

cPay – Testing Procedures and Production Implementation

Contents

GENERAL	3
PAYMENT PROCESS	4
CPAY MERCHANT LOGIN.....	4
PAYMENTS STATUS	5
REDIRECT CODE	6
REPORTS FROM MERCHANT MODULE	6
REFUND FOR APPROVED TRANSACTIONS	7
TEST PAYMENTS	7
CHANGING TO PRODUCTION CHECKSUM AUTHENTICATION KEY	10
COMMUNICATION WITH CASYS	11

General

This document contains information required for merchant integration on CaSys' cPay payment system. The document describes all steps that should be completed during testing period and production implementation.

Transaction is initiated by the customer/buyer, on the web site of the merchant. The customer/buyer selects from the offered goods and services and fills the basket. All data that describe the merchant, payment and the customer/buyer are collected on the merchant's web site. The data related with card that will be used in the payment process, are collected on cPay payment system, to which the customer/buyer is redirected from the merchant web site.

The data collected on the merchant's web site are transferred on cPay payment system within the redirect code. The following data should be transferred:

- Total amount (without decimal separators and last two digits must always be 00 e.g. xxxx00)
- Amount currency (payment currency on cPay payment system is Macedonian Denar – MKD)
- Payment details 1 (filled by the buyer or merchant)
- Payment details 2 (unique identifier of the transactions in the merchant's system)
- Merchant name and merchant identifier
- URL on which merchant receives information for the outcome of the transaction

Except these data, there is optional information such as customer/buyer name, address, postal code, country, phone number, e-mail that can be transferred within redirect code. Additional information also can be sent, original amount and original currency, but these are used by cPay only for informational purposes.

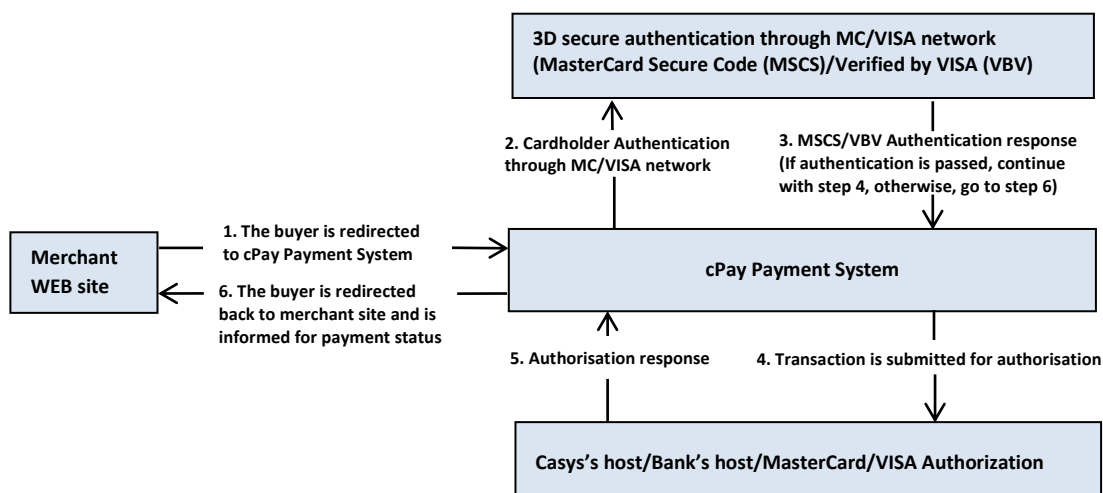
For security reasons of online shopping, information for the merchant's web site hosting must be known to CaSys, along with the addresses from which it can access, firewall usage etc.

When the customer completes shopping process and decides to pay, with pressing pay (checkout/buy) button on merchant's web site, he is redirected on cPay payment system.

Data of the card used in payment process, are entered on each transaction by the customer/buyer. Card/cardholder authentication is achieved with CVC2/ CVV2 and 3D security authentication (if the card is enrolled in 3D authentication model which depends from the Issuer).

When the payment process is finished, the customer/buyer is redirected back to the merchant's web site where he receives information about the status of the financial transaction and the outcome of the payment.

The following picture is an illustration of the shopping process described previously.



Payment Process

The payment process can be performed as:

- One step payment – the cardholder account is debited immediately.
- Two step payment – first, preauthorization transaction is performed and amount of the payment is reserved from the cardholder's account. Later, when the merchant is sure that the product/service can be delivered, preauthorization completion transaction is performed.

cPay Merchant LOGIN

When merchant is defined in cPay payment system, Merchant USER (email address) and Merchant PASSWORD are sent to contact person's e-mail address specified in the definition form sent by the Bank.

Merchant can use received Merchant USER and PASSWORD to [login](#) on cPay payment system, merchant menu, on which merchant have access on the following:

- Payments – Listing of payments performed on merchant's e-shop. Data for the transactions are kept online for 90 days
- Merchant (User) profile – Listing of user data and option for changing the password
- Redirect code – Downloading the redirect code template; download latest integration specification and Testing Procedure; download the CSS code for payment form; download cPay plugin for WooCommerce
- Transaction reports – Reports for all successful payments on merchant's e-shop

If the password for Login is forgotten, or account is locked because of several invalid login, you can use the forgot password option on cPay merchant module ([Forgot Your password?](#))

Payments Status

Explanation follows of the transactions status that can appear on cPay merchant module:

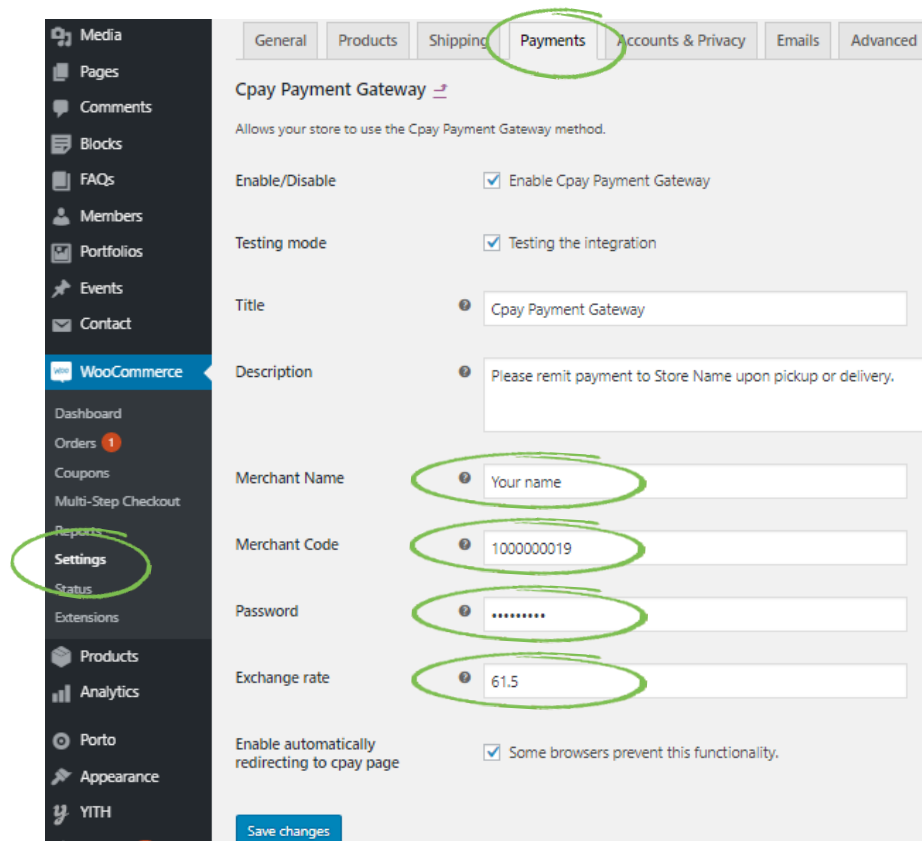
- **Успешна/Sent**
Successful transaction, successfully processed transaction.
- **Одбиена/Rejected**
Unsuccessful transaction, rejected by the card issuer or cPay
- **Authorized**
Successful pre-authorization transaction, the amount is reserved from cardholder account.
- **Completed authorization**
Successful completion of previous pre-authorization transaction. Completion amount is debited from cardholder account.
- **Нарачка во процес/New**
Pending transaction, transaction that is not yet confirmed by the client, it is temporary status. Later, this status will be change to one of the final statuses (if no action is taken by the client this status will be change to Expired)
- **Откажана/Canceled**
Unsuccessful transaction, transaction that is canceled by the client
- **Blocked**
Unsuccessful transaction, blocked because of set black/white list for the merchant
- **Blocked by Card Limits**
Unsuccessful transaction, blocked because of set limit for amount/number of transactions in defined period.
- **System Reversal**
Unsuccessful transaction, the transaction is not successfully processed in authorization and cPay system generates reversal.
- **Во 3D Secure автентикација/In 3D Secure authentication**
Pending transaction, the client is redirected to the bank ACS site for verification of the 3D Secure code/password, it is temporary status. Later, after appropriate action by the client, this status will be change to one of the final statuses. If the client do not take any action or closes the browser without entering the 3D Secure code, this status will be change to Expired
- **3D Secure автентифицирана/3D Secure authenticated**
Pending transaction, the client has successful entered the 3D Secure code and has passed 3D authentication, it is temporary status. Later, this status will be change to one of the final statuses. If the client closes the browser after entering the 3D Secure code, this status is changed to Expired.
- **3D Secure автентикацијата е неуспешна/3D Secure authentication failed**
Unsuccessful transaction, the client has entered an incorrect 3D Secure code and has failed 3D Secure authentication.
- **Рефундирана/Refunded**
Refunded successful transaction, a successful transaction was refunded by the bank on a request from the merchant. The Refund option can also be enabled on merchant module, please contact the bank.
- **Делумно Рефундирана / Partially Refunded:** successful partially refunded transaction, performed by the bank on a request from the merchant, The partial refund option can also be enabled on merchant module, please contact the bank
- **Expired**
Unsuccessful transaction. All transactions that are not completed on cPay will have this status, as explain above (previous statuses: New, In 3D authentication, 3D secure authenticated)

Redirect Code

The HTML redirect code is example/template of how and which fields need to be send in the cPay redirect in order to perform an online transaction. In this template the merchant can find the fields PayToMerchant, MerchantName and AmountCurrency, these fields are dedicated to the merchant and must be send as they are for all transactions.

- The redirect code is downloaded from cPay payment portal, from the Merchant menu.
- The redirect code is provided only as an example of the redirect form that the merchant ecommerce application should generate for each transaction and if any of the fields are modified manually, it will not work.
- The payment implementation in the merchant web site is developers' solution and can be done in any programming language (PHP, ASP.NET, Java). E-commerce web site developers are the only ones who know their own programming code, therefore, it is really up to them to create a module that works with their own software. However, where ever possible cPay technicians will always assist.
- If the developer is using CMS (WordPress, Magento, OpenCart, Shopify, BigCommerce, Drupal, Joomla, Prestashop), the implementation with the cPay Payment gateway needs to be merchants' side decision whether to use a plugin or to make its own solution.
- If WordPress platform is used and WooCoommerce for e-shop, Casys offers a plugin which is available at the following link "[Payment Gateway for Cpay with WooCommerce](#)".

It is free to download and easy to install, to set it up you will need to enter the parameters for your merchant.



The screenshot shows the 'Cpay Payment Gateway' settings page. The 'Payments' tab is active. The 'Enable/Disable' section has 'Enable Cpay Payment Gateway' checked. The 'Testing mode' section has 'Testing the integration' checked. The 'Title' field is 'Cpay Payment Gateway'. The 'Description' field contains the text 'Please remit payment to Store Name upon pickup or delivery.' The 'Merchant Name' field is 'Your name', 'Merchant Code' is '1000000019', 'Password' is '*****', and 'Exchange rate' is '61.5'. The 'Enable automatically redirecting to cpay page' checkbox is checked with the note 'Some browsers prevent this functionality.' A 'Save changes' button is at the bottom.

Merchant Name – value of the parameter MerchantName in the template redirect code;
 Merchant Code – value of the parameter PayToMerchant in the template redirect code;
 Password – TEST_PASS when testing is performed, afterward for production it is change with production checksum authentication key, which is sent to merchant in the zip file after successful testing;

Exchange rate – value for the exchange rate of the currency (EUR, USD....) from WordPress to national Bank currency (MKD).

*If payment form should be on another language (MK or EN), you can put an endpoint filter, and utilize appropriate PaymentURL (MK or EN).

**For more than one currency, your development team can also create filter for exchange rate

Reports from Merchant Module

The merchant can download reports for successful transactions from the merchant module of cPay, tab “ИЗВЕШТАЈ ЗА ТРАНСАКЦИИ” (“REPORT TRXIDS”). The report file can be downloaded in several formats (.txt, .csv, .xls, .xml). Data for the transactions are kept online for 30 days

An example of one record in .txt format follows:

277254,0010012800,46929,,24.04.2012 14:23:20,245,MKD,Sent

The explanation about fields in the record is listed in the following table:

Field	Lenght	Description
cPayRefID	6 - 10	Transaction Identification in cPay.
Sequence Number	10	Control number that the POS terminal generates for each transaction.
Details 2	max 100	Transaction Identification in the merchant system (Order Id).
Details 3	max 100	Not used. Always will be empty.
Transaction DateTime Format is: DD.MM.YYYY HH:MM:SS (24.04.2012 14:23:20)	16	Date and time of the transaction.
Amount	1 - 12	Transaction amount.
Currency	3	Transaction currency (MKD).
Status	4-23	Transaction Status (always will be “sent”, “authorized” or “completed authorisation”, since in the reports are shown only successful transactions).

Refund for Approved Transaction

There is option for enabling the full and partial refund functionality for approved transactions on merchant level. For this option, please contact the bank.

Pressing the Refund button completes the full refund of the transaction. Full refund of the transaction can also be done if the full amount of the transaction is entered in the amount entry field. If the transaction is successful, the status of the transaction changes to **Refunded / Рефундирана**.

A partial refund can be made if an amount less than the original amount is entered in the amount entry field. If the transaction is approved, the status of the transaction changes to **Partially refunded / Делумно рефундирана**, and the amount of the partial refund will be displayed in the Amount field.

Note: The responsibility for the refund of the transaction is on the merchant. Casys does not take responsibility for any unauthorized refund transactions performed from merchant module. It is important merchant not to share any login credentials. If password is compromised, change it immediately.

Test Payments

Test payments should be created with correct checksum. For the checksum creation, as explained in merchant integration specification, checksum authentication key is needed. Initially, for the test purposes authentication key is TEST_PASS and maximum amount for a transaction is 10 denars. After testing is successfully completed, i.e. all mandatory tests are performed and all notifications sent from cPay payment system are received by the merchant, checksum authentication key is changed (procedure for checksum authentication key management is explained later in this document) and transaction amount limitation is removed.

In order to check accuracy of the created checksum, payment request from the merchant web site should be sent to the following test URL:

https://www.cpay.com.mk/Client/page/default.aspx?xml_id=/mk-MK/.TestLoginToPay/

This test page is used only for checking the accuracy of the calculated checksum.

After correct creation of the checksum (the test page doesn't show an error), the merchant should:

- Create payment of 1 Denar
- Use one of the PaymentURL addresses listed in the merchant integration specification
- Perform test payment transactions.

The merchant must use the whole unit amount in the redirect code (the last two digits of parameter AmountToPay must always be 00 e.g. xxxx00).

For one step payments, the following payment transactions must be performed for test purposes prior going to production (All notifications, explained in next chapter, should be successfully sent to the merchant):

- **Case 1:** Successful transaction (redirect to OKUrl) - the cardholder's account is debited. Please include string with international special characters (e.g. string "Тест Стрѝњ" In the parameter Details 1) to make sure that the length of these characters and the checksum are correctly calculated. Length of each character should be count 1.
- **Case 2:** Unsuccessful transaction (redirect to FailUrl) - the cardholder's account is not debited (e.g. wrong expiration date or CVC2/CVV2 of the card is entered).

Please note that following payment transactions can happened in production, and those cases are optional for testing during implementation:

- **Case 3:** Cancelled transaction (redirect to FailUrl) - the data of the payment card are entered, the button **Продолжи/ Continue** is pressed, but on the next step, the buyer has cancelled the payment, button **Откажи/Cancel** is pressed. All notifications, explained in next chapter, should be successfully sent to the merchant.
- **Case 4:** Expired transaction - the data of the payment card are entered, the button **Продолжи/Continue** is pressed, but on the next step, the buyer has performed no action and transaction has time out. In this case email notification for unsuccessful transaction and push notification to FAIL URL will be sent to merchant after 30 minutes.

For the next scenarios, merchant will not receive all notifications (The merchant must be aware for these situations that might occur in production):

- **Case 5:** Successful transaction (redirect to OKUrl) – the browser should be close immediately after confirming the payment in last step (for less than 1 second e.g. only one tab in the browser, where payment will be performed, is opened; and after confirmation immediately close the browser with ALT+F4), the cardholder's account is debited. In this case the merchant will not receive notification via buyer's browser but will receive only email confirmation (with subject "order status") and push notifications, both initiated 15 minutes after the payment.
- **Case 6:** Successful transaction (redirect to OKUrl) – the browser should be close immediately after confirming the payment in last step (for less than 1 second e.g. only one tab in the browser, where payment will be performed, is opened; and after confirmation immediately close the browser with ALT+F4), the cardholder's account is debited. In this case the merchant will not receive notification via buyer's browser and push notifications, but will receive only email confirmation (with subject "order status") 15 minutes after the payment. Additionally, the merchant will receive and email for unsuccessful delivery of push notifications (with subject "failed merchant notifications"). For this case, for push messages sent from cPay server, the merchant server should respond with HTTP status other than 200 OK in order push messages not to be delivered from cPay server to merchant server (to OKUrl), and this should be configured on merchant side for testing purposes.
- **Case 7:** Successful transaction (redirect to OKUrl) – the cardholder's account is debited. In this case the merchant will not receive the push notifications but only notifications via buyer's browser and email confirmation (with subject "order status"). Additionally, the merchant will receive and email for unsuccessful delivery of push notifications (with subject "failed merchant notifications"). For this case, for push messages sent from cPay server, the merchant server should respond with HTTP status other than 200 OK in order push messages not to be delivered from cPay server to merchant server (to OKUrl), and this should be configured on merchant side for testing purposes.

For two steps payments, the following payment transactions must be performed for test purposes, prior going to production (All notifications, explained in next chapter, should be successfully sent to the merchant):

- **Case 1:** Successful transaction (redirect to OKUrl) – the preauthorization amount is reserved from the cardholder's account. Please include string with international special characters (e.g. string "Тест Striňg" In the parameter Details 1) to make sure that the length of these characters and the checksum are correctly calculated. Length of each character should be count 1. After that, preauthorization completion should be performed by the merchant, which debits the reserved amount from the cardholder's account.
- **Case 2:** Unsuccessful transaction (redirect to FailUrl) – the amount is not reserved from the cardholder's account (e.g. wrong expiration date or CVC2/CVV2 of the card is entered).

Please note that following payment transactions can happened in production, and those cases are optional for testing during implementation:

- **Case 3:** Cancelled transaction (redirect to FailUrl) -the data of the payment card are entered, the button **Продолжи/ Continue** is pressed, but on the next step, the buyer has cancelled the payment, button **Откажи/Cancel** is pressed. All notifications, explained in next chapter, should be successfully sent to the merchant.
- **Case 4:** Expired transaction - the data of the payment card are entered, the button **Продолжи/Continue** is pressed, but on the next step, the buyer has performed no action and transaction has time out. In this case email notification for unsuccessful transaction and push notification to FAIL URL will be sent to merchant after 30 minutes.

For the following scenarios, merchant will not receive all notifications (The merchant must be aware for these situations that might occur in production):

- **Case 5:** Successful transaction (redirect to OKUrl) – the browser should be close immediately after confirming the payment in last step (for less than 1 second e.g. only one tab in the browser, where payment will be performed, is opened; and after confirmation immediately close the browser with ALT+F4), the preauthorization amount is reserved from the cardholder's account. In this case the merchant will not receive notification via buyer's browser but will receive only email confirmation (with subject "order status") and push notifications; both initiated 15 minutes after the payment. After that, preauthorization completion should be performed by the merchant, which debits the reserved amount from the cardholder's account.
- **Case 6:** Successful transaction (redirect to OKUrl) – the browser should be close immediately after confirming the payment in last step (for less than 1 second e.g. only one tab in the browser, where payment will be performed, is opened; and after confirmation immediately close the browser with ALT+F4), the preauthorization amount is reserved from the cardholder's account. In this case, the merchant will not receive notification via buyer's browser and push notifications, but will receive only email confirmation (with subject "order status") 15 minutes after the payment. Additionally, the merchant will receive and email for unsuccessful delivery of push notifications (with subject "failed merchant notifications"). For this case, for push messages sent from cPay server, the merchant server should respond with HTTP status other than 200 OK in order push messages not to be delivered from cPay server to merchant server (to OKUrl), and this should be configured on merchant side for testing purposes. After that, preauthorization completion should be performed by the merchant, which debits the reserved amount from the cardholder's account.
- **Case 7:** Successful transaction (redirect to OKUrl) – the preauthorization amount is reserved from the cardholder's account. In this case the merchant will not receive the push notifications but only notifications via buyer's browser and email confirmation (with subject "order status"). Additionally, the merchant will receive and email for unsuccessful deliver of push notifications (with subject "failed merchant notifications"). For this case, for push messages sent from cPay server, the merchant server should respond with HTTP status other than 200 OK in order push messages not to be delivered from cPay server to merchant server (to OKUrl), and this should be configured on merchant side for testing purposes.. After that, preauthorization completion should be performed by the merchant, which debits the reserved amount from the cardholder's account.

Please note that all test payments are performed in production mode.

For all test cases the HTTP Referer parameter should be present with valid value.

If during testing the merchant faces with screen with information "System error", first please check all the parameters that are sent in the redirect code if they are according specification, if no errors are found you should contact CaSys' support team in order problem to be resolved.

Note 1: For two steps payment, with preauthorization and completion, if the merchant cannot deliver the product/service after successful preauthorization, release of the reserved clients' funds should be performed (cancelation of the preauthorization). The easiest way is to perform completion on 1 denar, which will debit the client account for 1 denar, and release the remaining amount of the cardholders account. In this case the merchant should inform the Bank about these preauthorization/completion transactions. It is recommended the acquiring Bank to inform the issuer Bank about this cancelation.

Note 2: All transaction performed on amount greater than 10 denars before changing the checksum authentication key will be declined.

The obligation for test conduction is on the merchant. When all test transactions are performed, the merchant should inform CaSys' support team in order analysis to be performed, for successfulness of performed test payments and notification delivery.

Changing To Production CheckSum Authentication Key

In order to start working in production mode, the merchant should inform CaSys' support team that the tests are finished and all test transactions are performed.

If transactions are not successfully processed in CaSys' system (i.e. the notifications are not successfully delivered to the merchant), additional correction by the merchant should be performed according provided instruction, and tests should be repeated.

After CaSys' confirmation of successful transactions processing in the system, and successful delivery of all notifications to the merchant, the checksum authentication key must be change.

The productive checksum authentication key is defined by Casys and sent only to merchant email. Subject of the email message will be:

cPay_MERCHANT NAME_Changing the checksum authentication key_Date – if the e-mail communication is conducted on other than Macedonian language

cPay_IME NA TRGOVECOT_Promena na CheckSum Avtentikaciski Kluch_Datum – if the e-mail communication is conducted on Macedonian language

The following rules must be followed:

1. CheckSum authentication key (which must be sent only by Casys representative) must be in zip file; the zip file should be password protected.
2. The password of the zip file is sent only to merchant email address, in another email, replying on the previous sent mail for changing the checksum authentication key.
3. The changing of the checksum authentication key is performed in the merchant system. To confirm that the changes made in both systems are correct, the merchant should perform at least one successful redirect to cPay Payment system
4. CaSys informs the merchant and the Bank representative that the checksum authentication key is successfully changed.

Without changing to production checksum authentication key, the merchant cannot implement its e-shop in production mode. Changing of the checksum authentication key is performed in working days in period from 08:30-15:30.

Communication with CaSys

During the implementation and testing, the merchant should use only e-mail communication with CaSys' support team. This way all involved parties will be informed about the activities, problems and the progress of the implementation. Please, do not use phone communication.

During implementation, for communication with CaSys' support team please use the following e-mail address ecommerce@casys.com.mk. In each request/e-mail please include representative person from the bank with which the merchant has agreement (email address of the representative person of the bank is not included when changing the checksum authentication key).

Note: After the implementation is finished, and checksum authentication key is changed i.e. production mode has started, the complete communication is carried out by the bank.

For e-mail communications with CaSys' support team please follow the rules for e-mail subject (the subject is listed in both English and Macedonian language, depending of the email language conversation) always be must enter a merchant name.

Example:

English - cPay_MERCHANT NAME_[Description of the request]_YYYYMMDD

Macedonian - cPay_IME NA TRGOVECOT_[Opis na baranjeto]_YYYYMMDD

Description of the request:

- **Problem with code implementation**
- **Requesting for test cases results**

Note: the merchant should provide info about cPayRefID for each performed test. For example, Case1: 25710201, Case2: 25710202, etc.

- **Push messages or email notifications are not delivered**
- **Changing the checksum authentication key**
- **Creation of additional user profile (email should be send only by representative of the Bank)**
- **If the problem is not listed in above examples**

Please follow the above rules in order your requests to be processed on time.