in format MM/YY.
RRN	String	No	Registration number of the transaction in the bank.

Refund

Is performed after a refund of previously charged funds (CHARGED) was made. Can be performed for a partial amount, but no more than the transaction amount. Fee-based operation, a commission will be charged. Provides information on the refund: the system is sending the refund request to the merchant's address, and the merchant service has to process this information.

Parameters are passed in the body of the request, the list is presented in the table below:

Parameter	Format	Required	Description
Event	Reserved value	Yes	Refund
Transaction_Id	Int(20)	Yes	Transaction ID in the system.
Order_Id	String(100)	Yes	Unique order identifier in the Partner system.
Service_Id	Int(12)	Yes	Partner service ID. 1 to 12 digits with no spaces or delimiters.
Amount	Int(12), symbol '.'	Yes	Refund amount (partial or full).
NewAmount	Int(12), symbol '.'	Yes	Remaining amount.
Currency	String(3)	Yes	Currency in ISO format (USD, EUR, RUB...).
DateTime	DD.MM.YYYY hh24.mi.ss	Yes	Created date of the payment.
CardMasked	String	Yes	Masked card number.
IsTest	Bit(0 или 1)	Yes	1 - test; 0 - production.
Cardholder	String(30)	No	Cardholder name.
Email	String	No	Email of the customer.
Phone	String(10-20), ahead '+'	No	Phone of the customer.
ExpirationDate	String	No	Expired date of the card in format MM/YY.
RRN	String	No	Registration number of the transaction in the bank.

Void

It is executed after a cancel of previously blocked funds (BLOCKED) was made. Can be performed for a partial amount, but no more than the transaction amount. Free operation, there is no a commission for it. Provides information on the cancel of the blocking: the system is sending the request to the merchant's address, and the merchant service has to process this information.

Parameters are passed in the body of the request, the list is presented in the table below:

Parameter	Format	Required	Description
Event	Reserved value	Yes	Void
Transaction_Id	Int(20)	Yes	Transaction ID in the system.
Order_Id	String(100)	Yes	Unique order identifier in the Partner system.
Service_Id	Int(12)	Yes	Partner service ID. 1 to 12 digits with no spaces or delimiters.
Amount	Int(12), symbol '.'	Yes	Payment amount. Corresponds to the one sent in the request.
Currency	String(3)	Yes	Currency in ISO format (USD, EUR, RUB...).
DateTime	DD.MM.YYYY hh24.mi.ss	Yes	Created date of the payment.
CardMasked	String(12-19)	Yes	Masked card number.
IsTest	Bit(0 или 1)	Yes	1 - test; 0 – production.
Cardholder	String(30)	No	Cardholder name.
Email	String	No	Email of the customer.
Phone	String(10-20), ahead '+'	No	Phone of the customer.
ExpirationDate	String	No	Expired date of the card in format MM/YY.
RRN	String	No	Registration number of the transaction in the bank.

Receipt

Is performed after a payment was successful. It informs that the payment was made successfully for further registration in the tax (online checkout) in the form of a check. The system sends a request to the address of the merchant with payment information, and the merchant service has to process this information.

Parameters are passed in the body of the request, the list is presented in the table below:

Parameter	Format	Required	Description
Event	Reserved value	Yes	Receipt
Transaction_Id	Int(20)	Yes	Transaction ID in the system.
Order_Id	String(100)	Yes	Unique order identifier in the Partner system.
Service_Id	Int(12)	Yes	Partner service ID. 1 to 12 digits with no spaces or delimiters.
Amount	Int(12), symbol '.'	Yes	Payment amount. Corresponds to the one sent in the request.
NewAmount	Int(12), symbol '.'	Yes	Remaining amount.
Currency	String(3)	Yes	Currency in ISO format (USD, EUR, RUB...).
DateTime	DD.MM.YYYY hh24.mi.ss	Yes	Created date of the payment.
IsTest	Bit(0 или 1)	Yes	1 - test; 0 – production.
Status	String	Yes	The payment status after the authorization: CHARGED — for deduction of the funds, REFUNDED — for refund of the funds.
Email	String	Yes	Email of the customer.
Phone	String(10-20), ahead '+'	Yes	Phone of the customer.
Description	String(250)	Yes	Transaction description in the request.

Repeating of webhook notifications

In response to the request, the system expects to receive a response with the status of HTTP 200. Upon received of another code, the system will continue to try to deliver the message within two days with an increasing interval between attempts.

Signature

All types of messages contain a **signature** parameter in the HTTP header, which contains the verification value of the request, being calculated using the HMAC algorithm. See example below with the real intermediate values for debugging signature generation.

Example:

- Notifications are sent using POST request,
- The message is the value of the **body** request, for example:

```
"serviceId=1&tranId=88800&amount=50.00&currency=RUB"
```

- The **secret_key** value of the service is used as the key, for example:

```
"secret_key_1"
```

- The hash is calculated by the **SHA256** function (we get the data in hexadecimal (!) encoding in lowercase):

```
"78e79b0052da99b32146527cc7c5ab13222a4e8a3ded3bd77254f271087cb2a3"
```

- The calculated value should be converted to the **base64** encoding:

```
"Nzh1NzliMDA1MmRhOTliMzIxNDY1MjYzdjYzZjNWFiMTMyMjJhNGU4YTnkZWQzYmQ3NzI1NGYyNzEwODdjYjJhMw=="
```

Signature sample (Python):

```
import hashlib
import hmac
import base64

def calc_signature(body, secret_key):
    message = body
    secret = bytes(secret_key).encode('utf-8')
    digest = hmac.new(secret, message, digestmod=hashlib.sha256).hexdigest()
    return base64.b64encode(digest)
```

Signature sample (PHP):

```

$requestType = "charge"; // possible values: charge, refund, pay...
$requestUrl = "https://secured.payment.center/v2/" . $requestType;

// array for parameters
$bodyRequestArray = array(
    'serviceId' => "YOUR_SERVICE_ID",
    'cardNumber' => "CREDIT_CARD_NUMBER", // Without spaces, for example,
'4111008030004444'
    'expMonth' => "EXPIRED_MONTH", // 2 digits, for example, '04'
    'expYear' => "EXPIRED_YEAR", // 2 digits, for example, '20'
    'cardHolder' => "CARD_HOLDER_NAME",
    'cvc' => "CVC",
    'orderId' => "YOUR_ORDER_ID"
    'amount' => "AMOUNT", // digits and dot ('.'), for example, '3500.45'
    'currency' => strtoupper("CURRENCY"), // RUB|USD
    'description' => "DESCRIPTION",
);

$body = http_build_query($bodyRequestArray);
$signature = getSignature($body, "YOUR_SECRET_KEY");

$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $requestUrl);
curl_setopt($ch, CURLOPT_POST, 1);
curl_setopt($ch, CURLOPT_POSTFIELDS, $body); //Post Fields
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
$headers = array(
    'signature:'. $signature
);
curl_setopt($ch, CURLOPT_HTTPHEADER, $headers);
$server_output = curl_exec ($ch);
curl_close ($ch);

function getSignature($body, $secretKey)
{
    // create signature
    $hash = hash_hmac('sha256', $body, $secretKey, false);
    return base64_encode($hash);
}

```