

**API CERTIFICATION CHECKLIST BASIC PAYMENT**

**Cs-**

Instructions for use

Medellín, September 2024

Version 1

**CONFIDENTIAL USE**

Document Statement

*This document was prepared by, for and shall remain the property of Evertec® for confidential use.*

*for its confidential use.*

*Customer agrees by its acceptance or use of these documents, to return them upon request to Evertec® and not to reproduce, copy, loan or otherwise disclose or dispose of their contents, directly or indirectly, and not to use them for any purpose other than that for which they were specifically prepared.*

|  |  |  |
| --- | --- | --- |
| Point | Description |  |
| Commercial activity | The site must only process products and/or services related to the commercial activities established at the beginning of the negotiation, in case of products not allowed by Placetopay the site will not be certified. | ☐ fulfill  ☐ Doesn't comply  ☐ Not applicable |
| Payment process and use of corporate image. | When initiating the payment, before the payment process to Placetopay is required to find the logo of Placetopay as well as the logos of the franchises that will be used on the site (VISA, DINERS, DISCOVER, MASTERCARD and AMERICAN EXPRESS) in turn the user must view the total amount to be paid and the breakdown of taxes that would be in the transaction (if applicable).  The system must avoid additional consumption when updating the status of a transaction when there is already a final status in the response of the **processtransaction**, so whenever there is a final status there should not be a new consumption to the **query** to know the status of the payment except for the PENDING status, according to the above at the time that a payment summary is provided and the transaction is updated in the commerce system, it should be done in a general way in DB maintaining traceability and avoiding additional consumption according to the status given by Placetopay.  **The source of the Placetopay logo before the redirect and in all the sections of the page that is included, must point to one of the urls provided.** https://static.placetopay.com/placetopay-logo.svg  https://static.placetopay.com/placetopay-logo-dark-background.svg  https://static.placetopay.com/placetopay-logo-square.svg  https://static.placetopay.com/placetopay-logo-square-dark-background.svg  **Note that the name Placetopay must be shown with initial capital letter or capital letter held together, avoiding any other usage such as: PlaceToPay, PlacetoPay, Place to Pay, etc.** | ☐ fulfill  ☐ Doesn't comply |
| Frequently Asked Questions | The frequently asked questions should be anywhere on the site, usually placed in the header or footer of the page, they were sent in the email at the beginning of the integration. | ☐ fulfill  ☐ Doesn't comply |
| Terms, conditions and privacy policy | The user must accept the terms and conditions before being redirected to the payment, likewise the merchant must provide the option to view the terms and conditions of the site (the terms and conditions are defined by the merchant). | ☐ fulfill  ☐ Doesn't comply |
| Use of taxes | The merchant must discriminate the VAT and ICE of the products in the transaction, this point is validated in the display of the value to be paid and in the request that has been sent to Placetopay.  The base, the type of tax and the value of the tax must be sent.  **This is mandatory if applicable within the core business.** | ☐ fulfill  ☐ Doesn't comply  ☐ Not applicable |
| Security requirements | The configuration data of the Placetopay connection must be stored as parameters either in the database or in some .ini, .json, .xml, .env, etc. file.  For sites that use JavaScript validation, it is necessary to avoid affecting the operation when accessing from a browser that has JavaScript execution disabled. This can be by preventing the page from loading or by performing server-side validation.  **Under no circumstances should the merchant store or display sensitive cardholder card data: Card number and CVV.** | ☐ fulfill  ☐ Doesn't comply |
| Pay and return button control | Double requests by the user or the merchant should be avoided in case the service takes a long time to respond when the payment button is clicked.  **Please note that, once the payment has been made, in case the user returns through the previous and next instructions of the browser, it is recommended that the order is reloaded again, since sending the same order to the payment process should be avoided as this will incur a double payment depending on the number of times the user does it.** | ☐ fulfill  ☐ Doesn't comply |
| Types of credit and interest calculation | The merchant makes available to the user the types of credit allowed for the payment process, according to the initial consumption to consult and validate the card **information**. Once the user selects the type of credit to use, the interest calculation must be shown according to the type of credit selected by the **interests** method:  **The type of credit selected by the user must be sent in the request at the time the process transaction is to be performed.** | ☐ fulfill  ☐ Doesn't comply |
| OTP generation and validation | The merchant must generate, validate and make available to the user a field either in a modal or within the same interface, which must be as required and allow the entry of only numerical values, according to the initial consumption to consult and validate the information card.  **Once the user enters the otp and it is validated against the validate service, the response will provide a signature that must be sent in the processtransaction as otp if the response is successful.**  In case the **otp** validation is not performed correctly, the error detail provided by the api when performing the validation must be given and if the 3rd attempt is fulfilled, which responds with a block to the operation, the operation must be blocked or terminated from the commerce. | ☐ fulfill  ☐ Doesn't comply |
| 3DS generation and validation | The merchant must set up a 3DS authentication flow facing the user either in a modal or through redirection, according to the initial consumption to query and validate the card information.  **Once the user returns from the validation, the authentication information must be consulted through the query, and the response will provide all the details that must be sent in the processtransaction as threeDS.** | ☐ fulfill  ☐ Doesn't comply |
| Pinpad-Pinblock Generation and Validation | The merchant must generate, request and make available to the user a PINPAD either in a modal or within the same interface, which must be as required and allow the entry of only numerical values, according to the initial consumption to consult and validate the information card.  **Once the user enters the pin, the pinblock is generated from the positions given by the user through the pinblock method and the response will provide the pinblock to be sent in the processtransaction as a pin.** | ☐ fulfill  ☐ Doesn't comply |
| Sending Kounts | The system must send in the **processtransaction** messaging a **kount** object with the attributes of a session which is a unique random value for each transaction and a default type. | ☐ fulfill  ☐ Doesn't comply |
| Field validation (PROCESS) | The system asks the user for the card number as a mandatory field, it only receives numeric values and has a length of 13 to 19 characters, validating the value typed through Luhn's algorithm. | ☐ fulfill  ☐ Doesn't comply |
| The application requests or presents the user with the expiration date as a mandatory field, validating that the expiration date is not expired and only receives the value of the month from January to December, that is, from 01 to 12 (always two digits). Allowing a maximum choice of 10 years, starting from the current date. | ☐ fulfill  ☐ Doesn't comply |
| The system prompts the user for the CVV2 as a masked mandatory field, it only receives numeric values and has a maximum length of 4 characters (American Express is the only one that must allow a maximum of 4 characters, Visa, Mastercard, Discover and Diners only 3) | ☐ fulfill  ☐ Doesn't comply |
| Validate that the reference is not repeated in any case, validate vs. pending, approved and rejected transactions in the database.  **Note that the reference must have a minimum length of 1 character and a maximum length of 32 characters.** | ☐ fulfill  ☐ Doesn't comply |
| The buyer-payer structure must be sent at the time of the payment request in Placetopay. The required information is: name, surname, email, ID, type of ID and mobile (cell phone). | ☐ fulfill  ☐ Doesn't comply |
| Required fields are validated in the commerce, an error message must be indicated to the customer if he/she has not filled in all the required data for the shipment to Placetopay. | ☐ fulfill  ☐ Doesn't comply |
| For the validation of the document, restrictions must be implemented in the field, according to the type of document selected by the user, the validations of the documentation can be taken as a reference:  [Document types - Placetopay Docs](https://docs.placetopay.dev/en/checkout/document-types) | ☐ fulfill  ☐ Doesn't comply |
| It must be validated that the mobile has the correct structure of a cell phone, avoiding the entry of letters and special characters except for the +.  Note that in case of sending the phone, it must be different from the mobile, since it belongs to a fixed or conventional line. | ☐ fulfill  ☐Doesn't comply  ☐ Not applicable |
| In case the identity document is identity card or passport (PPN):  Names and surnames must not have numbers or special characters, they must have only letters (including ñ, tilde and space).  In case the identity document belongs to a company:  It should be sent only under name, company name or trade name and in this case numbers are allowed. | ☐ fulfill  ☐ Doesn't comply |
| It must be validated that the e-mail has the correct structure of an e-mail. | ☐ fulfill  ☐ Doesn't comply |
| The end user's IP and browser agent are evidenced. | ☐ fulfill  ☐ Doesn't comply |
| Response handling for transactional statuses | When returning to the merchant for APPROVED transactions, a summary of the transaction must be displayed indicating at least: reference, date and time, status, reason, message, currency, total value, interest (Ecuador), type of credit (Ecuador), installments, receipt, authorization, bank and last 4 digits of the card.  Please note that the payment status is “Approved” or “Approved”, it should be handled with these words. | ☐ fulfill  ☐ Doesn't comply |
| When returning to the merchant for REJECTED transactions, a summary of the transaction must be displayed indicating at least: the reference, date and time, status, reason, message, currency, total value, interest (Ecuador), type of credit (Ecuador), installments, receipt, authorization, bank and last 4 digits of the card.  Please note that the payment status is “Rejected” or “Rejected”, it should be handled with these words | ☐ fulfill  ☐ Doesn't comply |
| When returning to the merchant for PENDING transactions, a summary of the transaction must be displayed indicating at least: the reference, date and time, status, reason, message, currency, total value, interest (Ecuador), type of credit (Ecuador), installments, receipt, authorization, bank and last 4 digits of the card.  Please note that the payment status is “Pending”, it should be handled with these words. | ☐ fulfill  ☐ Doesn't comply |
| It must be evidenced that the business performs the probe process (Cronjob) as a backup to resolve pending transactions in its database, for this purpose it must consult the current status of the transactions stored in the database with pending status so that in case the status has changed, it can be updated.  **In the test environment it should be executed with a periodicity of 5 or 10 minutes, only when tests are going to be performed by the trade; otherwise it should be kept inactive, while in production it should be executed every 15 minutes verifying transactions that have more than 7 minutes in pending status.**  The consumption towards the service to know the final status of a pending transaction must always be done through the **query** method, the use of the **search** method is only in case of loss of communication when the **processtransaction** is performed. | ☐ fulfill  ☐ Doesn't comply |
| When consuming the **processtransaction** service, a timeout is generated in the connection to Placetopay (it should be around 25 seconds) and no response is obtained from the service, the operation must be marked in pending status and search for the transaction using the **search** method, meanwhile this transaction must comply with the general behavior of this status (double payment control and probe process). | ☐ fulfill  ☐ Doesn't comply |
| If a user has pending transactions and tries to pay for a new transaction, the user should be shown an informative message that he/she has pending transactions with their respective references (at least the last one). | ☐ fulfill  ☐Doesn't comply  ☐ Not applicable |
| Proof of paymentde pago | Proof of payment is evidenced in accordance with each of the statements of transactions. | ☐ fulfill  ☐Doesn't comply  ☐ Not applicable |
| Transaction history | The use of payment history is evidenced in user 1.  Approved, pending and rejected transactions must be shown in descending order, with the following data: reference, date and time, status, value with its respective currency and authorization.  **The value of the transaction must be maintained throughout the execution of the transaction and also be reflected in the history. Additionally, it must be guaranteed that the payment status update is done under the same flow, i.e., if the transaction has a final status: approved, rejected or pending in the payment summary, it must be shown in the history without depending on any other process except for the pending status.** | ☐ fulfill  ☐Doesn't comply  ☐ Not applicable |
| Security of the Information | The business is PCI certified (Current) | ☐ fulfill  ☐Doesn't comply  ☐ Not applicable |
| The business has an SSL certificate (valid). | ☐ fulfill  ☐ Doesn't comply |
| A TLS protocol >= 1.2 is used. | ☐ fulfill  ☐ Doesn't comply |
| Under no circumstances does the system store sensitive cardholder information. | ☐ fulfill  ☐ Doesn't comply |
| The system does not show the CVV and card number on payment statements, sales receipts or any other user-facing section. | ☐ fulfill  ☐ Doesn't comply |
| If the development uses a web interface (even if it is an intranet) the information capture URL should not be masked (hidden) using techniques such as IFRAMES. | ☐ fulfill  ☐ Doesn't comply |
| The minimum information for a future claim (date and time of transaction, receipt number, transaction value, authorization number, maximum 4 last digits of the card number, reference and promissory note, the latter if applicable) is saved in the application's database. | ☐ fulfill  ☐ Doesn't comply |
| Processing information | Once a transaction is made, the same data that was validated, entered or selected in the user interface is sent to the Placetopay API:   * Card number * CVV * Expiration Date * Installment or Type of Credit (Ecuador only) * Total Value * VAT * Refund Basis * User Information * Security Protocols Information | ☐ fulfill  ☐ Doesn't comply |
| Consistency of information | The information sent to Placetopay must not have contrasting information regarding the transaction in commerce, the information must be consistent between platforms. | ☐ fulfill  ☐ Doesn't comply |
| Reverse side of transactions | The reversals process must be defined in case the merchant performs reversals in his system or is going to use the administrative console. | ☐ fulfill  ☐Doesn't comply  ☐ Not applicable |

[](https://www.facebook.com/Evertecinc/)[](https://www.instagram.com/evertec.inc/?hl=es)[](https://www.linkedin.com/company/evertec/posts/?feedView=all)[](https://twitter.com/evertec_inc/)