CIB BANK

Electronic Card Transactions on the Internet

CIB Bank Zrt.

eCommerce

Internet-based Card Acquiring Service

Technical Documentation

Frequently Asked Questions

CIB Bank Zrt. CIB Bank Ltd. H-1027 Budapest, Medve utca 4–14. H-1995 Budapest Telephone: (06 1) 423 1000 Fax: (06 1) 489 6500 Court of Registration: Company Court of the Metropolitan Court of Budapest Company registration no.: Cg. 01-10-041004 Tax number: 10136915-4-44 Group tax number:: 17781028-5-44 Group Community VAT number: HU17781028 Stock exchange membership: Budapest Stock Exchange Ltd. Operating licence number: 957/1997/F, III/41. 044-10/2002. BIC (SWIFT) code: CIBHHUHB

Bank of INTESA SANPAOLO

Contents

Questions related to the network

Q: What are the premises of a successful transaction?

A: Only transactions closed (by MSGT32) and acknowledged (MSGT31, RC=00) by the bank may be considered successful. The query message (MSGT33) and its reply (MSGT31) are not sufficient, transactions may still be reversed.

Q: The bank’s server is not answering. Why?

A: The bank’s server does not communicate with the store via TCP ports 80 or 443 that are traditionally dedicated to this purpose, and therefore, if any of the network filters (switch, router, firewall) located between the store’s server and the internet is not prepared for communication via these ports, the request will not reach the bank. The connection can be verified from the store’s server using command-line applications (e.g. cUrl or wget).

Q: Customers from xxx service provider/country cannot reach the payment page. Why?

A: The IP address of the bank’s server is identified by the customer’s internet service provider. The customer’s internet service provider may have synchronisation problems or it may be unable to determine the exact address of the bank’s server for any other reason. In this case the customer is recommended to report the error to his/her internet service provider or, if possible, to retry the purchase via another internet service provider.

Q: The bank’s response is always “500 Server error” or “403 Forbidden”. Why?

A: The bank’s response always arrives in the source (content) of the page, with text/plain mime encoding. In case of successful processing, the http status is 200, but in case of error it is 403 (encryption error) or 500 (processing problem). There are certain connection management devices (applications or functions libraries/classes) on which connection is interrupted immediately in this case, causing the loss of the error message. It is advisable to use devices that are suitable for reading the full content even in case of error.

Q: The answer to all of my questions is RC=D04. Why?

A: Please check if the IP address from which your question was sent has been registered for the bank in advance. If not, please have it registered as soon as possible.

Questions related to encryption

Q: Both encryption and decryption worked perfectly on the test server. Why does it not work on the live server?

A: The bank provides two separate keys for test run and for live operation. The names of these keys are identical, but their contents are obligatorily different. It is the responsibility of the webshop operator to ensure that the keys are delivered to the appropriate locations.

Q: Is it possible to use the IEB0001 identifier with the encryption key provided with it?

A: No. Each merchant receives a unique identifier, none of which may be IEBXXXX. The encryption key that we attached to the documentation and to the ekiCrypt encryption module is only suitable for testing the operation of the attached application, not for bank communication.

Q: Messages A, B and C work perfectly in bank communication, but X and Y do not. What could be the reason?

A: Make sure that all the requests were encrypted using the same key. Since the name of the test key is the same as the name of the activation key, this theoretically eliminates the possibility of using different keys for encrypting messages originating from the same source. In case of divided systems (e.g. cloud-based services), however, it is possible that the installation of the keys on certain elements of the server park was unsuccessful.

Q: We have switched from a server running a Windows-based operating system to a Unix-based one. Why is encryption not working?

A: Unix-based systems differentiate between small and capital letters in file names. If the encryption application returns with a UER_NOFILE error code, it is advisable to check the file name. The web server max also have insufficient privileges reading the file. During installation, a reading privilege must be granted to the technical user of the web server (but only to him/her) with respect to the key file and the directory in which it is stored.

Q: Sometimes the message returning together with the customer (MSGT21) cannot be decrypted. Why?

A: The ekiCrypt functions library and the sakide application built upon it can handle URL-encoded messages, by default. Since the web servers may URL-encode the returning message, the application package may produce an error due to the + and / signs within the message. We recommend that incoming messages be automatically URL-encoded, as this operation "corrects” the URL-decoded message, but does not change anything in the originally URL-encoded message.

Q: Is it possible to use the encrypting algorithm with both 32-bit and 64-bit systems?

A: In the case of technologies applying virtual machines or in case of languages that “hide” hardware particularities, yes. For hardware-specific binaries we have attached a 32-bit and a 64-bit version.

Q: The sakide application has been signalling an error since the operating system upgrade. What shall I do?

A: It is possible that, together with the operating system, some of the (mostly string and memory management) system functions have also been modified, possibly resulting in errors due to different links. In this case, please contact the bank’s contact person, specifying the steps of error reproduction, as well as the exact parameters of the old and the new operating systems and of the hardware on which they run.

Q: How can I verify the authenticity of CIB Bank’s payment page?
A: Primarily by clicking on the green padlock in the browser's address bar. In this case the browser displays all the available information on the confidentiality of the connection, and provides an opportunity for viewing the certificate chain (click here for more information). CIB Bank purchases the certificate necessary for encryption from Symantec Corp., which you can check by clicking on the “Norton-secured” logo in the top right corner of the payment page. If the browser signals that the payment page is not secure, please make sure that you are using the latest version of the browser (older versions may have incomplete lists of the so-called top level root CA certificates) and, if so, please inform us immediately.

Q: The sakide application does not provide any kind of output. Why?
A: If run successfully, the application writes the result on the standard output, whereas in case of error there can be no output at all. For a more precise error finding you should launch the application in verbose mode (-v). This way the error message is transferred to the standard error channel.

Q: The sakide program returns with a UER_BADURL error code. What is the problem?
A: Please check if you tried to apply the encryption in the right direction. Parameter –e is used for encryption, parameter –d is used for decryption. Conversely, the application produces a UER_BADURL error.

Q: The sakide program (or the application implemented in my own system) produced the following encrypted value as a result of the encryption: PID=<kereskedőazonosító>&CRYPTO=1&DATA=AwMD, to which the bank returned an error message. What is the problem with the message?
A: AwMD is the encryption of the empty message, that is, the input algorithm of the shop became damaged during the processing.

Q: Does the bank’s server support SSL connection?
A: Due to an error in SSL encryption (see POODLE attack) the bank does not support SSL encryption. Instead, we recommend the TLS encryption, whichever version of it may be accessible.

Q: When calling the merchant’s URL, the TLS connection produces an error. Why?
A: The merchant’s URL can only be accessed via an http protocol.

Questions related to the payment process

Q: One by one, the transactions fail due to time-out. How can I avoid this?

A: The message necessary for closing (MSGT32) can only be accepted from the bank's point of view, if the authorisation has already been completed (with any result). The store can only confirm the completion of the authorization when the customer returns (MSGT21) or, if this does not happen (e.g. the customer closes the browser window, as a result of which redirection fails) it can check the transaction status using the message reserved for this purpose (MSGT33) and, as soon as the authorisation has been completed, it can confirm it even if the customer does not return.

The bank's response (MSGT31) to MSGT33, its interpretation, and the possible subsequent steps:

RC value	Explanation	Confirmation	New MSGT33
PR	Authorisation still in progress	not possible	necessary
TO	Authorisation failed due to time-out	not possible	not necessary
00	Authorisation closed, successful reservation	necessary	not necessary
Anything	Authorisation closed, unsuccessful reservation	not necessary	not necessary

Q: What happens to transactions that failed due to time-out?

A: In this case the bank always initiates a reversal, which essentially means that the amount reserved on the customer's account will be made available to the customer again for free use. After that, the transaction cannot be confirmed any more, and the response to the inquiry message (MSGT33) will be the RC=TO value.

Q: The customer receives a blank page after clicking on the Payment button. What could be the cause of this?

A: The payment consists of multiple steps, in the course of which the customer's browser may touch the website of various companies concerned (CIB Bank, MasterCard, VISA or the card-issuing bank). The last of these pages is indicated in the browser's location bar, and thereby it is possible to locate the company on whose web server the assumed error occurred. Please immediately notify us of all similar cases, specifying the server name in the Location bar (but first cover all the parameters included in it, if any) so we can eliminate the error as soon as possible. For the sake of safety, please ask the Customer to check if his/her internet connection operates properly, prior to reporting the error.

Q: Why do I get the RC=NT value in the bank's response (MSGT31)?

A: The bank's server provides an NT value if it finds no transactions corresponding to the request. Please check if the correct merchant ID, transaction ID and amount is specified in the request.

Q: After how much time can an authorisation be considered failed due to time-out? Can this period be changed? Is it visible?

A: By default, the authorisation qualifies as failed due to time-out after 10 minutes. This value can be modified in any direction after prior agreement. An interval of 5-60 minutes is recommended. It cannot be blocked, although a successful authorisation can be confirmed with a combination of the appropriate messages (MSGT33 and MSGT32), prior to the moment of time-out.

Q: Can the initialisation message (MSGT10) be used for redirection?

A: No, because the customer's browser is not able to interpret the bank's encrypted message (MSGT11), and therefore the payment process will be interrupted in this step. The customer may only be redirected using the message designed for this purpose (MSGT20).

Q: Is it possible to display the payment page without redirection, downloading it in lieu of the customer?
A: After successful initialisation the customer must always be redirected to the bank's payment page.

Q: Is it possible to initialise a transaction in advance and to direct the customer to the payment page only after a certain period of time?
A: The bank closes the transaction after a predefined time-out.

Q: Is it possible to confirm an authorisation (MSGT32) several times?
A: With the first confirmation, the bank closes the authorisation, and it cannot be modified any more. Every confirmation message sent after that will result in an error.

Q: Is it possible to return the customer after payment to a non-standard point?
A: Yes, in the initialising message (MSGT10), in the URL value, after the server name you must provide the port number, separated by a colon (http://server.dom:<port>/). However, you must keep in mind that in the case of most customers, the network rules do not permit this connection.

Q: The customer has reported that it takes a long time (10-60 seconds) until he/she can return to the webshop after having entered the card data and clicked on the Payment button. What happens in this case?
A: After the customer has provided the card information, the bank directs the customer to the card companies, and, through them (if necessary) to the issuing bank, so that he/she can enter the confirmation code related to the transaction (which can be a general or a one-time password) (3D Secure). If the card type is MasterCard or Maestro, redirection takes place in any case, which increases the authorisation period by 5-10 seconds on average. After entering the code, the bank authorises the transaction (which means an additional period of 5-10 but not more than 40 seconds), after which the customer's browser is redirected to the webshop.

Other questions

Q: The bank's response message only contains RC=SXX or RC=DXX codes. Why?

A: The bank's server is only able to send an encrypted response message if it has successfully processed the merchant's message. In case of error it produces an error message corresponding to the error type. A list of error types is available in the Reference guide. In this case it is advisable to make sure that the message has been prepared using the appropriate parameters, it has been sent as the appropriate step in the process, using the appropriate encryption key. It must be highlighted that the encryption key attached to this documentation is not suitable for communication with any of the bank servers, and it is only suitable for testing the operation of the application.

Q: What URL value can be applied in the initialisation message (MSGT10)?

A: A full-featured domain name (FQDN) that is not parametered. A few examples, without being exhaustive:

URL	Acceptable
server1	No
http://server1	No
http://server1.hu	No
http://server1/	No
http://server1.hu/	Yes
https://server1.hu/	Yes
ftp://server1.hu/	No
http://127.0.0.1/	Yes
http://server1.hu/path/script.ext	Yes
http://server1.hu/path/script.ext?param=value	No
http://http://server1.hu/	No

Q: Why does the transaction ID in the bank's response contain a + sign?

A: The identifier must be 16 characters long. If the merchant's software sends a shorter ID, the bank's server automatically supplements it to the length of 16 characters, including spaces, the URL-encoded format of which is the + sign.

Q: Why do I get MSGT11 messages with RC=02 value?

A: The transaction ID sent in the initialisation message (MSGT10) is already reserved. This ID must be generated prior to starting each payment as a pseudo-random value. Modern programming language versions perform a 'reseed' step prior to each random number generation process (regeneration of the value that serves as the basis for the random number generation), but this should also be executed explicitly, in a forced manner, prior to the calculation of the identifier.

Q: In what format must the sum payable be provided?

A: For Hungarian forint, it is to be specified as an integer number, in the case of euro it must be rounded to two decimals. In this latter case the two decimals are always obligatory. The whole part is separated by the fraction by a dot.

Q: Do I need to store the transaction data?
A: Yes, partly because this is a precondition for a successful transaction, and partly because it will later be very useful in providing information to the customer.

Q: Is it advisable to send an e-mail to the customer regarding the result of the transaction?
A: Yes. Sometimes the customer does not wait for the result of the authorisation and closes the browser, and therefore immediate notification becomes impossible. The e-mail must contain the same data items as those that customer may see on the confirmation webpage (transaction ID, amount, currency, response code description and authorisation number).

Q: Does the customer need to be identified prior to starting the payment?
A: Yes, this is a precondition for a successful bank test. Identification is possible by applying any generally accepted method (by providing a one-time or a permanent password or by verification of biometric data).

Q: Can a customer ID (UID) contain an e-mail address?
A: The UID field may only contain the characters allowed in the specification (small and capital letters, numbers, dashes, underscores or spaces).

Q: Is it possible to escape the parameters used for communication, and can they also contain any extra characters (e.g. line break)?
A: There is no possibility to escape any parameters, either encrypted or unencrypted (this is not necessary either, due to the URL-encoding) and they cannot contain any whitespace characters (e.g. line break or tab).

Q: Is there a version of the bank's payment page optimised for mobile devices?
A: Yes. Please let us know as soon as possible if you wish to request a mobile template for the vPOS terminal. It is important to emphasize that only one template can be assigned to the same terminal, so if you wish to use both a desktop and a mobile template for your website, then you will need at least two terminals.