E-commerce ING WebPay Service Guide

Table of Contents

Introduction

The goal of this document is to describe ecommerce trading operations, with their related possibilities and obligations. The document is both for persons from the company who use them and for persons with financial-accounting or administrative tasks.

Important! For the proper operation and security of the service, the Merchant must make sure that the Users have confirmed that they have understood the instructions and procedures comprised in this Guide.

The parties agree that the content of this document is available, both in Romanian and English languages therefore, in case of any inconsistencies, the Romanian version will prevail.

Chapter I - General Rules regarding the acceptance of the Card by the Merchant

1.1. Making the Transactions

Sale:
In order to implement a Transaction, the Merchant:

a. shall accept for payment valid Cards of the type specified by the Bank, produced by Card Holders for the purchase of products and services at prices identical to those charged in the case of cash payment transactions and for similar products and/or services;
b. shall provide the Card Holders, via the communication channels specified and accepted by the latter, with an electronic receipt certifying the payment execution;
c. shall ask the Card Holder to provide the contact information required to send such receipt.
d. shall perform the Transactions in strict compliance with the specifications included in the e-commerce service guide

Receipt
After completing a Transaction or obtaining an Authorization Code, the Merchant shall issue a payment confirmation (Receipt) which includes the Transaction or Authorization details.

The standard receipts issued by the Merchant shall include the following identification data: Merchant name; address of the registered office of the Merchant; identification code of the Merchant; commercial name (including the internet address of the Store); card number (partially truncated); name of the Card Holder; generic description of the purchase; RRN (Retrieval Reference Number, representing the reference number of the transaction in the system of ING Bank); Receipt number; Transaction Authorization Code; date and time of the Transaction or Authorization; the value of the Transaction and the currency in which the transaction was performed.

Transaction cancellation: The Merchant may attempt to cancel a previously performed Transaction, provided the authorization of the Transaction which is subject for cancellation was performed fewer than 14 calendar days before, and the Card Holder or the Merchant waived the Transaction.

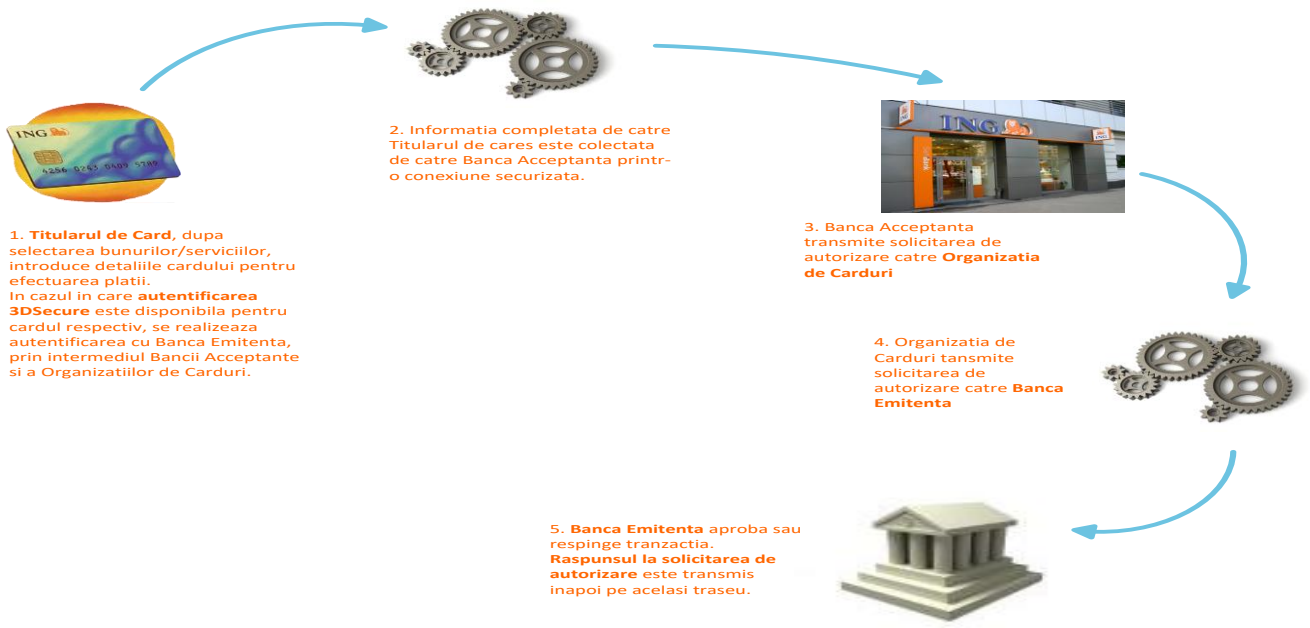
A Transaction may be cancelled before the Batch Settlement, according to the e-commerce Guide, directly by the Merchant from the e-commerce app, and automatically leads to the cancellation of the right to settle the respective Transaction

The cancellation of Transactions may be cancelled after the Batch Settlement and the cancellation of settled Transactions may be performed by the Merchant, by a written request to ING Bank, signed by the authorized person within the business relations with the Bank and/or directly by the Merchant from the e-commerce app, according to the e-commerce Guide, if this facility is granted by the Bank. The Merchant shall authorize ING Bank to automatically debit the

E-commerce Account or, at the Bank's discretion, any of its current accounts in Lei and/or foreign currency in order to process the Merchant's Transaction cancellation request, or to withhold the relevant value from the amounts to be settled.

In case of cancellation, a Transaction or Authorization shall be canceled partially or entirely. The Transaction cancellation shall be made prior to the Batch Settlement Procedure operated in the relevant Store.

Schematic presentation of an e-commerce transaction:



Financial reporting of transactions:

ING shall provide to the Merchant, via the internet banking platform specific to the business segment, reports with settled transactions, within 2 (two) calendar days after the Settlement date. The reports shall be available according to the aforementioned information and may be stored by the Merchant for 90 calendar days after they are posted in the dedicated interface of the ING Business and InsideBusiness channels, namely 30 days in the InsideBusiness Payments CEE interface, and then they cannot be viewed and stored from the internet banking platform.

What should each Merchant know about electronic commerce:

- All card transactions must be authorized (thus avoiding the use of cards declared lost / stolen or which have no funds available)
- Merchants are responsible for fraudulent transactions made on their website, regardless of whether or not they have received authorization for the respective transaction.
- If they operate directly with card data (e.g. transactions manually entered in the Virtual Terminal) they must adapt their systems in accordance with the PCI DSS (Payment Card Industry - Data Security Standards) rules, mandatory standards for storing and viewing sensitive information regarding cards)
- One must never store CVV2 or CVC2 codes for future use

- Intermediate merchants in payment systems or commercial systems are jointly and severally liable for transactions with the final Merchant (e.g. travel agencies with the hotel)
- They must accept for payment all VISA or MasterCard cards, in accordance with the rules of the contractual framework of the e-commerce service;
- They shall display the VISA, MC, Maestro and all the other logos regarding the types of cards and the types of services accepted in card payments
- All additional taxes (excise duties, VAT, etc.) must be disclosed separately, but included in the total amount of a transaction
- They must carry out commercial transactions only in their own name and interest or on contractual bases
- In the electronic environment, the date of the transaction is considered the product delivery date (not the date on which the order was placed)
- The cardholder must be informed about the method of delivery, the period of delivery and the taxes related to it
- The reimbursement and cancellation policy must be clearly stated and agreed by the customer before the transaction is made
- The transactions for which the delivery of the service or product is carried out in the future must be carried out by the pre-authorization / authorization process
- One must NEVER apply additional taxes for using the card as payment
- One must use the card strictly in relation to the transaction agreed by the client (not for other collections or verifications which are not necessary)
- The term in which a transaction can be disputed (the Merchant can receive a refusal to pay) is maximum 120 days from the date of the transaction

1.2. Code of best practices in electronic commerce - Essential information that must appear on the website

Confidentiality policy

- inform the client about the collected data and how it will be used;
- inform the client about the access to this data;
- offer the client the possibility of not processing his/her data;

Information security

- display all the means by which the customers' data is secured and the level at which they are secured;
- create a page with frequently asked questions & answers on how to protect the customer when shopping online;
- display all the logos of the security systems you use: e.g. Verified by VISA or Mastercard SecureCode;

Payment methods

- display the payment methods agreed by your site and clearly mention the options: debit card, credit card etc.

Description of goods / services

- make sure that the goods or services offered are described as clearly and completely as possible (technical characteristics, functionalities, whether or not they are the object of a promotion / discount, country of origin, service if applicable, present an accurate image of the product where possible etc. .)

Ways of completing the order:

- describe / exemplify how to complete the order;
- update information on available stocks;

Sending

- you must mention the delivery methods;
- the customer must opt for a single delivery method, if there are several;
- explain the shipping options (duration and costs);
- offer the shipment tracking service if you have the possibility, inform the customer if there are delays in the delivery of the ordered product / service;

- inform the client about the ways of returning the ordered goods and who pays the costs of the return;
- mention the responsibility regarding the damage of the goods during transportation or of those blocked in customs;

Invoicing

- detail the invoicing method, the period of time when the amount will appear on the bank statement, the merchant / transaction identification data that will appear on the bank statement. By these details, eliminate possible confusions;
- encourage the client to keep the invoicing data;
- explicitly display the total amount of the transaction, the taxes and fees included (VAT) and the currency in which the invoice is issued;
- mention the possibility that at the moment when the account is debited there will be exchange rate differences;

Canceling the order and returning the money

- make sure you have a clear and transparent policy for money cancellation and return;
- every time offer customers the opportunity to accept or reject the site policy;
- in case of subscription transactions, make sure that the client's taxation ceases after the cancellation of the subscription and inform the client in this regard;

Contact address

- provide the customer with all your contact details: e-mail, telephone, address or questionnaire to be filled in on the site as well as the work schedule of the assistance service;
- develop an internal response policy to customer messages and transmit this policy to customers, indicating to what extent the estimated response time is possible;

Restrictive policies

- display on the site the exceptions regarding the acceptance of orders, the delivery of goods and products, the country of origin of the card holder (e.g. if you do not deliver outside the EU);

1.3. Risk in electronic commerce

1.3.1. Risk awareness and employee training

It is important to know as many methods of fraud prevention on the Internet as possible, to make them known to the persons in the company who are involved in the acceptance activity and to train the personnel directly involved in managing these risks.

Typical e-commerce risks:

a. Fraud
   - the data of stolen cards is used for purchasing goods or services;
   - family members use the card data without the card holder's consent;
   - clients who falsely claim not to have received goods or services;
   - security breach - compromising card data by various methods for accessing them
   - phishing – a fake sale page, similar to the genuine one, used by fraudsters in order to obtain customers' card data. Subsequently, the card data obtained in this manner is used in order to carry out fraudulent transactions.

b. Types of payment refusal that may result from the fact that:
   - the goods and services are not correctly described on the site;
   - there are technical errors in orders;
   - the product cancellation and the return policy of the company is not complied with;

- the goods or services were not received or received late;
- there were disagreements regarding the price, commissions, taxes;
- there were technical errors such as invoicing duplications;
- there are confusions related to the name of the merchant that appears in the bank statement;

1.3.2. Risk approach

From a risk perspective, it is useful that each Merchant, for its protection and that of its clients, to implement its own means of monitoring and preventing risk.

One of the main tasks that is included in the attributions of a Merchant is, in case of transactions on the Internet as in the case of card ones, authentication, namely identifying the person who places the order and offers to pay by card.

The main means of identifying the customer, card holder, during an e-commerce operation are:
- CVV2 or CVC2 - three-digit VISA and Mastercard codes on the back of cards, used especially for authentication.
- VbV and MSC - "VISA Secure" and "Mastercard Identity Check" are the names of the two security systems, for the identification of the card holder, offered by VISA and Mastercard. They involve the authentication of the card holder by the method provided by the issuing bank.

Additional means of verification:
- records are recommended, on merchant level, of fraudulent or suspicious transactions (for example: the name of the order issuer must be the same as the name of the card holder, e-mail addresses, delivery addresses, username, phone numbers, etc.) by complying with all the data protection legal requirements
- tracking order frequency; if a customer exceeds a normal number of orders placed on the site, during a limited period of time, there may be a suspicion of fraud. It is advisable to keep records on clients, and when there is suspicion to make additional checks.
- it is good to establish a customer profile (which are the amounts that are usually spent, purchases usually made, whether a customer issues orders with delivery to multiple addresses or whether more customers have the same delivery address or other common data, etc.)
- records of returned orders and managing the reasons for which they were returned
- monitoring the operations according to the IPs from which the orders come (pay attention to orders coming from the same IP with different cards; the same card from several IPs; etc)

Managing transactions with a high risk of fraud:
- educate customers and personnel regarding risks associated to phishing cases, to ensure a high level of security for the devices they use;
- Do not access links received in e-mails or unsolicited text messages or from suspicious sources;
- use fraud prevention means in order to identify high-risk transactions: e.g., check the elements from previously confirmed fraud cases, check the exceeding of the set limits, etc.; international IPs must be regarded as high risk; thus, for these you need to take additional measures, namely you need to check as many security elements as possible: CVV2, validation through a link sent to the e-mail address, telephone verification, requesting additional identification documents: passport, utility invoice, etc.
- Carefully manage the cases where the delivery address is not the same as the invoicing address;
- Check the type of the delivery address; pay increased attention to high risk locations such as: prisons, mailboxes, hospitals, public addresses in general;

1.3.3. Chargeback

What it is, how to avoid it and how to recover challenged amounts (any losses)

If a card holder initiates a payment rejection, the issuing bank sends the request to the accepting bank (of the merchant). The accepting bank requests substantiating documents / details regarding the respective transaction of the merchant, and the

latter must send all the documents related to the transaction, within the granted time limit. The lack of an answer or an incomplete / illegible answer may lead to the cancellation of the collection by the merchant.

Follow the best practices:

- Do not complete a transaction if the authorization request has been declined and you do not request a new authorization. Request another form of payment.
- Act promptly when clients with justified disputes are entitled to get their money back (card crediting / refund). When card holders contact you directly in order to resolve a dispute, initiate card crediting in a timely manner so as to avoid unnecessary disputes and processing costs. Send customers an email in order to immediately notify them of initiating the crediting of the disputed amount.
- Provide detailed replies to document requests (which need to be legible, complete and correct).

Respond to the bank's requests with all the information regarding the transactions and be sure to include in the answer the following (mandatory) elements:

- card number;
- card expiry date;
- card holder’s name;
- transaction date;
- transaction amount;
- authorization code;
- merchant’s name;
- online address / site of the merchant ;
- a general description of the provided goods or services;
- delivery address - if applicable;

You can also provide additional information that can help resolve your request and thus reduce the risk of receiving payment refusal, such as:

- transaction time;
- client’s e-mail address;
- client’s phone numbers;
- computer IP
- client’s invoicing address;
- a detailed description of the provided goods or services;
- if available, a receipt signature upon the delivery of the goods or services;

Monitoring of refusals: The best practices for monitoring payment refusals can be:

- Tracking / recording payment refusals and their disputes according to the reason / code for which they were initiated. Each payment refusal reason involves specific methods to be remedied and strategies to reduce them.
- If your activity combines traditional sales with Internet transactions, track / record the payment refusals separately for these types of activities.
- Card organizations monitor the activity of all merchants regarding the number of payment refusals and their type and alert the accepting banks when some of their merchants have received an excessive number of payment refusals.

1.3.4. Tourism merchants

If you carry out activities related to tourism, such as: airlines, hotels, travel agencies, cruise lines and car rentals, the conditions under which you can accept payments by card, as well as the conditions in which you offer services, have some particularities.

In particular, for these Merchants, there are additional obligations and rights.

Among the obligations:

- displaying, as clearly as possible, the terms and conditions, especially the cancellation and reimbursement conditions, by avoiding abusive clauses
- to offer the service which they undertook or something superior in case of the unavailability of the contracted service
- to send a confirmation of reservations as soon as they are accepted
- in case of the cancellation of reservations, it is mandatory to send a confirmation thereof, in which the connection between the cancellation and the initial confirmation is clearly displayed
- to assume responsibility jointly with the business partner, if it offers services by intermediaries
- it is essential to establish communication with the client, therefore a valid e-mail address is mandatory
- display as clearly as possible the obligations of the client at the time when he / she intends to use the contracted service (they must have a certain type of card or the card with which they made the reservation, they must have identity documents, and ensure that they have money for deposits, etc.)
- mention the adjacent costs (airport charges, extra luggage, access to SPA centers, airport transportation, etc.)
- reverse unfinished and canceled card operations. In this way you will make the money available to the card holder.
- it is important to capture and retain the IP of the computer from which the order was placed

Among the rights:
- you can retain deposits from the card and get pre-authorizations before providing the contracted services
- you can benefit from special conditions in case of payment refusals, depending on the reason why a card holder refuses the transaction, details you can ask the bank at that time

1.4. Security policy regarding the use and processing of card data in accordance with PCI DSS

1.4.1. Card Data

For transactions made in the physical absence of the card, a series of card data has been established, to which the customer / Merchant can have direct access. These are: **User's name** as registered on the card, **card number**, **expiry date**, as well as **card verification code** (CVV2 on VISA or CVC2 on MasterCard). This card data is generically called Cardholder Data and Sensitive Authorization Data and are used in absent-card transactions. Because of their vulnerability, they are subject to a protection policy from card organizations.

An important aspect to keep in mind is that the merchant is NOT allowed to store the card verification Code in any form after authorization. The accepting bank makes available to the merchant the necessary systems for processing the card transactions without handling or storing the Card Data or the Authorization Sensitive Data.

A more complete and accurate definition of Card Data is given by PCI Security Standards Council) www.pcisecuritystandards.org

Important! Merchants from which the Bank requests certain reports which are necessary according to the PCI Security standards, have the obligation to comply with the instructions of the Bank and to provide the respective reports in the range indicated by the Bank.

1.4.2. Card Data Storage

In order to make and validate the reservation, the Sensitive Authorization Data is stored until the transaction is completed. The storage environment and the access to information must comply with the PCI DSS norms.

Warning! After authorization, the CVV2/CVC2 card verification code must be deleted or made illegible. This card information is no longer required for subsequent operations (fill-in, late charge) or in the process of a possible payment refusal.

1.4.3. Here are some recommendations for setting and managing passwords:

- Length: At least 8 characters
- Structure: At least one uppercase letter, at least one digit and at least one special character: !@#$%^&*
- Do not use personal data known by other persons, do not write down, do not make the password public.

- Access will be strictly limited to the person / persons with professional attributions in operating card payments. It is recommended to track the assignment of passwords to new employees (by training) and to cancel the access for persons who terminate their employment or receive attributions in another activity.

- The password management system should allow:
- Periodic changes at intervals of maximum 90 days. Not allowing the same password to be used when renewing. Changing the password whenever you have any suspicion about it being known by other people.
    - After granting a new password, it is mandatory to change it so that the user uses a password known only to him/her.
    - Lock the account after entering the password incorrectly three times in a row.

More details can be found at https://www.pcisecuritystandards.org

Chapter II - User Manual for the E-commerce Application Interface

The e-commerce service (**ING WebPay** Service) is the service that allows you to accept cards for payment via the Internet.

The **ING WebPay administration interface** (E-commerce application) allows you to view the payment orders initiated by clients, to select / download transaction reports, and to cancel orders (if the delivery of goods is no longer desired).

For any information or notifications, please call write to us at e-mail address supportwebpay@ing.com

2.1. Technical requirements necessary for using ING WebPay - Administration Interface

The **ING WebPay - Administration Interface** service is available from any location in the world as long as there is an Internet connection:

- a computer with Internet connection
- Windows 2k, XP, Vista, Mac OSx or subsequent operating system
- a browser (Microsoft Internet Explorer, Mozilla Firefox, Safari)
- resolution of at least 800 * 600 SVGA

Warning! Please ensure that your site meets the standard security requirements by periodically updating the used platforms.

2.1.1. Username and password

The users of the E-commerce application will receive the initial password for activating the service and the web address by email, at the email address declared to ING Bank at the time of requesting the service. In order to obtain the Username (user code) the legal representative / agent of the company in the relationship with the bank needs to call 021 403 83 04.

Users of the E-commerce application can benefit from the following rights granted by the Merchant:
1. API user - the employee has the right to initiate transactions via the E-commerce application
2. User Reporting - the employee has the right to view the transactions carried out via the E-commerce Application and to draft reports regarding them
3. Administration User - the employee is, in additions to holding the privileges of a Reporting User, allowed to cancel or change a transaction on the same day of its execution, when this is carried out prior to the day closing. The Reporting User and/or the Admin User cannot be the same person as the Technical Contact Person.

2.1.2. Password reset

If Users have forgotten the password or have their account blocked, the legal representative / agent of the company in the relationship with the bank must call 021 403 83 04 for unblocking. Users will receive the unblock code by email, immediately after the call.

2.2. COT / Batch Settlement

The closing of the day is performed daily, automatically.

The deadline for performing transactions before the closing of the day is COT 22:00. All transactions performed before this limit will be settled within the settlement period mentioned in the Agreement, and those performed after COT will enter the next settlement cycle.

2.3. Login and logout

2.3.1. How to access the ING WebPay application

The administration interface is available on the website:

https://securepay.ing.ro/consola/index.html

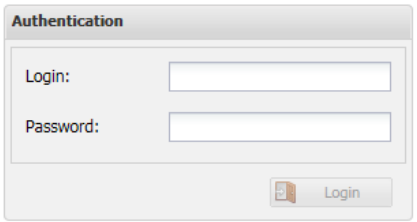


Figure 1

The authentication is performed by entering the user code assigned by ING Bank and the corresponding password (Fig. 1).
!Warning. The fields are "case sensitive", please comply with the format of the usernames and passwords transmitted by ING Bank.

2.3.2. Possible authentication errors and error messages

If an invalid user code or an incorrect code is entered, the following error message will be displayed: ”*Form has errors. Bad credentials*”.

After 3 consecutive incorrect entries the account will be blocked. In order to unblock the account, the legal representative / agent of the company in the relationship with the bank needs to contact ING Bank at 021 403 83 04.

2.3.3. Logout

In order to close the session, select the Logout button at the top right of the screen.

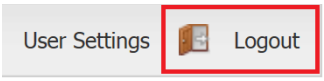


Figure 2

2.4. Viewing transactions

By selecting the Orders option from the main menu (Fig. 3). The menu will load automatically within seconds of logging in.

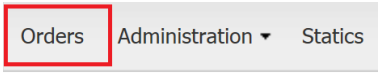


Figure 3

The platform allows the viewing of transactions according to certain selection criteria available in the Filter menu (on the left side of the screen). The transactions will be displayed in the order of their performance: **the most recent in the selected time period.**

You can update the list of transactions at any time (e.g. in order to include new ones) by selecting the Search button.

2.4.1. Filtering and displaying transactions

By accessing the options available in the Filter submenu (Fig. 3.1), you can search and view transactions according to the following selection criteria:

- Period From – To
  - ✓ The displayed transactions will be those performed during the selected period, they may be approved or rejected according to the Order Status, or may be limited by other selection criteria.
- Minimum and maximum amount: Maximum / Minimum amount
  - ✓ The displayed transactions will be those with the authorization amount comprised during the selected period, they may be approved or rejected according to the Order Status, or may be limited by other selection criteria.
    Warning! The value entered in both fields must comply with the format "0.00", otherwise the filtering will not be performed.
- Payment status: Order Status – Created, Approved, Declined, Reversed, Deposited, Refunded
- Reference: Reference number
  - ✓ It allows the identification of a single transaction depending on the internal reference “RRN” usually used by ING Bank; it can be useful in communicating with the Bank
- Order number: Order number
  - ✓ Allows the identification of a single transaction depending on the reference granted at the time of payment by ING Bank or transmitted by the Merchant (see Chapter 3.7.1), and displayed on the payment page; may be useful in the communication with the payer or the Bank
  - ✓ The order number is set automatically to be sent by ING. If the Merchant transmits this parameter, it is very important to notify the bank, in order to change this setting. (see Chapter 3.7.1)
- Other specific criteria.

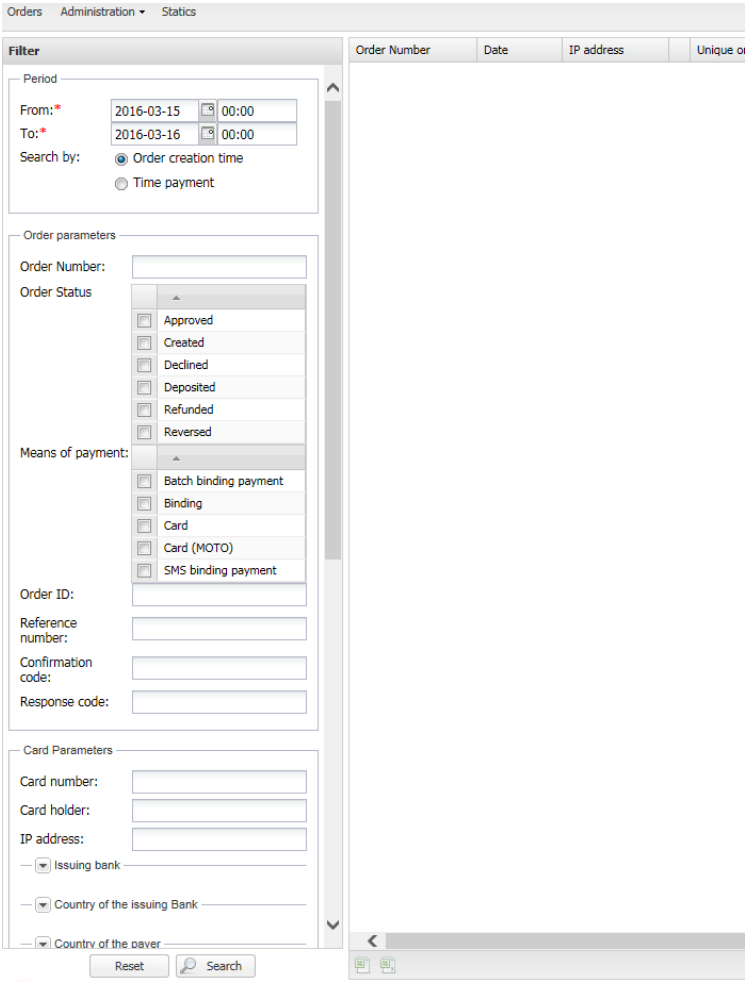


Figure 3.1

WARNING!

Selection criteria remain active throughout the session, which can create confusion when transactions are selected without taking into account the previously used criteria. Therefore, in order to update transactions, access the Reset button, and then other selection criteria can be applied or the selection criteria can be modified, and then access the Search button for updating.

2.4.2. Downloading transactions

In order to download a transaction or a list of transactions on the local station for processing by various software, access the "Export to Excel" option or the "Export to CSV" option available at the bottom left of the screen (Fig. 3.2).

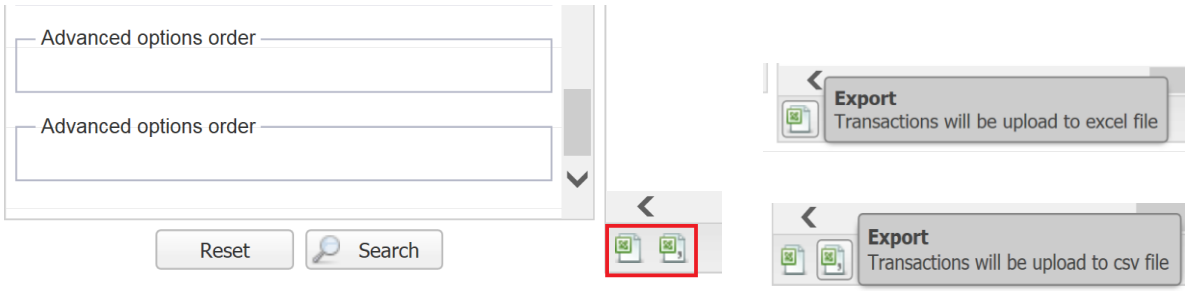


Figure 3.2

2.4.3. Selecting a transaction

The additional details of a transaction can be accessed by double-clicking on the transaction. These details will be displayed in a separate tab in the used browser. (Fig. 3.3):

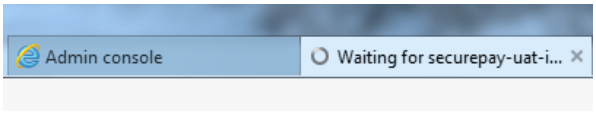


Figure 3.3

2.4.4. Canceling a transaction

After selecting the transaction (see Chapter Figure *3.2 2.4.3. Selecting a transaction*), you can cancel a transaction until COT (22.00) by accessing the Reverse option available in the newly opened tab (Fig. 3.4):

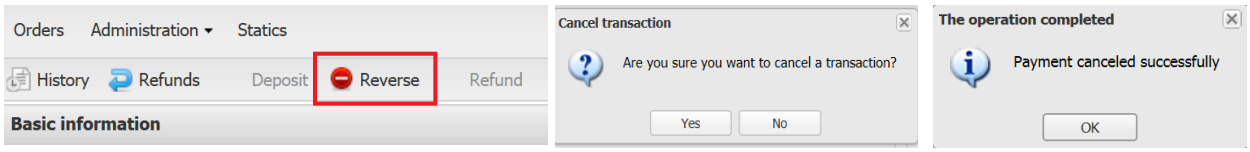


Figure 3.4

The status of the transaction will change to "Reversed". Updating the list of transactions in the Orders menu can be performed by selecting the Search button.

Warning! The option of canceling a transaction is available both for authorizations and for pre-authorizations for their entire duration of their validity or before they are completed.

2.4.5. Refund

After selecting the transaction (see Chapter *Figure 3.2 2.4.3. Selecting a transaction*), you can return a transaction after COT (22.00) by accessing the Refund option available in the newly opened tab (Fig. 3.5). A new window will open, where you need to input the amount to be returned.

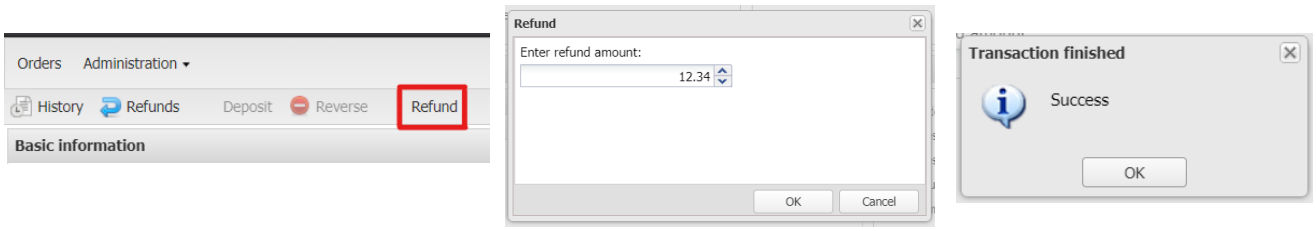
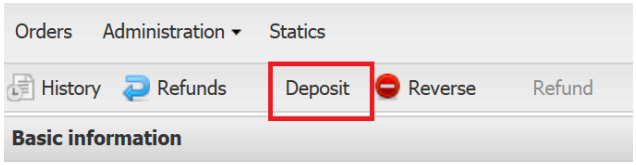


Figure 3.5

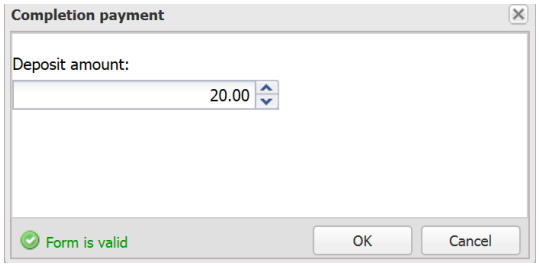
Then, after pressing the “OK” button, a new window will be displayed, confirming the successful performance of the return, and the status of the transaction will be modified to “Refunded”. The updating the list of transactions from the Orders menu can be performed by selecting the Search button.

2.4.6. Completing a pre-authorization

After selecting a pre-authorization transaction (valid only for Merchants with the respective option, (see Figure 3.2 2.4.3. *Selecting a transaction*), it may be completed by accessing the Deposit option (Fig. 3.5):



and entering the amount in the following box:



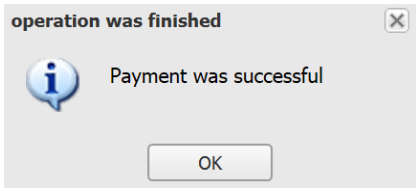


Figure 3.5

Warning! The amount is entered with two decimals by using the point separator "." (e.g: 20.00). A transaction can only be completed for an amount less than or equal to the pre-authorized amount.

After completing the transaction, the Reverse button becomes inactive, and the transaction will have the "Deposited" status (Figure 3.7). The updating the list of transactions from the Orders menu can be performed by selecting the Search button.

WARNING!
The validity term for a pre-authorization is 14 calendar days for transactions performed with VISA/Mastercard cards and 7 calendar days for transactions performed with Maestro cards, starting with the date on which the transaction is performed by the payer. If this term is exceeded, the preauthorization expires and the money cannot be collected. In such situations, the payer must perform a new approved transaction.

! If a pre-authorization is completed after the afore mentioned term, please check in the History menu (Figure 3.6) the correct result of this operation, because the status of the transaction will not change in the interface (the transaction will still have the Approved status).

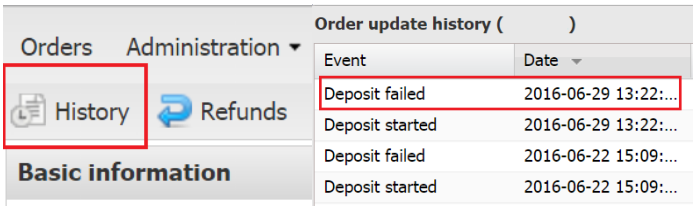


Figure 3.6

Completions cannot be canceled later, if you want to return the completed amount, you need to contact the assistance department at 021 403 83 04 or to submit a specific application at the ING Bank headquarters.

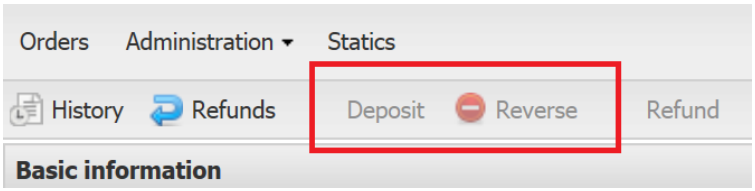


Figure 3.7

The completion of a pre-authorization can be performed even from the web interface by a WebService. For more details on this option, please check Chapter 3.7.3.5.

2.4.7. Order details (status, settlement, time-out, colors)

The table below represents all possible statuses of an order:

	State name in the console	Internal name	Description
1	CREATED	started	The order was created
2	APPROVED	payment_approved	The order amount was preauthorized successfully
3	DECLINED	payment_declined	Authorization / preauthorization was declined
4	REVERSED	payment_void	The order was reverced
5	DEPOSITED	payment_deposited	Money were deposited
6	REFUNDED	refunded	Money were refunded

When a cardholder begins to pay, the status is "Created" and goes to the "**Deposited**" status after the transaction is authorized (when it was successfully completed). If it is not successfully completed, it goes to "**Declined**", and if it is subsequently reversed, to "**Reversed**".

The **status** in which the transaction can be considered successfully completed and the product can be released is "**Deposited**". In order to find out the result of the transaction online (in real time), the communication protocol indicated in Chapter III, section 5.3 must be implemented (for details discuss with the person who ensures technical assistance, the one who implemented the card payment service).

A **payment session** remains open for **10 minutes**, and then the transaction ends with "time out".

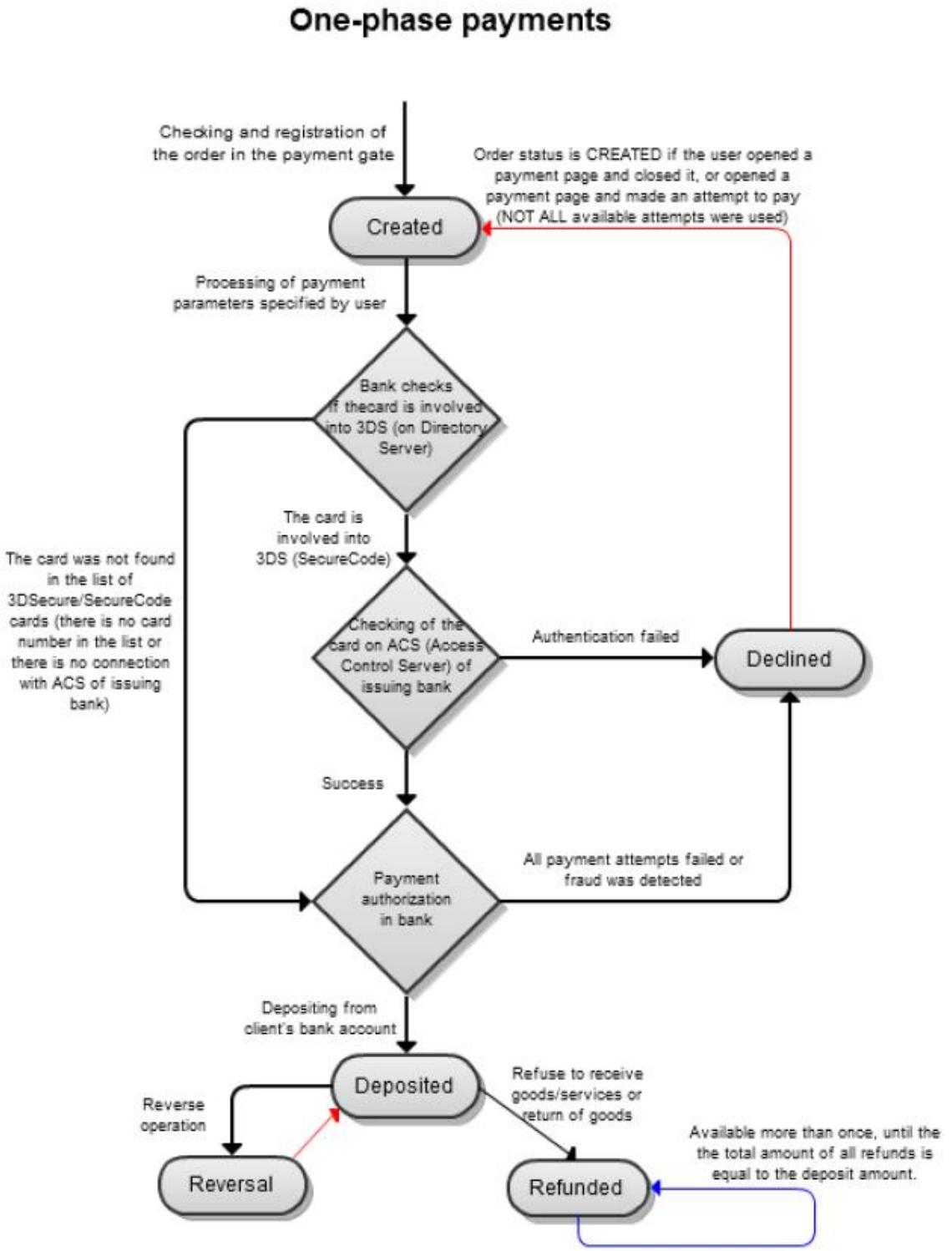
The duration of passing from one status to another depends on the duration of the actions that take place between statuses. For example., if the customer of the store (card holder) takes longer to validate the 3D Secure password, the transition from "Created" to "Deposited" will be longer.

A payment is already collected in the merchant account if, by accessing its details (double-clicking on the payment), in the History menu, the stateExplanation field has the final status "Day Ended".

The **settled amounts** can be seen in the e-commerce account the day after the date when the payments (authorizations) were performed by the customers of the store (for the transactions performed before COT 22.00, when the settlement takes place automatically).

Payment **reports** can be obtained from the application, both via the reporting user and via the administration user. Access Orders -> Filter -> The intended filtering criteria are applied -> Search-> Export to Excel/ Export to CSV (the ones for which the money will be collected are those with the status “Deposited”).

The **colors** from the application related to the "State" field (yellow, green, red) are not related to the amounts collected in the account, the transactions that were rejected or accepted, etc., but they are strictly for the internal use of the bank.



2.5. Changing the password

By accessing User Settings - Change password (Fig. 4), you can change the password of a User.

WARNING!

The passwords accepted by ING Bank are complex passwords, consisting of at least 8 characters, at least one special character (e.g. $, #, & etc ...), at least one digit and at least one capital letter. No spaces.

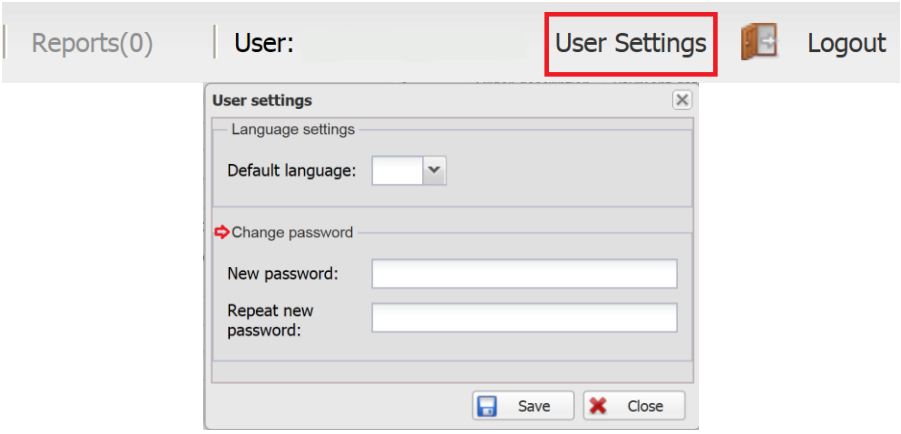


Figure 4

2.6. Technical and operational assistance

For any information or notifications, please call (021) 403 83 04 or send an e-mail to supportwebpay@ing.com
The situations in which specialized support is needed can be the following:

- Impossibility of accessing the ING WebPay administration page
- Problems in viewing transactions or downloading transactions
- Impossibility of changing a password
- Impossibility of carrying out transactions by card holders on the payment page
- Questions about the status of a transaction
- Other similar situations

Chapter III - API User's Manual

ING WebPay API

Technical specifications

This document describes the technical steps that are required in order to connect the merchant's site to the ING WebPay service, in order to initiate transactions and obtain the authorization status for each transaction. The documentation is intended for the technical contact person(s) designated by the Merchant in order to develop the application.

3.1. Definitions

Management console: web interface for the ING WebPay service, used by the merchant to view, cancel and edit transactions

ING WebPay: the ING Bank server that hosts the Payment Page and the Merchant Administration Console

API user: the technical user assigned by ING Bank to the technical contact of the Merchant, in order to introduce and verify payments via the ING WebPay API.

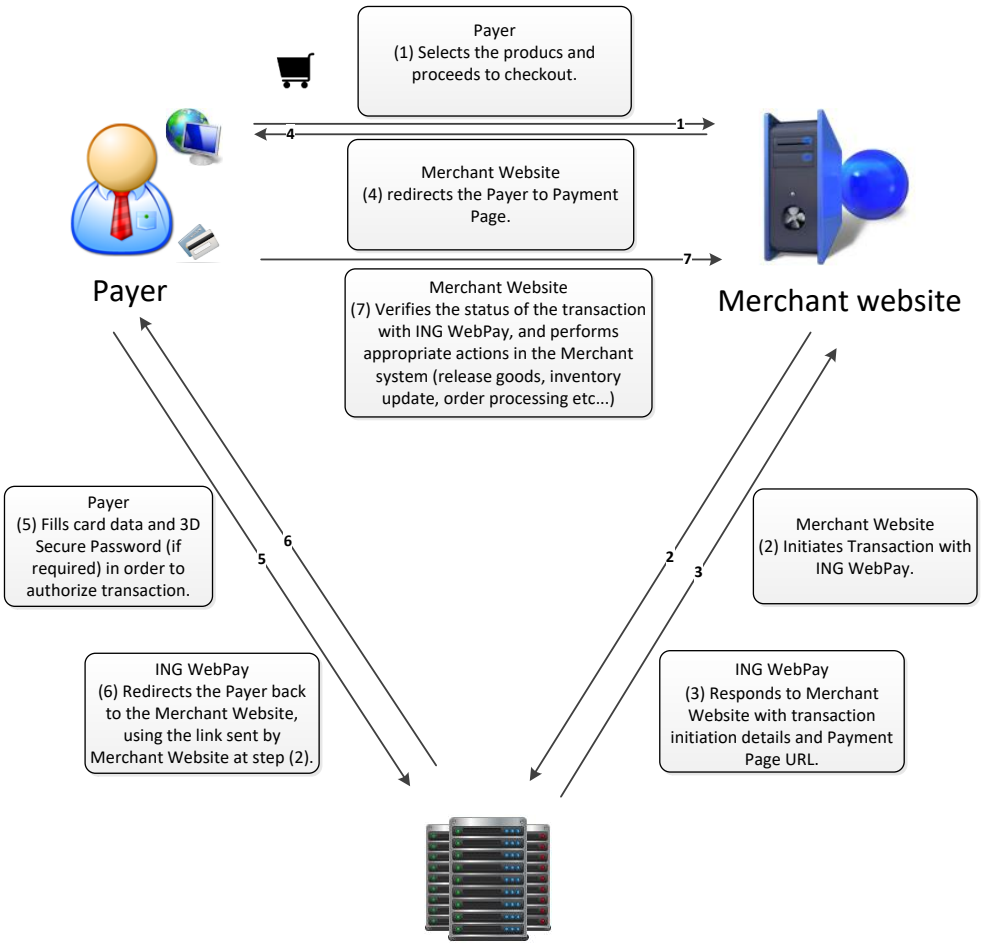
Merchant site: a server belonging to the Merchant, which includes the shopping cart and the back-office functionality

Order ID: Unique ID assigned by ING WebPay to a transaction

Payer: the person who intends to purchase commercial goods by using the card

Payment page: web page hosted on the ING WebPay server which will be used for collecting the card holder’s data

3.2. Process of an E-commerce transaction



3.3 First steps before implementing the API:

1. Before beginning the implementation of the API, the API User and the appointed person in the relationship with the Bank ("Technical Contact" / API User) will receive at the e-mail address indicated in the Application for granting ING WebPay, the details of the test environment (API username / password and Administration username / password for test environment)
2. Follow the steps indicated in the email and the ones below.
3. After receiving the API user codes and passwords related to the test environment, Support WebPay will request, by e-mail, the company logo in .jpeg format, size 160x60 px and the information outlined below, in order to customize the payment page:

** The transaction is processed by ING Bank NV Amsterdam - Bucharest Branch on behalf of XXX (name of the merchant / company / name of the company that owns the site). Your card details are not made available to the merchant.*

*** If the bank which issued your card and your card participate in the 3DSecure system, on the following screen you will be invited to enter the authentication data for 3DSecure.*
For further details on processing your order, please contact the merchant XXX (name of the merchant / company / name of the company that owns the site) at telephone number ZZZ or at e-mail address xxx@yy.ro.

Warning! When implementing the ING WebPay service in several currencies (RON/EUR), ING Bank will create and send by e-mail different usernames and passwords for each currency. Therefore, the implementation will be performed twice, for both sets of users.

3.4. "Pay By Link" function

The merchant has the possibility of implementing the "Pay by Link" function in accordance with the General Conditions attached to the Internet Card Acceptance Agreement and this Guide.

The ING WebPay service allows the merchant to implement the "Pay by Link" function by using the same parameters for initiating the transaction, and the payment process is described in the following Chapters.
The difference occurs when the order is initiated. Traditionally, the order is created by the customer directly on the merchant's website, by selecting and adding in the shopping cart the desired products / services. In the case of "Pay by Link" the order is created by the merchant and sent by e-mail to the customer in the form of a link managed by the declared website of the merchant containing the order details: the "check-out" page.

For the implementation of the "Pay by link" function, please observe the following requirements:

- The payment process will be described clearly and correctly on the merchant's main site, along with the other payment methods
- The following information will be displayed on the site: Delivery terms and conditions; Product return policy; Complaint resolution policy; All sections required by the Regulations of the Card Organizations or the national legislation mentioned in the contractual documents.
- The link of the "check-out" page administered by the merchant's declared site will be sent to the customer by e-mail (Warning! not the ING Bank payment page).
- In order to access the "check-out" page, the client will be required to log in (e.g. username and password)
- We recommend that the "check-out" page be of the "https" type or the "check-out" page mention that the payer will be directed to the secure "https" payment page. These items must be verified by the payer before the transaction is authorized, in order to avoid the risk of phishing.
- The "check-out" page will contain the following information: Company data (sole registration number, name, country of origin, registered office and contact details); Order details (product description, unit price and total price); Delivery method and related cost; Check for the acceptance of the Terms and Conditions, the Return Policy and the Cancellation Policy;
- On the check-out page, the validity term of the offer will be mentioned, in order to avoid the situation where the customer subsequently pays and the offer can no longer be ensured by the Merchant.
- All payment parameters (see Chapter 3.7) will be transmitted by the server of the (declared) site of the merchant and cannot be modified by the payer.

3.5. API authentication

The Merchant site will always initiate requests to ING WebPay for accessing the services. Thus, ING WebPay authenticates the Merchant's Website based on the API User code and the password assigned to the technical contact of the merchant.

In order to prevent web attacks, the Merchant's Website must verify the ING WebPay certificate, thus ensuring that the request is sent by a secure service. The Merchant's site should use a

mechanism that allows the certificate to be changed (if ING Bank updates the certificate) and the possibility to change its configuration manually (if ING Bank uses an expired certificate). Also, please refer to the document "hosted_payment_page_security_visa.pdf" or check the Visa Europe security updates. The Merchant's Site needs to meet the PCI DSS security standards and it needs to be constantly updated. Do not use your local browser to call the API (e.g. AJAX), in order to avoid disclosing the merchant's password.

3.6. Description of API fields

In order to implement the ING WebPay e-commerce service, please follow the steps below. If your site uses an "open source" E-commerce platform, please inform by e-mail our support service (SupportWebPay@ing.ro) in order to verify the possibility of installing plug-ins for installation.

3.6.1. Transaction initiation

The Merchant site initiates a transaction by sending an HTTPS message to https://securepay.ing.ro/mpi/rest/register.do in order to perform the sale (if you are not sure about the type of the transaction you need to initiate, please talk to the ING Bank representative about possible versions) or https://securepay.ing.ro/mpi/rest/registerPreAuth.do for the preauthorization payment version with the specifications below. For further details on pre-authorizations, see chapter *3.7.3.5. Completion or reversal of Pre-authorized transactions*.

(For the test environment, please check the URL links presented in chapter 3.9. Steps needed to promote the ING WebPay service in production)

3.6.1.1. Parameters

Field	Type	Mandatory	Value/Comment
userName	AN..30	Yes	API user code of the merchant as provided by ING Bank
password	AN..30	Yes	Password for the API user code of the merchant, technical contact of the merchant For further details, check the API authorization
currency	N3	Yes	Mandatory parameter 946 for transactions in RON. 978 for transactions in EUR.
orderNumber	AN..32	Yes/No	The sole identification element of a transaction; may be set by the Merchant or may be assigned automatically by ING WebPay. The orderNumber parameter will be automatically assigned by ING WebPay. If set by the Merchant, ING must be informed in order to avoid the rejection of the transaction. Please verify the details below*
description	AN..512	No.	The description of the transaction may be sent by the merchant and shall be displayed on the ING WebPay platform. The field may be left empty.
amount	N..20	Yes	The value of the transaction without the decimal separator For example, 102.31 is sent as 10231.
returnUrl	AN..512	Yes	The URL link to which the payer will be redirected by ING WebPay after the authorization of the transaction The URL link will be sent in an unencoded form.
language	A2	No.	ro or en depending on the language set by the payer. A default value is set for each merchant.
email	AN	No.	The option set by default by the bank. The e-mail address must be valid.
reconciliationId	AN..20	No.	Fill in the information intended to be exposed in the reconciliation financial reports (it may contain the same information as the “description field”)

orderBundle	JSON	Yes	**{}**
jsonParams	JSON	Yes	Mandatory value of the parameter: {"**FORCE_3DS2**":"**true**"}

***** *- if the system is configured to receive the "OrderNumber" from the website of the Merchant, ING shall not generate this code and shall reject the transaction if it did not receive the OrderNumber from the Merchant*
- if the system is configured to generate the "OrderNumber" without receiving it from the site of the Merchant, and the site sends this parameter, the transaction will be automatically rejected by the system.
- ! We recommend to send this information, if you have it, as based on it the issuer takes the decision to authenticate the transaction. In its absence, the authentication may be rejected because there is not enough information in order to approve the transaction.

ING WebPay replies with the information required for continuing the payment: the link of the payment page and the sole ID of the transaction (OrderId)

3.6.1.2. Reply messages

Name	Type	Mandatory	Value/Comment
orderId	AN..64	No.	The sole ID of the order assigned by ING WebPay to the transaction in progress. The field is not present if the transaction has not been authorized.
formUrl	AN..64	No.	The URL link of the payment page; the site of the merchant must redirect the payer to the payment page in order to fill in the card data required for the payment. The field is not present if the transaction has not been authorized.
errorCode	N3	No.	If there are errors during the initiation of the payment, ING WebPay shall fill in the field with the related error code. Please refer to table 3.7.1.3.Error codes
errorMessage	AN..512	No.	Description of the error returned by ING WebPay (displayed in the language requested during the initiation of the transaction)

3.6.1.3. Error codes

Value	Description
0	No error encountered.
1	Duplicated order
3	Unknown or forbidden error. A mandatory
4	parameter has not been specified. Incorrect value
5	of a requested parameter. System error.
7	

3.6.1.4. Possible error messages

Value	Description (adapted by ING Bank for the transaction language)
1	An order with the same number has already been processed.
1	An order with the same number has been registered but not paid
3	Unknown value.
3	Incorrect value.
4	The "Currency" parameter is missing

4	The “Language” parameter is missing
4	The “orderNumber” parameter is not filled in
4	The “Merchant name” parameter is not filled in
4	The “amount” parameter is not filled in
4	The “returnUrl” parameter is not filled in
4	The “password” parameter is not filled in
5	The “Amount” parameter is incorrect
5	The “orderNumber” parameter is incorrect
5	The name of the merchant is unknown
5	The “Language” parameter is incorrect
5	The “orderId” parameter is incorrect
5	The “password” parameter is incorrect
5	The username is inactive
7	System error

3.6.1.5. Example of an initiation reply message (test environment)

Resp: {"formUrl":"
https://securepay-uat.ing.ro/mpi_uat/merchants/teste_eod/payment_en.html?mdOrder=86faed41-d33b-4f10-b3bf- 9c2a98ba4bd7","orderId":"86faed41-d33b-4f10-b3bf-9c2a98ba4bd7"}

The site of the merchant should redirect the payer to the payment page in order to fill in the card data.

3.6.2. Authorization performance

The payer will fill in the card data on the payment page, and ING WebPay will authorize the transaction. If necessary, ING WebPay will redirect the payer to the server of the issuer for the 3D Secure authentication.

After the transaction is initiated, ING Bank will redirect the payer to the web page from the return URL (returnUrl) described in Parameters, and the site of the Merchant can check the status of the transaction by accessing the API.

3.6.3. Obtaining the transaction status

In order to request details regarding the initiated transaction, the site of the Merchant will send an HTTPS message to https:// securepay.ing.ro/mpi/rest/getOrderStatus.do with the following fields:

Field	Type	Mandatory	Value/Comment
orderId	AN..64	No.	The sole ID of the transaction assigned by ING WebPay to the transaction in progress. The field is not present if the transaction has not been authorized.
userName	AN..30	Yes	The API user code of the merchant as provided by ING Bank
password	AN..30	Yes	The password for the API user, set by the technical contact. Please verify the API authentication
language	A2	No.	ro or en depending on the language set by the payer. A default value is set for each merchant.

ING WebPay replies with the necessary information:

3.6.3.1. Reply message

GetOrderStatus:

Name	Type	Mandatory	Value/Comment
OrderStatus	N2	No.	Payment status. The value is selected out of the versions described below. This parameter is missing if the status does not correspond to those from the list.
ErrorCode	N3	No.	If there are errors during the initiation of the payment, ING WebPay shall post the error code in this field. Please refer to table 3.7.3.3. Error codes.
ErrorMessage	AN..512	No.	Description of the error returned by ING WebPay (the message is displayed in the language used when initiating the transaction)
OrderNumber	AN..32	yes	A parameter sent to the site of the Merchant in Parameters or automatically assigned by ING Bank, depending on the option of the Merchant (see Chapter 3.7.1.1).
Pan	N..19	no	Truncated number of the card used for payments. Indicated only for paid orders.
expiration	N6	no	Expiry date of the card in YYYYMM format. Indicated only for paid orders.
cardholderName	A..64	no	Name of the card holder. Indicated only for paid orders
Amount	N..20	yes	Value of the payment in minimum monetary units (cents, “bani”).
depositAmount	N..20	yes	Value of the payment collected in minimum monetary units (cents, “bani”).
currency	N3	no	Payment currency code according to ISO 4217. 946 for RON, 978 for EUR
approvalCode	N6	no	Authorization code IPS
authCode	N3	no	Transaction authorization code
Ip	AN..20	no	Ip address of the payer
clientId	AN..255	no	Client code (identifier) in the Merchant’s system. Used for applying a connection. Present only if the merchantis allowed to create this connection (future function)
bindingId	AN..255	no	The connection identifier created during the payment of the order or used for payment. Present only if the Merchant is allowed to create this connection (future function)

GetOrderStatusExtended

Name	Type	Mandatory	Value/Comment
ErrorCode	N3	No.	If there are errors during the initiation of the payment, ING WebPay shall post the error code in this field. Please refer to table 3.7.3.3. Error codes.

ErrorMessage	AN..512	No.	Description of the error returned by ING WebPay (the message is displayed in the language used when initiating the transaction)
OrderNumber	AN..32	Yes	A parameter sent to the site of the Merchant in Parameters or automatically assigned by ING Bank, depending on the option of the Merchant (see Chapter 3.7.1.1).
OrderStatus	N2	No.	Payment status. The value is selected out of the versions described below. This parameter is missing if the status does not correspond to those from the list.
ActionCode	N6	Yes	The reply code generated by the internal transaction authorization system.
ActionCodeDescription	AN..600	No.	The description of the transaction, may be sent by the merchant and will be displayed on the ING WebPay platform. The field may be "null" if the Merchant does not send this parameter when the transaction is initiated. It is the content of the text included in the description parameter sent to the register.do service
Amount	N..20	Yes	Value of the payment in minimum monetary units (cents, "bani").
Currency	N3	No.	Payment currency code according to ISO 4217. 946 for RON, 978 for EUR
Data	TIMESTAMP6	Yes	Transaction date
OrderDescription	AN..512	No.	The description of the transaction may be sent by the merchant and shall be displayed on the ING WebPay platform. The field may be "null" if the Merchant does not send this parameter when the transaction is initiated.
Ip	AN..20	No.	Ip address of the payer
merchantOrderParams	AN..1024	No.	These are additional parameters for certain payments. In case of standard payments the field is not populated.
attributes	AN..250	No.	The orderNumber for the query payment is returned. Practically it is a request echo of the form: "attributes":[{"name":"mdOrder","value":"246f1288-7ba9-4c3f-ab3d-65125ce3f73f"}]
cardAuthInfo	AN..130	No.	This parameter comprises: The card expiry date in format YYYYMM; card holder's name; authorization code received from the issuing bank, Truncated number of the card used for the payment. Details are indicated only for paid orders; "cardAuthInfo":{"expiration":"201804","cardholderName":"test","approvalCode":"448520","pan":"425603

Value	Description
0	Order registered but not paid
1	Preauthorized payment (for 2-step transactions)
2	Authorized transaction
3	Cancelled transaction
4	Reversed transaction
5	Transaction initiated by the ACS system of the issuing bank
6	Rejected transaction

„getOrderStatus" does not return the status description. For detailed information, the web service

„getOrderStatusExtended” may be used. Both services use the same parameters only the reply is different.

The production link for „getOrderStatusExtended” is:
https://securepay.ing.ro/mpi/rest/getOrderStatusExtended.do

3.6.3.4. Error codes

Value	Description
0	No system error
2	The transaction is refused, as there are errors in the payment credentials.
5	Incorrect value of a parameter.
6	Unregistered OrderId

3.6.3.5. Examples of reply messages for the transaction status:

Example for „getOrderStatus”

Resp:
{"expiration":"201512","cardholderName":"testc","depositAmount":0,"currency":"946","authCode":2,"ErrorCode":"2","ErrorMessage":"Payment is declined","OrderStatus":6,"OrderNumber":"12266","Pan":"425601**0206","Amount":100,"Ip":"192.168.5.158"}

Example for „getOrderStatusExtended”

{"errorCode":"0","errorMessage":"Success","orderNumber":"107370","orderStatus":6,"actionCode":210,"actionCodeDescription":"TransactionDenied","amount":100,"currency":"946","date":1403680642722,"orderDescription":"null","ip":"193.17.195.110","merchantOrderParams":[],"attributes":[{"name":"mdOrder","value":"ff0b026c-c319-4e0f-af1f-230834b0eaec"}],"cardAuthInfo":{"expiration":"201604","cardholderName":"testc","pan":"425603**2773"}}

3.6.3.6. Completion or reversal of Pre-authorized transactions

In case of pre-authorizations (initiated by https://securepay.ing.ro/mpi/rest/registerPreAuth.do), two actions are possible: reversal (cancellation) or transaction completion.

The reversal (cancellation) of a transaction may be performed in two ways:

1. By the administration console, log in by using the administration user code, select the respective transaction (Status Approved), then press the “Reverse” button. (Please refer to chapter 2 – 2.4.4. Canceling a transaction).
2. By sending an HTTPS message to https://securepay.ing.ro/mpi/rest/reverse.do with the following parameters: User, password, orderID.

Completion may be performed in two ways:

1. By the MPI platform, log in by using the administration user code, select the respective transaction (Status Approved), then press the “Complete” button and input the transaction amount. (Please refer to chapter 2 - 2.4.5. Completing a pre-authorization)

2. By sending an HTTPS message to https://securepay.ing.ro/mpi/rest/deposit.do with the following parameters: preAuth Order id (generated when initiating PreAuth), Language, Amount, User and password. If the sent amount is 0, the transaction is automatically completed with the initial amount.

Please note that you cannot complete the preauthorization for an amount higher than the one that was initiated.

WARNING!
The validity term for a pre-authorization is 14 calendar days for transactions performed with VISA/Mastercard cards and 7 calendar days for transactions performed with Maestro cards, starting with the date on which the transaction is performed by the payer. If this term is exceeded, the preauthorization expires and the money cannot be collected. In such situations, the payer must perform a new approved transaction.

! If a preauthorization is completed after the aforementioned interval, please check in the History menu (Chapter 2.4.5 Completing a preauthorization) the correct result of this operation, as the transaction status will not be modified in the interface (the transaction will continue to have the status Approved).

3.7. "email confirmation for orders" function

This function involves the automated transmission by e-mail of the payment confirmation, both to the payer (see Chapter 3.7.1.1.Parameters), and to the Merchant.

Each payment confirmation may contain the following information:

- *Amount* and *Currency*
- *Status*
- *OrderNumber*
- *Merchant name*
- *Cardholder name*
- *Date*
- *Order Description*

This function is activated as follows:

- Merchant - activated based on the option expressed in the granting application (ING WebPay) or the data modification application (ING WebPay)
- Payer - activated based on the option of the Merchant expressed by sending the e-mail address of the Payer by the ING WebPay application. The Merchant assumes the responsibility of getting the consent of the payer for the Bank to use the e-mail address as a means for sending the payment confirmation and ensuring the validity of the e-mail address.

3.8. Test scenarios

At least an approved transaction.
At least a refused transaction (incorrectly inputting the card expiry date or CVV2)
At least an approved transaction, but reversed by the Administration User.

! **Recommendation:** when performing tests, the amounts must be different for each initiated transaction.
The API user is not entitled to check the test transactions in the administration console.

In order to check operations with test cards, Administration / Reporting users must log in at https://securepay-uat.ing.ro/consola/index.html (for additional details please check "Chapter 2" of this Guide)

The Reporting User only has rights for viewing and drafting reports in the ING Webpay administration console. The Administration User, besides the rights of the reporting User, also has the possibility of cancelling or changing a transaction on the same day of its performance, when this is carried out prior to the closing of the day and of modifying a preauthorized transaction.

3.9. Necessary steps for promoting the ING WebPay service in production:

1. After implementing the test scenarios indicated in Chapter 3.8, you must send an e-mail to: SupportWebPay@ing.ro and inform us that you wish to promote the E-commerce service in production;
2. The WebPay Support team implements the payment solution, by checking the following aspects:
   - The site does not expose sensitive data to the local browser (e.g. API user code and password);
   - Clear confirmation messages are sent for approved/rejected transactions;
   - All the data is sent in the format accepted by the systems of the bank.
3. Also, in this step the Bank performs a final verification of the site, and if it identifies aspects that do not comply with the internal and external regulations (VISA/Mastercard), they will be notified in order to be remedied before the activation of the payment service. If the identified problems cannot be remedied, the Bank may take the decision to terminate the Acceptance Agreement. If the tests are successfully completed, ING Bank generates the credentials for the production environment. Each user, including the API user, will receive an e-mail with the production password and will have to follow the steps indicated in the Guide (Chapter 2), in order to activate the user codes.
4. The director of the company must call the Customer Service of ING Bank at telephone number (021) 403 83 04 in order to obtain the user codes of each person appointed in the application for granting the e-commerce service (only the password is sent in the e-mail).
5. After activating the API user, in the production environment in the MPI console (https://securepay.ing.ro/consola/index.html), please modify the following URL links in the developed script (by replacing the TEST link with the LIVE one):

Name	TEST	LIVE
Register	https://securepay-uat.ing.ro/mpi_uat/rest/register.do	https://securepay.ing.ro/mpi/rest/register.do
Pre-authorization	https://securepay-uat.ing.ro/mpi_uat/rest/registerPreAuth.do	https://securepay.ing.ro/mpi/rest/registerPreAuth.do
getOrderStatus (if you use it)	https://securepay-uat.ing.ro/mpi_uat/rest/getOrderStatus.do	https://securepay.ing.ro/mpi/rest/getOrderStatus.do
getOrderStatusExtended (if you use it)	https://securepay-uat.ing.ro/mpi_uat/rest/getOrderStatusExtended.do	https://securepay.ing.ro/mpi/rest/getOrderStatusExtended.do
Web Service Reversare*	https://securepay-uat.ing.ro/mpi_uat/rest/reverse.do	https://securepay.ing.ro/mpi/rest/reverse.do
Web Service Fill In*	https://securepay-uat.ing.ro/mpi/rest/deposit.do	https://securepay.ing.ro/mpi/rest/deposit.do

*In order to use these web services, the person appointed in the relationship with the bank / legal representative must ask the bank to grant these additional rights based on a standardized form.

6. If you have managed to implement the service in production, please send an e-mail to SupportWebPay@ing.ro with the address of the site.

7. The ING technical team will check the ING WebPay service by performing a transaction with a valid card, which will be displayed as rejected (this only checks that the systems are connected and a reply is received).
8. The director of the company will receive a confirmation e-mail that everything is all right and that the card payment becomes accessible to the clients of the site. Until the reception of this e-mail the service is suspended. This confirmation e-mail will also send the financial data of the service (Merchant ID, Terminal ID, IBAN, etc.).

For any technical issue, do not hesitate to contact the ING WebPay support service at e-mail address: SupportWebPay@ing.ro.

Chapter IV – Test data for simulating transactions and testing the functions of the ING WebPay application - test environment

In order to simulate transactions and test the functions of the ING Web Pay application in the administration console, you may use the test data indicated below. The transactions performed in the test environment do not involve a real fund transfer.

User codes:

- API user code: **TEST_API** & password: **q1w2e3r4Q!**
- Administration user code: TEST_ADMINISTRARE & password: Ing.12345!

!Warning Please do not modify the authentication passwords of the aforementioned users, as the data may also be used by other merchants.

Administration console: https://securepay-uat.ing.ro/consola/index.html
Transaction simulation link: https://securepay-uat.ing.ro/mpi_uat/merchants/testecomerciant/test.html
Card data (test):

Type	Details
Visa	4256031168525366 Cardholder Name: ING VISA Exp. Date: 05/21 CVV2: 865 3D Secure Password: test123!

!**Warning** The administration console (test environment) is provided to the applicant, for informational purposes, only as a test environment. The aforementioned test data may be used only for the purpose indicated in the first paragraph of this Chapter. The ING WebPay E-commerce Service Guide is provided to the applicant only in order to present the technical solution provided by ING Bank related to the internet card payment acceptance services and the characteristics of the ING Web Pay application.

By accessing the administration console - test environment, the applicant accepts the conditions indicate in this chapter and understands that it provided the aforementioned test data and of the ING WebPay E-commerce Service Guide for purely informational purposes, and this does not represent an offer from ING Bank or ING Bank assuming any obligation to conclude an agreement with the applicant for internet card payment acceptance services.

Consequently, any implementation / development performed by the beneficiary of the administration console - test environment on its computer data, based on the test data indicated in this Chapter, in order to perform transaction simulations and test the functions of the ING Web Pay application in the test environment is under the full responsibility of the beneficiary of this test data and on its expense, and the liability of ING Bank

cannot be bound for any costs incurred by the beneficiary, if its request to provide the E-commerce service (ING WebPay) is not approved by ING Bank.