

# **Electronic Card Transactions on the Internet**

**CIB Bank Zrt.**



**Internet-based Card Acquiring Service**

**Technical Documentation**

**Best practices**

## Contents

<b>PREAMBLE.....</b>	<b>3</b>
<b>THE INTEGRATION PROCESS.....</b>	<b>4</b>
<b>TEST CRITERIA .....</b>	<b>5</b>
<b>TRANSACTION ERROR CODES.....</b>	<b>7</b>



## **Preamble**

This document provides guidelines for the development of the CIB Bank payment module at the webshop. It contains the information necessary for customer notification and for integrating the module as fast as possible.

## The integration process

After the contract has been signed, the Bank makes available to the Webshop operator this document package (including the sample source and binary codes), as well as the support necessary for development and integration.

### *Development and integration phase*

The bank provides the Merchant the descriptions, sample programs and encryption keys necessary for the development, and provides continuous support for the period of the development phase. The support is provided by e-mail. In case of e-mail support, please always indicate the following data:

- Designation of the merchant's system
- Exact designation of the operating system running the merchant's application package (in case of unix-based systems the kernel version as well)
- Exact designation of the application environment, including the version number
- Exact description of the problem, the steps of the reproduction, data supporting identification (transaction ID, time stamp, IP address, etc.)
- In case of a program error, the relevant part of the code

The bank keeps contact with the Merchant using the e-mail address specified by the Merchant in the contract

### *Testing phase*

At the end of the integration phase, the Bank's testing staff execute a test purchase, in the course of which they make sure that the webshop complies with all the technical and business conditions (the conditions are set out in the section entitled "Test criteria"). Testing can be requested in an e-mail message sent from the e-mail address registered in the contract, specifying the following data:

- Webshop address
- Merchant identifier (AAA9999 format)
- If necessary, the customer profile data prepared in advance (user ID and password)
- Short description of the purchase process
- In case of mobile application, the method of downloading the app, or the installation kit

The test results will be documented, which the bank's employees will send to the webshop's contact person by e-mail. Depending on the errors detected during the test, the testing phase may consist of one or more consecutive tests, each lasting for 2 or 3 days on average.

### *Go live phase*

After successful testing, the bank permits the merchant to use the bank's production eCommerce system. The activation process consists of the following steps:

1. The bank's staff send an e-mail message containing the activated encryption keys in an encrypted attachment, to the merchant's e-mail address registered in the contract.
2. The password ensuring the encryption of the zip files is personally delivered at a branch chosen by the Merchant.
3. The bank's employees complete the registration of the Merchant's data in the production environment.
4. The bank's staff send to the Merchant an e-mail containing the production web addresses and the confirmation of the activation.

The go live phase lasts for 1 or maximum 2 working weeks on average.

## Test criteria

It is in the webshop's and the bank's common interest to ensure that, after the go live, customers be able to pay with their bank cards as efficiently as possible, and that these conditions be fulfilled as soon as possible. The bank's staff provide support for this purpose, such as addressing any protocol-related issues occurred during the development (except for any environmental and programming language particularities of developments completed in the individual environment, although we do our best to also address these issues), as well as the overall testing of the completed module.

During the testing process, the staff of CIB Bank check the operation of the webshop, against both business and technological criteria. The purpose of the testing is to ensure that, during the bank transactions, all three participants (the customer, the webshop and the bank) are provided with all the available (and permitted) information.

The list below includes a non-comprehensive recommendation, on the basis of which the bank's employees can complete the testing of the webshop prior to activation.

### *Display of the bank's logo*

The webshop is obliged to display CIB Bank's logo on the main page of the webshop and on the page on which the possible payment methods are presented. The logo must point to the <http://www.cib.hu/> website or to the 'Customer information' page. Any of the CIB logo files available in the annex of the documentation may be used as a logo. The following text must be displayed together with the logo: "Card payment service provider:"

### *Display of card logos*

Similarly to the bank's logo, the logos of the accepted bank card types must also be indicated, in a place that is clearly visible by the customer (in the header, at the bottom of the left-hand side menu line, on the right or left hand side of the footer). The logos need not be placed as links, and the text assigned to them must be: "Accepted cards:" The VeriSign (Norton) logo can only be indicated on the website of the webshop if it has its own certificate to this effect.

### *Accessibility of the bank's payment information*

The information that constitutes a part of the documentation must be indicated in a place easily accessible by the customer. If this is not the login page, it must be indicated there in the form of a link pointing to it. The text that accompanies the link may be one of the following: "Help", "Customer information", "Purchase conditions", "Payment methods" or "Bank card payment". It is also compulsory to indicate the merchant's availability (tax number, registered office, phone and e-mail), as well as the General Terms of Contract and the guarantee conditions.

### *Indication of the HUF value of the payable amounts*

The price of each product/service available for purchase must be indicated in Hungarian forint value, even if the webshop can only launch euro-based transactions. In this latter case, the euro value must also be indicated. The forint amount must also be indicated in the case of the shipping cost and the total amount (see section "Description of products/services in the webshop").

### *Description of products/services in the webshop*

All the products/services available in the webshop for purchase must be provided with a short description, consisting of at least a few words, sufficient for clear identification. The prices of the products/services available for purchase must be indicated in advance, prior to their placement into the basket, as follows:

- in each case in forint (the indication may be HUF, Forint or Ft.)
- If settlement is in euro, the price must also be indicated in euro, in addition to the forint amount (the indication may be EUR or Euro)

### ***Customer registration***

The customer's registration in the webshop is not obligatory, although it is strongly recommended in order to facilitate future administration, as no personal data is transferred to the bank. During the registration process the merchant should require the following customer data: name, address, contact details (tel. or e-mail), invoicing or delivery address

### ***Confirmation of transaction outcome***

After the customer returns to the webshop, the merchant must inform him/her on the result of the transaction. This information must contain the following obligatory elements:

- Transaction ID (TRID)
- Transaction result code (RC)
- Text describing the result of the transaction (RC)
- Paid amount (AMO)
- The authorisation number provided by the issuing bank (ANUM)

The text that accompanies the above values must be identical to the elements of the above list.

### ***Timeout management***

The maximum permissible period for card payment is 15 minutes, after which the transaction will be closed. If no transaction closing message (MSGT32) arrives from the webshop prior to closing, the bank reverses the successful authorisation, and it instructs the issuing bank to release the amount reserved on the customer's account. As a result of this the transaction becomes unsuccessful. In order to avoid a timeout, the webshop must, at regular intervals (every 1 or 2 minutes), inquire the bank on the transaction status.

### ***Providing a possibility for repeating the payment***

If the payment is unsuccessful, the customer must be given an opportunity to purchase the content of the same basket as part of a new transaction. In this case, the customer may also exercise his/her right to empty the basket.

## Transaction error codes

In relation to online card payments we recommend that, during unsuccessful transactions, the customers be provided with information on the causes of the errors.

In order to facilitate this process, we have created four groups from the codes available in message 31 in response to message 32. In relation to these groups, we have also formulated those warning messages that facilitate customer information.

### *Possible errors related to the card*

03, 09, 12, 13, 20, 21, 22, 30, 34, 36, 42, 52, 54, 55, 56, 87, 88, 90

- Please check if you have entered the correct card number!
- Please check if you have entered the correct card expiry date!
- Please check if your card is valid!
- If you have an EC/MC card, please check if you have entered the last three digits of the number in the signature field on the back of your card (CVC code)!
- Please check if your card is valid for internet purchases!
- Please check if there is a 3-digit CVV code on the back of your Visa card! If yes, please enter!

### *Possible errors related to the account*

14, 15, 16, 17, 23, 24, 29, 32, 35, 45, 69, 70, 72, 74, 75, 76, 77, 78

- Please check if there is sufficient coverage on your account for this purchase!
- Please check if you have exceeded your approved limit!

### *Possible problems in the connection*

08, 10, 19, 27, 31, 50, 60, 64, 65, 71, 86, 93, A2, A9

- Line probably disconnected during transaction. Please try again.
- Transaction failed due to time-out. Please try again.

### *Possible technical problems*

01, 02, 04, 05, 06, 07, 11, 18, 25, 26, 28, 33, 38, 39, 40, 41, 43, 44, 46, 49, 51, 53, 57, 61, 62, 63, 66, 67, 79, 80, 81, 85, 92, 94, 96, 98, R0, C2, X0, NT

- If you have been returned to the payment page using the browser's 'back', 'reload' or 'refresh' function, the system will automatically reject your transaction for security reasons. Please restart the purchase.