



# GUÍA DE CERTIFICACIÓN API

Instructivo de uso

Agosto 2025

Versión 1.5.1

**USO CONFIDENCIAL**

### ***Declaración del Documento***

*Este documento fue preparado por, para y se mantendrá bajo la propiedad de Evertec® para su uso confidencial.*

*El cliente acuerda por su aceptación o uso de estos documentos, devolverlos a solicitud de Evertec® y no reproducirlos, copiarlos, prestarlos o de otra forma revelarlos o disponer de sus contenidos, directa o indirectamente y no usarlos para ningún otro propósito que no sea aquel para el cual fueron específicamente preparados.*

## TABLA DE CONTENIDO

|   |    |
|---|----|
| 2. ACTIVIDAD COMERCIO .....                                 | 5  |
| 3. LOGOS DE PLACETOPAY .....                                | 5  |
| 4. PREGUNTAS FRECUENTES.....                                | 6  |
| 5. TÉRMINOS, CONDICIONES Y POLÍTICAS DE PRIVACIDAD .....    | 6  |
| 6. PROCESO DE PAGO .....                                    | 6  |
| 7. USO DE IMPUESTOS (TAXES) .....                           | 7  |
| 8. REQUISITOS DE SEGURIDAD.....                             | 7  |
| 9. CONTROL BOTÓN PAGAR Y REGRESO .....                      | 8  |
| 10.1. WEBHOOK DE EVENTOS.....                               | 11 |
| 10.2. LIGHTBOX EN VALIDACIÓN DE CUENTA BANCARIAS ACH.....   | 13 |
| 10.3. MANEJO DE ESTADO PENDIENTE.....                       | 14 |
| 11. GENERACIÓN Y VALIDACIÓN DE 3DS.....                     | 17 |
| 12. GENERACIÓN Y VALIDACIÓN PINPAD-PINBLOCK.....            | 18 |
| 13. AUTENTICACIÓN KOUNT .....                               | 19 |
| 14. VALIDACIÓN DE CAMPOS .....                              | 20 |
| 15. CONTROL DE IDEMPOTENCIA (PAGOS DUPLICADOS).....         | 23 |
| 16.2. CHECKOUT .....  | 24 |
| 16.3. CANCELACIÓN DE UNA PREAUTORIZACIÓN .....              | 25 |
| 16.4. REINTENTOS DE CAPTURA (CHECKOUT) .....                | 25 |
| 17.1. COBRAR MEDIO DE PAGO TOKENIZADO .....                 | 26 |
| 17.2. TOKENIZACIÓN MEDIO DE PAGO ATH CON PIN .....          | 27 |
| 17.3. INVALIDACIÓN DE TOKEN .....                           | 28 |
| 18. MANEJO DE RESPUESTAS PARA ESTADOS TRANSACCIONALES ..... | 28 |
| 18.2. TIMEOUT 32 SEGUNDOS .....                             | 32 |
| 19. COMPROBANTE DE VENTA .....                              | 32 |
| 20. HISTÓRICO TRANSACCIONAL.....                            | 32 |
| 21. SEGURIDAD DE LA INFORMACIÓN .....                       | 33 |
| 22. PROCESAMIENTO DE LA INFORMACIÓN .....                   | 33 |

|   |    |
|---|----|
| 23. COHERENCIA DE LA INFORMACIÓN.....               | 34 |
| 24. DIRECCIÓN IP Y AGENTE DE NAVEGACIÓN .....       | 34 |
| 25. ENVIO EXTRADATA.....                            | 35 |
| 25.1. CUSTOMER ACCOUNT NUMBER .....                 | 35 |
| 26. REVERSO DE TRANSACCIONES.....                   | 36 |
| 26.1. REEMBOLSO DE TRANSACCIONES .....              | 36 |
| 27. INFORMACIÓN RELEVANTE .....                     | 38 |
| 27.1. FORMATO DE PLANTILLAS DE RESPUESTA .....      | 38 |
| 27.3. CONSIDERACIONES .....                         | 40 |
| 28. PROCESAMIENTO CON CUENTAS BANCARIAS (ACH) ..... | 41 |
| 29. Webhook Devoluciones ACH (PR Opcional).....     | 41 |
| 29.1. Validar firma.....                            | 44 |

**Nota:** Este documento es para guiar al cliente en la configuración del servicio de API Gateway de PlacetoPay. La documentación pública para las configuraciones se puede encontrar en el siguiente enlace: [Placetopay Docs](#). deben dirigirse a la sección “Servicios API” y seleccionar “Gateway”.

Una vez realizada la integración con Evertec PlacetoPay es necesario realizar una certificación en la cual se evalúan diversos puntos para garantizar el funcionamiento correcto de la integración y proteger la integridad de datos; por tanto, los enlaces y datos de pruebas deben estar libres de errores de programación.

A continuación, se describen los diferentes aspectos para tener en cuenta en el proceso de certificación que se van a evaluar en con el servicio de API de PlacetoPay.

## 2. ACTIVIDAD COMERCIO

Se valida que el sitio web / App / Portal sólo este procesando productos y / o servicios relacionados con las actividades comerciales establecidas al inicio de la negociación, en caso de productos no permitidos por Evertec Placetopay el sitio no será certificado.

## 3. LOGOS DE PLACETOPAY

El sistema donde se realizó la integración debe de mostrar al usuario el logo de Placetopay, este logo se puede tomar de alguna de las siguientes URL's:

- <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>

Adicional a esto, debe contener un hipervínculo a nuestra página principal informativa: <https://placetopay.dev/>.

También se sugiere agregar los logotipos de las franquicias disponibles para hacer pagos, a fin de que el cliente tenga conocimiento de los medios de pago habilitados para el comercio.

#### 4. PREGUNTAS FRECUENTES

Se debe incluir dentro de un apartado del sitio, una sección de Preguntas Frecuentes (FAQ) y mencionar los pagos a través de Evertec Placetopay. En caso de que el comercio no cuente con una sección de FAQ, se deben incluir de igual forma las preguntas frecuentes proporcionadas en la documentación.

**Nota:** En las FAQ no debe mencionarse o hacer alusión a términos de pagos en línea ni pagos online, adicionalmente estas preguntas frecuentes se compartirán al inicio de la integración.

#### 5. TÉRMINOS, CONDICIONES Y POLÍTICAS DE PRIVACIDAD

Para garantizar la transparencia y el cumplimiento de las normativas aplicables, el comercio debe establecer Términos y Condiciones claros y una política de gestión de información del usuario accesible adicionalmente estos deben añadir en un apartado por ejemplo en el pie de página, etc. Estos deben cumplir con los siguientes lineamientos:

- Los T&C deben ser visibles para el usuario antes de procesar el pago.
- El comercio debe permitir al usuario consultar y aceptar las condiciones generales de manera explícita antes de finalizar la compra.
- El comercio es responsable de definir los términos y condiciones generales que regulen sus operaciones.

#### 6. PROCESO DE PAGO

El sistema le debe permitir al usuario comprador, visualizar el monto total a pagar antes de pasar al servicio de pagos implementado, este valor debe de coincidir con el valor enviado a Evertec Placetopay dentro de la mensajería.

El comercio definirá el proceso para realizar el desglose del producto o servicio donde se evalúan los valores e impuesto a cobrar al tarjetahabiente. Puede ser a través de formulario, carrito de compras, tienda virtual, selección de recibo u otros.

El sistema debe asegurarse de no generar consumos adicionales al actualizar el estado de una transacción si el response del **process** ya indica un estado final. Esto significa que, si ya hay un estado final, no se debe realizar un nuevo **query** para verificar el estado del pago, excepto cuando el estado sea PENDIENTE. De acuerdo con lo anterior, en el

momento que se brinda un resumen de pago y se actualiza la transacción en el sistema del comercio, se debe hacer de forma general en la base de datos manteniendo la trazabilidad y evitando consumos adicionales acorde al estado dado por Evertec PlacetoPay.

## 7. USO DE IMPUESTOS (TAXES)

En caso de que dentro de la reglamentación del país y modelo de negocio sea obligatorio el envío de impuestos hacia los bancos, el comercio debe discriminar dichos impuestos de los productos en la transacción. Se debe enviar la base, el tipo de impuesto y el valor del impuesto.

En caso de enviarse se valida que el comercio incluya dichos valores correspondientes dentro de la solicitud de pago, el request enviado, el desglose de IMPUESTOS, donde se le debe mostrar al usuario.

Para hacer uso de este deben enviarse cada tipo de impuesto según lo descrita la documentación [Montos y monedas - Placetopay Docs](#)

**NOTA:** Si el Número de Control Fiscal está habilitado y será generado como parte del Proceso de Transacción, se requiere enviar el Desglose de Impuestos correspondiente. De lo contrario, el Número de Control Fiscal puede generarse incorrectamente.

## 8. REQUISITOS DE SEGURIDAD

Los datos de configuración de la conexión de Evertec Placetopay deben ser almacenados como parámetros ya sea en la base de datos o en algún archivo **.ini**, **.json**, **.xml**, etc. Esto se debe hacer por buenas prácticas de programación y para que, al momento de actualizar la llave, el proceso sea más sencillo.

Para los servicios que usan validaciones con JavaScript se debe evitar que se afecte la operación cuando se ingresa desde un navegador que tiene deshabilitada la ejecución de JavaScript. Puede ser evitando la carga de la página o realizando validación del lado del servidor.

Se recomienda implementar contraseña cifrada en AES256 para realizar la autenticación de los usuarios en el sitio del comercio.

Por ningún motivo el comercio deberá almacenar o mostrar datos sensibles de las tarjetas de los tarjetahabientes. Los datos que se consideran sensibles son:

- Número de tarjeta de crédito.
- CVV (Código de verificación).

## 9. CONTROL BOTÓN PAGAR Y REGRESO

Deben evitarse y controlarse las solicitudes múltiples por parte del usuario en caso de que el servicio tarde mucho tiempo en responder cuando se pulsa el botón de pago. El botón debe estar desactivado mientras se procesa el pago.

Tenga en cuenta que, una vez completado el pago, si el usuario hace clic en un botón para volver al sitio web / aplicación / portal del comercio, se debe realizar una validación para garantizar que el pago no se procese de nuevo. Esta acción evita la duplicación de pagos por parte del usuario. Este apartado se explica más técnicamente en el [punto 15](#) de esta guía.

## 10. VALIDACIÓN DE CUENTAS – ACH (DÉBITO DIRECTO A CUENTAS BANCARIAS)

Según las normas de **NACHA**, los pagos mediante ACH (débito directo a cuentas bancarias) deben validar la cuenta bancaria al menos la primera vez. Para cumplir con este requisito, el comerciante puede utilizar un servicio externo de validación de cuentas o el servicio de validación propio de Evertec PlacetoPay, el cual se detalla en los siguientes párrafos.

Evertec PlacetoPay proporciona un servicio propio de validación de cuentas. En este servicio existen dos tipos de validación:

- **Validación instantánea:** Permite obtener de inmediato el estado de la verificación en la consulta, agilizando el proceso para el usuario y el comercio.
- **Validación por micro depósitos:** En este método, la validación puede tardar entre 1 y 2 días, ya que se realizan pequeños depósitos en la cuenta bancaria del usuario para su confirmación. Durante este periodo, la cuenta permanecerá en estado **pendiente** hasta que se complete la verificación (Este apartado se detalla en el [punto 10.2](#) de esta guía.)

Este servicio permitirá al usuario validar sus cuentas bancarias utilizando el método **CreateSession**.

Con este método, se puede crear una URL que contendrá la Sesión con el validador de cuentas y exponerla al usuario para validar sus Cuentas Bancarias. Una vez el usuario



finalice la validación de la cuenta, este será redireccionado al parámetro enviado en el “returnUrl” Para verificar el estado de la Sesión del Validador, se debe ejecutar una consulta con el Método **CheckSessionStatus**.

Una vez validada la cuenta, se generará el “**verificationCode**” (Firma de Validación). Este valor debe enviarse dentro de la Solicitud de Pago.

Además, una vez validada la cuenta, se pueden realizar validaciones adicionales (en caso tal se requiera, para este caso se debe de utilizar el método [Validar Cuenta Existente](#)). Otra opción es que el comercio almacene de forma segura la cuenta bancaria del pagador, código del banco, número de ruta y el tipo de cuenta junto con el token del método de pago para futuras transacciones.

Una vez se tengan estas validaciones completadas, y se requiere procesar una transacción, se debe de enviar la petición de la siguiente forma:

```
{
  "auth": {},
  "payer": {
    "name": "Test",
    "surname": "Test",
    "email": "pruebas2p.juanserna@gmail.com",
    "mobile": 3006108300
  },
  "payment": {
    "reference": "Test_ach_1",
    "description": "Pruebas ",
    "amount": {
      "currency": "USD",
      "total": 20
    }
  },
  "instrument": {
    "account": {
      "bankCode": "021502011",
      "bankName": "FIRSTBANK (PUERTO RICO)",
      "accountType": "CCD",
      "accountNumber": "4111111111111111",
      "franchise": "_021502011_",
      "verificationCode": "eyJhbGciOiJSUzI1NiJ9"
    }
  },
  "ipAddress": "127.0.0.1",
  "userAgent": "Testing"
}
```

**Nota:** Es fundamental garantizar que los datos obtenidos de la consulta se almacenen de forma cifrada, este procedimiento es crucial para proteger información sensible y prevenir

riesgos asociados con el acceso no autorizado, fuga de datos, posibles intentos de fraude, entre otros.

```
"account": {  
  "bankCode": "221571473",  
  "bankName": "FIRSTBANK (PUERTO RICO)",  
  "accountType": "DDA",  
  "accountNumber": "4111111111111111",  
  "franchise": "_221571473_",  
  "verificationCode": "..."  
}
```

### 10.1. WEBHOOK DE EVENTOS

Debido a que las validaciones de las cuentas ACH se realizan mediante una sesión, se tiene la necesidad de conocer el resultado de dicha validación, debido a esto se debe de implementar una URL de notificación (Webhook) con la finalidad de que esta reciba una estructura json indicando el estado de dicha sesión, la estructura json contendrá los siguientes datos:

- Sesión aprobada

```
{  
  "status": {  
    "status": "APPROVED",  
    "reason": "00",  
    "message": "La solicitud ha sido aprobada exitosamente"  
  },  
  "requestId": "53eccc5c-bbb8-36ae-a4f0-dfc8a791e736",  
  "signature": "0cd51ffd7cb58c0a36fb7b926838b1feb6336512" }
```

- Fallo por intentos fallidos

```
{
  "status": {
    "status": "REJECTED",
    "reason": "38",
    "message": "Ha realizado el número máximo de intentos fallidos"
  },
  "requestId": "53eccc5c-bbb8-36ae-a4f0-dfc8a791e736",
  "signature": "0cd51ffd7cb58c0a36fb7b926838b1feb6336512" }
```

- Sesión expirada

```
{
  "status": {
    "status": "REJECTED",
    "reason": "XD",
    "message": "La solicitud ha vencido"
  },
  "requestId": "53eccc5c-bbb8-36ae-a4f0-dfc8a791e736",
  "signature": "0cd51ffd7cb58c0a36fb7b926838b1feb6336512" }
```

- Sesión cancelada por el usuario

```
{
  "status": {
    "status": "REJECTED",
    "reason": "?C",
    "message": "Verificación cancelada por el usuario"
  },
  "requestId": "53eccc5c-bbb8-36ae-a4f0-dfc8a791e736",
  "signature": "0cd51ffd7cb58c0a36fb7b926838b1feb6336512" }
```

**Nota:** Tener en cuenta que, una vez recibida la notificación, se deben de seguir los pasos mencionados en la siguiente documentación:

### Webhook de Eventos

## 10.2. LIGHTBOX EN VALIDACIÓN DE CUENTA BANCARIAS ACH

PlacetoPay permite implementar este servicio dentro de un iframe/lighbox generado por el comercio. Se debe tener en cuenta y validar los mensajes enviados desde el Iframe para eventos como:

Validación aprobada:

```
{
  "type": "close",
  "payload": {
    "status": {
      "status": "OK",
      "reason": "00",
    },
    "account": {
      "status": {
        "status": "OK",
        "reason": "00",
        "message": "La solicitud ha sido aprobada exitosamente",
        "date": "..."
      },
      "bankCode": "POPULAR",
      "bankName": "Banco Popular",
      "accountType": "SAV",
      "accountNumber": "...",
      "verificationCode": "..."
    },
  },
} }
```

Validación cancelada:

```
{
  "type": "close",
  "payload": {
    "status": {
      "status": "REJECTED",
      "reason": "?C"
    }
  }
}
```

```
    },  
    "account": null  
  }  
}
```

Validación rechazada:


```
{  
  "type": "close",  
  "payload": {  
    "status": {  
      "status": "REJECTED",  
      "reason": "38",  
    },  
    "account": null  }  
}
```


**NOTA:** Se debe capturar los detalles del estado de la verificación, es importante hacer captura de este, ya que, si no se ejecuta, no va a hacer posible tener la actualización si el usuario completo la validación. Por favor basarse para la implementación en la documentación oficial: [Soporte para Lightbox](#)

### 10.3. MANEJO DE ESTADO PENDIENTE


Para los escenarios donde se realiza una validación con micro depósitos (recordando que puede tomar 1 o 2 días hábiles), se debe tener en presente que, al momento de consultar esa sesión, la respuesta del servicio sería “rechazada”, posteriormente el usuario tiene la posibilidad de generar una nueva sesión donde pueda confirmar la validación iniciada, en este proceso el servicio envía un OTP al usuario con la finalidad de verificar su identidad.

A continuación, se muestra a detalle el flujo del usuario en este tipo de escenario.


  
wolvertec




**Pendiente de Micro-depositos**  
Su cuenta esta en proceso de verificación.



Debe ingresar y confirmar los micro-depositos en la fecha indicada para completar su pago.




Nos comunicaremos contigo una vez los micro depósitos se hayan realizado




Si desea realizar el pago en estos momentos, puede validar otra cuenta o seleccionar otro medio de pago.

Validar otra cuenta

Salir

  
wolvertec

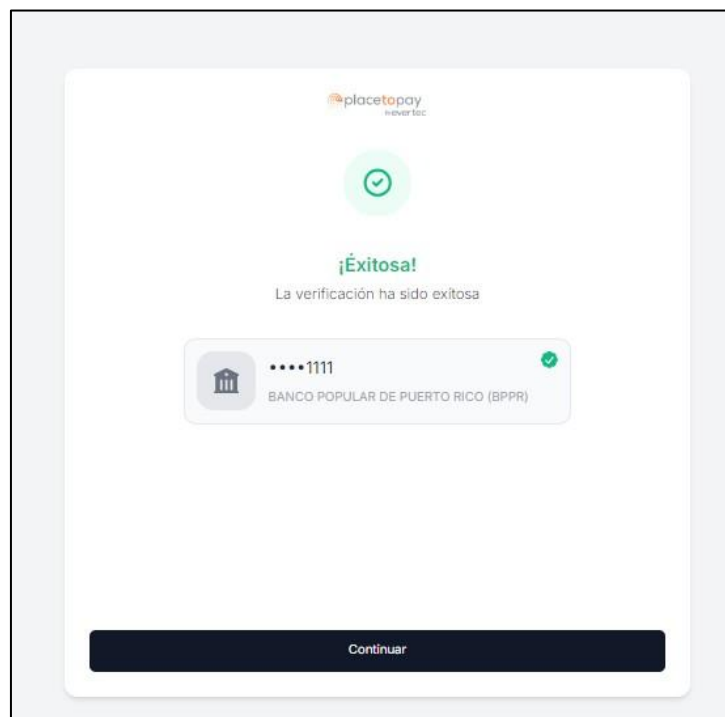


**¡Hola Juan Serna!**  
Por seguridad, por favor ingresa el código de validación que hemos enviado a tu correo **inte.p2p\*\*\*\*\*@\*\*ail.com**.

[Generar otro código de validación](#)

Validar código

Volver al comercio



De esta forma una vez el usuario regrese de dicha validación previamente iniciada, el comercio podrá encontrar los datos de dicha cuenta en caso tal la validación haya sido aprobada.

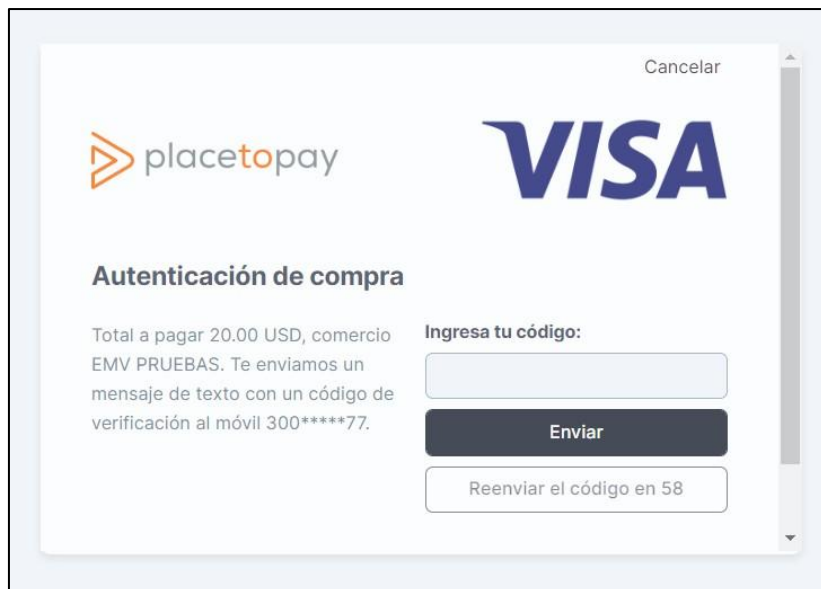
```
{  
  "status": {
```



```
{
  "status": "APPROVED",
  "reason": "00",
  "message": "La verificación ha sido exitosa",
  "date": "2025-01-17T17:14:21+00:00"
},
"data": {
  "requestId": "...",
  "account": {
    "bankCode": "221571473",
    "bankName": "FIRSTBANK (PUERTO RICO )",
    "accountType": "SAV",
    "accountNumber": "...",
    "franchise": "_221571473_",
    "verificationCode": "..."
  },
  "expiresAt": "2025-01-17 17:28:45"
}
}
```

## 11. GENERACIÓN Y VALIDACIÓN DE 3DS

El comercio debe de levantar un flujo de autenticación de 3DS de cara al usuario ya sea en una modal o través de redirección, de acuerdo con el consumo inicial para consultar y validar la información de la tarjeta **Solicitud de información:**



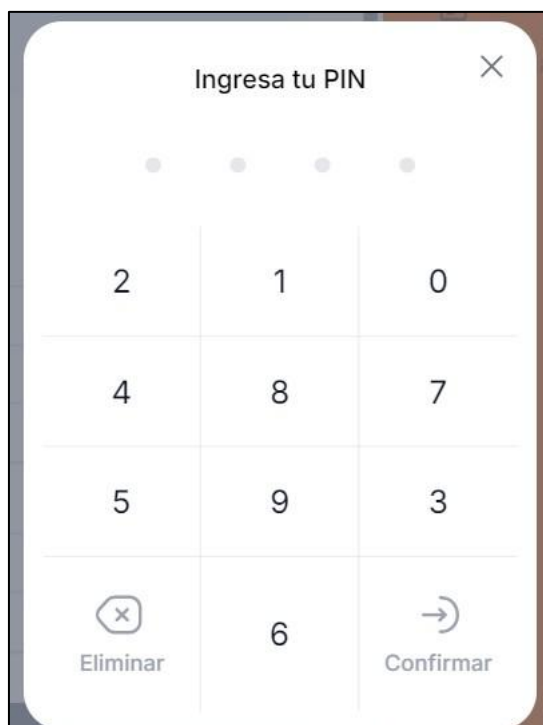
The screenshot shows a 3DS authentication modal. At the top right is a "Cancelar" button. The modal features the "placetopay" logo on the left and the "VISA" logo on the right. Below the logos, the title "Autenticación de compra" is displayed. Underneath, a message states: "Total a pagar 20.00 USD, comercio EMV PRUEBAS. Te enviamos un mensaje de texto con un código de verificación al móvil 300\*\*\*\*\*77." To the right of this message, the text "Ingresa tu código:" is followed by a text input field. Below the input field is a dark "Enviar" button. At the bottom right, there is a button that says "Reenviar el código en 58".

Una vez el usuario retorna de la validación se debe consultar la información de la autenticación mediante el **3DSquery**, y el response brindará todo el detalle que debe ser enviado en el **Transaction Processing** como **threeDS**.

Adicional a esto, favor basarse en la documentación oficial: [Generación 3DS](#)

## 12. GENERACIÓN Y VALIDACIÓN PINPAD-PINBLOCK

El comercio debe generar, solicitar y poner a disposición del usuario un PINPAD ya sea en un modal o dentro de la misma interfaz, el cual debe estar como requerido y permitir el ingreso de únicamente valores numéricos, de acuerdo con el consumo inicial para consultar y validar la información de la tarjeta **Solicitud de información**:



Una vez el usuario ingresa el pin, se genera el PinBlock a partir de las posiciones dadas por el usuario mediante el método **PinBlock** el response brindará el PinBlock que deben enviarse en el **Transaction Processing** como pin.

Adicional a esto, favor basarse en la documentación oficial: [Solicitud de PinPad](#)

Para las operaciones con PinPad el comercio puede implementar la librería con la siguiente documentación: [PinPad SDK - Placetopay Docs](#)

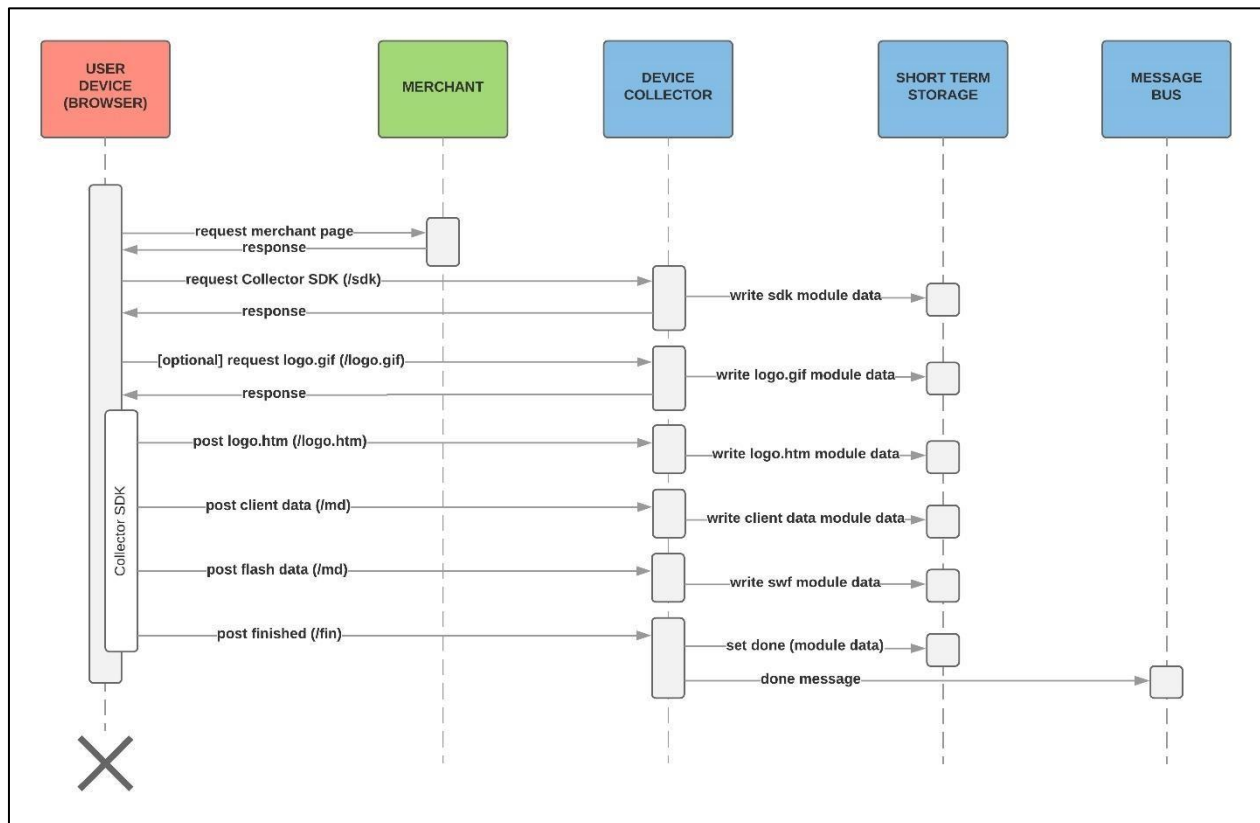
### 13. AUTENTICACIÓN KOUNT

El sistema debe de enviar en la mensajería del **Transaction Processing** un objeto kount con los atributos de una sesión qué es un valor aleatorio único por cada transacción

```
"kount": {
  "session": "C0485"
}
```

Adicional a esto, favor basarse en la documentación oficial: [Placetopay Docs](#) y [Kount - Placetopay Docs](#)

Este servicio bloquea el fraude, reduce la fricción con los tarjeta habientes y genera confianza para las de transacciones realizada en Placetopay como proveedor antifraude.



Para las integraciones que requieren validación de seguridad kount para el control antifraude, es importante realizar los siguientes pasos:

1. Después de registrarte para los servicios de Kount y recibir un ID de cliente, agrega el SDK del Cliente Web a tu sitio web para integrar el Colector de Datos del Dispositivo. Para mas información ver documentación: [How to Integrate the Web Client SDK for Device Data Collection into Your Website – Kount Developer](#)
2. Luego de obtener la información se debe crear el id de sesión del dispositivo, ver documentación: [How to Create a Session ID for the Device Data Collector \(DDC\) – Kount Developer](#)
3. Para crear la sesión kount debe generarse con los datos **clientId= 201000**, **Environment=TEST (sandbox)** o **Environment=PROD (production)** una vez obtenida la conexión Data device collector (DDC) enviar el kount sesión en el objeto kount.

```
"kount": {  
  "session": "ba2ccc0c27d84921ae9034da92ebc74d"  
}
```

4. Para descargar el repositorio del SDK de kount, en el siguiente enlace: <https://github.com/luisfelipeggh/kount-ddc?tab=readme-ov-file>

## 14. VALIDACIÓN DE CAMPOS

El comercio debe como mínimo enviar los siguientes campos requeridos en la solicitud de pago:

Datos del comprador y pagador(buyer-payer):

- Nombre del comprador-pagador.
- Apellido del comprador-pagador.
- Email del comprador-pagador.
- Teléfono celular del comprador-pagador.

Datos del pago (payment):

- Referencia (única por transacción)
- Descripción
- Moneda ● Valor.
- Impuesto (opcional)
- Base de devolución (opcional)
- Recurrencia (En caso de habilitar el servicio)
  - Periodicidad

- Intervalo
- Fecha próximo pago
- Número máximo de periodos
- Fecha para finalizar la recurrencia
- Url para confirmación de pagos (opcional)

#### Datos de la tarjeta (instrument)

- Tarjeta
  - Número o PAN
  - Expiración
  - CVV
- threeDS
  - Id
  - Enrolada
  - Autenticada
  - Firma valida
  - Eci
  - Cavv
  - Xid
  - Version
  - Extra
    - Motivo estado de la autenticación
    - AcstransId
    - threeDSServerTransID
- Pinpad (En caso tal de habilitar el servicio)
  - TransactionId
  - Posiciones
  - PinBlock
  - Longitud
- Pin
- Account (En caso tal de habilitar el servicio)
  - bankCode
  - bankName
  - accountType
  - accountNumber
  - franchise
  - verificationcode
- Kount
- AVS (En caso de habilitar el servicio)

- Session
- Type

#### Datos adicionales

- IP.
- Agente de navegación.

Importante: Debe tener en cuenta que cada uno de los campos debe contener información coherente. Adicional a esto, favor basarse en la documentación oficial en caso de cambios: [Placetopay Docs](#)

- El sistema solicita al usuario el número de tarjeta como un campo obligatorio, sólo recibe valores numéricos. y tiene una longitud de 13 a 19 caracteres, validando el valor digitado a través del algoritmo de Luhn.
- La aplicación solicita o presenta al usuario la fecha de vencimiento como un campo obligatorio, validando que la fecha de vencimiento no esté vencida y sólo reciba el valor del mes de enero a diciembre, es decir, del 01 al 12 (Siempre a dos dígitos). Permitiendo como máximo la elección de 10 años, a partir de la fecha actual.
- El sistema solicita al usuario el CVV2 como un campo obligatorio enmascarado, sólo recibe valores numéricos y tiene una longitud máxima de 4 caracteres (American Express es la única que debe permitir como máximo 4 caracteres, Visa, Mastercard y Discover solo 3).
- La referencia debe contener una longitud máxima de 32 caracteres alfanuméricos y no debe contener o almacenar el número de la tarjeta y caracteres especiales siendo única por cada solicitud.
- Para los datos del comprador y pagador(buyer-payer) se debe validar cada uno de los campos que están siendo enviado a Evertec Placetopay como requeridos al momento que el usuario está ingresando la información.
- Para los campos nombre y apellido no se debe de permitir el ingreso de números ni caracteres especiales, sin embargo, debe permitir el ingreso de la tilde, espacios y la letra Ñ. Para empresas se debe solo el nombre legal del comercio y para este caso si se debe permitir números.
- Para los campos numéricos como móvil o teléfono no debe permitir el ingreso de letras, ni caracteres especiales.
- Para el campo email debe contar con una estructura valida,  
[usuario/a]@[dominio].[Tipo de origen].[Extensión].
- La dirección IP y agente de navegación deben de ser las pertenecientes al dispositivo del usuario final.

En el proceso de paga no siempre el comprador es el mismo titular, por lo que se debe tener en cuenta esta información al momento de enviar estos datos a Evertec Placetopay.

**Nota:** La implementación de preguntar por la propiedad de la tarjeta, se considera una buena práctica y es opcional, sin embargo, si el comercio toma la determinación de no implementar esto, debe garantizar que siempre envían la información del pagador o tarjetahabiente.

## 15. CONTROL DE IDEMPOTENCIA (PAGOS DUPLICADOS)

La validación para evitar transacciones duplicadas debe realizarse durante el Flujo del Proceso de Pago, este proceso se puede hacer mediante el envío del keyword de Idempotencia "IdempotenceKey", el cual es un valor único definido por el comercio para cada transacción, debe enviarse dentro de la Solicitud de Pago.

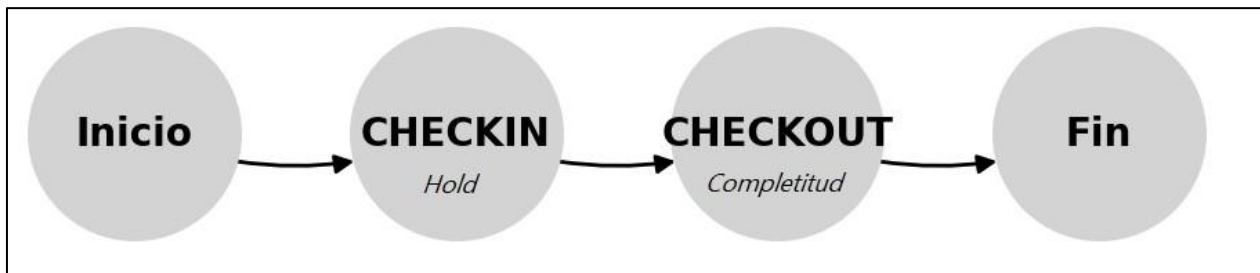
```
{ ...  
  "idempotenceKey": "ABCD1234",  
  "instrument": {  
    ...  
  }  
}
```

Para más detalles por favor basarse en la documentación oficial: [Control de Idempotencia - Placetopay Docs](#)

NOTA: El Comercio generará y enviará el Parámetro IdempotenceKey con un valor único basado en la Lógica de Negocio para cada transacción. El sistema impedirá que se procesen transacciones con la misma IdempotenceKey.

## 16.PROCESAMIENTO PAGOS CON PREAUTORIZACIÓN.

Para el procesamiento con pagos preautorizados, el usuario/tarjeta habiente debe completar el proceso reservando el monto solicitado de su tarjeta de crédito, una vez se realice la reserva, este valor puede ser confirmado, modificado o cancelado.



**Nota:** Tener en cuenta que este ítem aplica si se realizó la contratación del medio del servicio Preautorización.

### 16.1. CHECKIN:

Se utiliza como depósito de garantía por la utilización de un bien o servicio. Para reservar el monto se debe enviar en la petición los siguientes datos:

```
"action": "checkin",
"payment": {
  "reference": "pay_checkin_1",
  "description": "Payment with pre-auth",
  "amount": {
    "currency": "USD",
    "total": 10
  }
}
```

### 16.2. CHECKOUT

Para confirmar/capturar el valor preautorizado de la reserva se debe enviar la siguiente información:

```
"internalReference": 11012331, //código de referencia interna
"authorization": "000000", //número de autorización entregado por la
entidad financiera.
  "amount": {
    "currency": "USD",
    "total": 15
  },
```



```
"action": "checkout"
```

Nota: El internalReference se entrega en la respuesta del servicio.

### 16.3. CANCELACIÓN DE UNA PREAUTORIZACIÓN

Para anular una reserva (Check-in) previamente autorizada se debe enviar el action del checkout por un valor igual 0.

```
"internalReference": 11012331,  
"authorization": "000000",    "amount": {  
    "currency": "USD",  
    "total": 0  
},  
"action": "checkout"
```

La preautorización es cancelada y se libera el monto retenido en las peticiones previas.

Para más info acerca de preautorización: [Tipos de transacciones - Placetopay Docs](#)

### 16.4. REINTENTOS DE CAPTURA (CHECKOUT)

En caso de que las transacciones preautorizadas, al momento de realizar el proceso de captura, ocurra algún error y decline la transacción, el comercio deberá realizar un máximo de 3 reintentos de captura. Estos reintentos se recomiendan que se realicen cada 60 segundos. En caso de que al tercer intento el error persista, se deberá anular la operación enviando el action del checkout por un valor igual a 0 (cancelación de la preautorización)

| Date                | Amount | Status   | Type     |
|---------------------|--------|----------|----------|
| 2024-04-04 21:18:45 | 0,00   | Approved | Checkout |
| 2024-04-04 21:18:16 | 201,00 | Declined | Checkout |
| 2024-04-04 21:18:12 | 201,00 | Declined | Checkout |
| 2024-04-04 21:18:02 | 201,00 | Declined | Checkout |
| 2024-04-04 21:12:22 | 190,00 | Approved | Checkin  |

## 17. PROCESAMIENTO DE PAGOS CON TOKENIZACIÓN.

Al realizar un pago con tokenización el usuario debe ingresar la información de tarjeta para que luego sean encriptados los datos de tarjeta (número y fecha de expiración), esto con el fin efectuar el cobro sobre ese medio de pago.

Para realizar la tokenización es necesario enviar los datos de tarjeta con el método del servicio *tokenize*, ver documentación: [Placetopay Docs](#)

**Nota: Tener en cuenta que este item aplica en caso tal se haya contratado el servicio de tokenización.**

### 17.1. COBRAR MEDIO DE PAGO TOKENIZADO

Al obtener el token o subtoken después de que el tarjeta habiente hizo la tokenización, se debe enviar la siguiente información:

```
"payment": {
  "reference": "1122334455",
  "description": "Testing",
  "amount": {
    "currency": "USD",
    "total": 100
  }
},
"instrument": {
  "token": {
    "token":
    "e07ca9986cf0ecac8a557fa11c07bf37ea35e9e3e3a4180c49"
  }
},
```

El token o subtoken se podrá obtener en la respuesta del método en el arreglo instrument.

El token o la llave encriptada, generada por un proceso de tokenización, permite generar cobros sin interacción del usuario o pagos a un clic.

**Importante:** Para pagos que requieran envío de pin (Puerto Rico) es necesario solicitar a la tarjeta habiente esta información de seguridad para su procesamiento:

```
"payment": {
  "reference": "1234567890",
  "description": "Token payment with pin",
  "amount": {
    "currency": "USD",
    "total": 19.9
  }
},
"instrument": {
  "pin": "0B880E2326F6409E",
"token":
"ee1d56a192dc07e4e403cdaa2569407118a0e19dc185b1e63bad2b2edc2a3bf0",
  "subtoken": "5172915969800005",
  "franchise": "ath_card",
  "franchiseName": "ath_card ",
  "lastDigits": "0005",
  "validUntil": "2018-12-31"
}
}
```

Es muy importante que la información del pagador sea enviada en el servicio de cobro con token, ya que esta se valida en el procesamiento en cara a la seguridad transaccional y validación de datos de tarjeta habiente.

## 17.2. TOKENIZACIÓN MEDIO DE PAGO ATH CON PIN

Al realizar un proceso de tokenización para el medio de pago ATH con PIN, es importante tener en cuenta que, para poder efectuar el cobro, únicamente debe hacerse cuando el usuario utiliza alguna wallet solicitando nuevamente el ingreso del PIN. Esto significa que, deben disponerle al cliente un PINPad con el fin de que el usuario pueda digitarlo en la interfaz.

**Nota:** Es importante tener en cuenta que, para este medio de pago, no es posible que del lado del comercio genere un cobro recurrente o periódico, ya que esta operación no permite cobros sin el ingreso del pin (operación PINless)

### 17.3. INVALIDACIÓN DE TOKEN

Es muy importante la administración de tokens o llaves para los instrumentos de pago, teniendo almacenada esta información de forma segura y controlar los estados de dichas llaves en bases de datos.

Para la invalidación de un token que existe en tu base datos es necesario enviar la siguiente información:

```
{
  "auth": {...},
  "locale": "en_PR",
  "instrument": {
    "token": {
      "token":
      "a3bfc8e2afb9ac5583922eccd6d2061c1b0592b099f04e352a894f37ae51cf1a"
    }
  }
}
```

Ver documentación para invalidar token: [Tokenization \(invalidate\)](#)

**Nota:** Se valida que en caso de estar tokenizando un medio de pago, se exponga un botón o un apartado donde el usuario pueda inhabilitar/eliminar el medio de pago.

### 17.4. ELIMINACIÓN DE TOKEN POR RECHAZOS.

Tener en cuenta que se debe de tener un control sobre los medios de pago tokenizados, donde si alguno de estos genera un rechazo consecutivo (3 veces) el medio de pago debe de ser removido de forma automática utilizando el método Invalidate token. Esto se debe implementar ya que las marcas tales como Visa, Mastercard, entre otras... generan multas/sanciones en caso tal se intente realizar cobros con algún medio de pago que rechace continuamente.

## 18. MANEJO DE RESPUESTAS PARA ESTADOS TRANSACCIONALES

Al momento que el usuario culmine su proceso de pago, se debe mostrar el detalle de la transacción, como mínimo deben visualizarse los siguientes datos:

- Referencia. (Requerido)
- Estado final de transacción (Requerido)
  - Aprobado
  - Rechazado
  - Pendiente
  - Fallido
- Razón y mensaje
- Fecha y hora. (Requerido)
- Valor total. (Requerido) ● Recibo.
- Autorización.
- Últimos 4 dígitos de la tarjeta

**USD \$33.18**

**Aprobada**

**Fecha:** 2018-02-05 22:17:11

**Total pagado:** USD \$33.18

**Autorización / CUS:** 000000

**Recibo:** 1449217016

**Referencia:** 192837465

**Estado:** Aprobada

**Código Respuesta:** 00

Si desea indicarle más información al usuario final, puedes seguir el formato de [FORMATO DE PLANTILLAS DE RESPUESTA](#) descrita en este documento, mostrando el estado de acuerdo con la respuesta emitida por Evertec Placetopay.

Recomendaciones alineadas a la experiencia de usuario:

- Respuesta aprobada: es posible adicionar un vínculo o botón que le permita al usuario y/o cliente ir al inicio (home) del proceso del pago, de igual forma se evaluará la recepción.

Volver al inicio

- Respuesta rechazada y fallida: se recomienda adicionar un vínculo o botón que le permita al usuario y/o cliente reintentar el pago.

Reintentar pago

### 18.1. CONTROL TRANSACCIÓN PENDIENTE:

Se puede visualizar una transacción en estado pendiente por respuesta directa de la entidad financiera o la no recepción de respuesta por parte de Evertec Placetopay (TimeOut).

Existen tres formas de obtener el estado final de una transacción: la primera, a través de la respuesta del servicio en el momento de realizar el **TransactionProcessing**; la segunda, en caso de recibir un estado PENDIENTE, mediante el método **TransactionQuery** utilizando la referencia interna; y la tercera, a través del servicio de **TransactionSearch**, que actúa como una medida de contingencia en caso de pérdida de comunicación al crear la transacción con el **TransactionProcessing**.

Nota: El consumo hacia el servicio para conocer el estado final de una transacción pendiente siempre debe hacerse mediante el método **Transaction Query**, el uso del método **Transaction Search** es únicamente en caso de pérdida en la comunicación cuando se realiza la transacción.

Se cuenta con dos formas para obtener el estado final de una transacción, mediante la URL de notificación (webhook) y la sonda o tarea programada (cronjob):

- **Url de notificación:** Este proceso tiene la finalidad de informar a su sistema cuando las transacciones cambian de estado pendiente a un estado final. La url de notificación es configurada por el comercio en los puertos 80 o 443 y debe estar programada para recibir una petición tipo POST por parte de Evertec Placetopay, tiene una estructura similar a la siguiente:

```
{
  "status": {
    "status": "APPROVED",
    "reason": "00",
    "message": "Aprobada",
    "date": "2024-07-11T15:22:37-05:00"
  },
  "internalReference": 1,
  "reference": "5834381",
  "signature": "9c0f8ff164d0af4a795f71ee127d8926f56d05fb"
}
```

Al consumir el servicio **Transaction Processing**, se puede genera automáticamente un timeout de la red de pago en caso tal no haya una respuesta a tiempo.

- **Sonda o Cronjob (opcional):** Este proceso consiste en una tarea programada (cronjob) la cual se encarga de consumir el método **Transaction Query** (consulta de transacción) sobre las transacciones que quedaron en estado pendiente en sus registros, este procedimiento se debe ejecutar cada 12 minutos verificando las transacciones que tengan más de 5 minutos en estado pendiente.

Cuando se encuentre una transacción en estado pendiente o en proceso en la base de datos, el sistema debe informar y presentar el siguiente evento:

- Un **mensaje control de doble pagos** informando al usuario la existencia de transacciones pendientes, antes de realizar un nuevo pago. Por ejemplo: ■ “En este momento su pedido con \*#Referencia\* y valor de \*#Amount\* se encuentra en un estado de PENDIENTE de no recibir confirmación por parte de su entidad financiera, por favor espere unos minutos y vuelva a consultar más tarde para verificar si su pago fue confirmado de forma exitosa. Si desea más información sobre el estado actual de su operación puede comunicarse a nuestras líneas de atención al cliente \*000-00-00\* o enviar un correo electrónico a email@email.com y preguntar por el estado de la transacción: <#CUS/Autorización>\*\*\*”.

## 18.2. TIMEOUT 32 SEGUNDOS

Para las respuestas que se brindan mediante el proceso de webhook puede ocurrir un encolamiento durante el proceso de notificación, esto puede ocurrir por demoras en la respuesta de la red procesadora. En ese sentido, el equipo de desarrollo del comercio

debe configurar un TimeOut con un tiempo de espera máximo de 32 segundos para recibir esta notificación. En caso de exceder este tiempo, el comercio deberá marcar la transacción como fallida y proporcionar una respuesta de cara al cliente como 'Transacción declinada'.

## 19. COMPROBANTE DE VENTA

En caso de que desde el sistema se envíen comprobantes de venta (Impresión, e-mail, archivo exportado, mensaje de voz) propios de acuerdo con cada uno de los estados de transacción y se presente información relacionada al pago, se valida que la información mostrada se contraste con la información de la transacción verificando que de acuerdo con los campos mostrados la información sea coherente con relación al pago. Se recomienda que el usuario visualice la siguiente información:

- La referencia.
- Fecha y hora de la transacción.
- Estado de la transacción.
- Total pagado por el usuario.
- Tipo de crédito y diferido (Ecuador) o cuota seleccionada por el usuario final.
- Los cuatro últimos dígitos de la tarjeta
- Banco

Sino se cuenta con un comprobante de pago propio se toma como referencia el comprobante emitido por Place**topay** Evertec.

## 20. HISTÓRICO TRANSACCIONAL

En caso de que sea necesario autenticarse en el sitio del comercio para realizar un proceso de pago, se debe permitir consultar el estado de por lo menos las últimas diez (10) transacciones realizadas. Cada registro debe contener como mínimo los siguientes datos ordenados de forma descendente por fecha:

- Fecha y hora de la transacción.
- Número de referencia (emitida por el comercio).
- Autorización/CUS. (opcional)
- Estado de la transacción.
- Valor (debe estar concatenado con el tipo de moneda según ISO 4217).



| FECHA Y HORA           | REFERENCIA | ESTADO           | AUTORIZACIÓN/CUS | VALOR     |
|------------------------|------------|------------------|------------------|-----------|
| 31/01/2022 6:50 p. m.  | ORDEN_515  | PENDIENTE        | 5555             | USD \$200 |
| 31/01/2022 1:00 p. m.  | ORDEN_501  | APROBADO         | 5439             | USD \$289 |
| 30/01/2022 10:59 a. m. | ORDEN_459  | RECHAZADO        | 5276             | USD \$76  |
| 29/01/2022 3:05 p. m.  | ORDEN_420  | APROBADO PARCIAL | 5002             | USD \$526 |

Nota: En caso de que no se haga uso de login en la página y por reglas de negocio no sea posible implementar un apartado donde se puedan consultar los pagos, se le debe informar al analista de Evertec Placetopay, la razón o motivo para que sea analizada y dar la excepción sobre este.

## 21. SEGURIDAD DE LA INFORMACIÓN

El sistema y comercio deben de cumplir los siguientes criterios:

- El comercio debe estar certificado en PCI (vigente)
- El sistema bajo ningún motivo almacena información sensible del tarjetahabiente.
- El sistema no muestra en los resúmenes de pago, comprobantes de venta o cualquier otro apartado de cara al usuario el número de la tarjeta (como máximo BIN y últimos 4 dígitos)
- El sistema no muestra en los resúmenes de pago, comprobantes de venta o cualquier otro apartado de cara al usuario el CVV de la tarjeta.
- Se guarda en la base de datos del aplicativo la información mínima para un futuro reclamo (fecha y hora de transacción, número de recibo, valor de la transacción, número de autorización, máximo 4 últimos dígitos del número de tarjeta, referencia y pagaré, éste último si se aplica).
- El sistema debe contar con un certificado digital válido, realizando la captura de información utilizando el protocolo seguro HTTPS.
- Se debe utilizar el protocolo de TLS 1.2 o superior.
- Si el desarrollo utiliza una interfaz web (así sea intranet) la URL de captura de información no se enmascara (oculta) mediante técnicas como IFRAMES.

## 22. PROCESAMIENTO DE LA INFORMACIÓN

Al realizar una transacción, se envía al aplicativo Evertec Placetopay los mismos datos que fueron validados, digitados o seleccionado en la interfaz de usuario:

- Número de tarjeta
- CVV
- Fecha de Vencimiento
- Valor Total
- Moneda

- Referencia
- Descripción
- Impuesto (opcional)
- Base de Devolución (Opcional si no se usan impuestos)
- Información del usuario
- Información de los protocolos de seguridad

## 23. COHERENCIA DE LA INFORMACIÓN

La información enviada a Evertec Placetopay no debe tener contrastes en cada interfaz en la cual se presente información referente al pago, de acuerdo con esto se debe cumplir con los siguientes aspectos:

- La fecha y hora de la transacción presenta un valor consistente entre la base de datos del desarrollo del comercio, la consulta de la consola de Evertec Placetopay y el comprobante de venta generada por el desarrollo cuando se realizan transacciones.
- Los cuatro últimos números de la tarjeta aparece de manera única y coincidente entre la base de datos del desarrollo del comercio y la consulta de la consola de Evertec Placetopay.

## 24. DIRECCIÓN IP Y AGENTE DE NAVEGACIÓN

Cuando se envíe la petición para procesar la transacción con el método ***Transaction Processing*** es importante enviar los parámetros ipAddress y userAgent como se menciona en el punto VALIDACIÓN DE CAMPOS (processTransaction). Son datos adicionales requeridos que deben enviar para el control de filtro de seguridad transaccional.

Ejemplo:

```
...  
"ipAddress": "192.168.1.109",  
"userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64)  
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0  
Safari/537.36"  
...
```

La dirección IP debe ser tomada del dispositivo del cliente ya sea realizando una función desde tu código o por medio de un script según tu lenguaje de programación, de igual modo con el agente de navegación, ya sea en una página web o una aplicación en donde se encuentre integrado el servicio.

## 25. ENVIO EXTRADATA

Puedes enviar información adicional en las peticiones por medio de extrada. Si dentro del proceso de pago se necesita añadir, por ejemplo, una segunda referencia u otro dato relevante en la petición. lo puedes realizar por medio de un arreglo de objetos llamado **additional**.

Ejemplo:

```
...
"additional": {
  "merchantCode": "468231",
  "terminalNumber": "00990101"
},
...
```

### 25.1. CUSTOMER ACCOUNT NUMBER

Si deseas enviar particularmente información adicional sobre una cuenta de cliente donde tenga servicios y que de esta forma es identificado desde tu sistema como un número de cuenta de cliente, debes enviar la extrada de la siguiente manera:

```
" additional ": {
  " CustomerAccountNumber ": "8100312356677"
}
]
```

**Nota:** Las siguientes claves NO son permitidas: `_accountNumber`, `userAgent`, `fingerprint`, `sourcePlatform`, `tokenizationID`, `trazabilyCode`, `transactionCycle`, `RequestId`, `PartnerAuthCode`.

## 26. REVERSO DE TRANSACCIONES

Se debe definir el proceso de reverso de transacciones, en caso de que el comercio vaya a realizar reversos a través del api expuesto por Placetopay Evertec, se debe confirmar al analista, con el fin de que éste valide la funcionalidad y garantice el correcto funcionamiento, por otra parte, si se va a usar la consola administrativa debe ser informado a través del correo en el hilo del analista encargado.

Nota: El reverso solo será posible antes de la hora de conciliación, en caso tal se requiera realizar este proceso posterior a la hora definida, se debe de realizar un reembolso, de la misma forma se debe de informar si los reversos se realizaran mediante la API o mediante la consola administrativa.

## 26.1. REEMBOLSO DE TRANSACCIONES

En caso de que se desee realizar reembolsos a través del api expuesta por **Placetopay Evertec**, se debe confirmar al analista, con el fin de que éste valide la funcionalidad y garantice el correcto funcionamiento, por otra parte, si se va a usar la consola administrativa debe ser informado a través del correo en el hilo del analista encargado.

Nota: Tener en cuenta que los reembolsos serán efectivos si se realizan posterior a las 3:00 PM (Hora de corte estándar).

### 26.1.1. TIPOS DE REEMBOLSOS REEMBOLSO PARCIAL

#### Reembolso Total

Se utiliza para reembolsar la totalidad del monto aprobado en la transacción.

```
{
  "auth": {},
  "internalReference": int,
  "authorization": "int",
  "action": "refund",
}
```

A continuación, se detallan puntos importantes de la respuesta de una transacción consultada posteriormente a un reembolso:

Nos encontraremos el objeto “refunded” el cual nos indica con “true” que la transacción fue reembolsada.

```
"refunded": true,
```

## Reembolso parcial

Se utiliza para reembolsar una parte del monto aprobado en la transacción, se debe enviar la propiedad “amount” en la petición, este dato debe contener el monto que se quiere reembolsar.

```
{
  "auth": {},
  "internalReference": int,
  "authorization": "int",
  "action": "refund",
  "payment": {
    "amount": {
      "currency": "string",
      "total": int
    }
  }
}
```

Los reembolsos parciales se pueden realizar tantas veces como sea necesario hasta que se complete el monto total aprobado en la transacción. Una vez que una transacción se ha reembolsado por completo, no es posible realizar otro reembolso.

**Nota: Los reembolsos parciales solo se puede efectuar una vez la transacción haya pasado por la hora de corte y se hayan conciliado, que generalmente es al siguiente día hábil.**

A continuación, se detallan puntos importantes de la respuesta de una transacción consultada posteriormente a un reembolso:

Nos encontraremos el objeto “refunded” el cual nos indica con “true” que la transacción fue reembolsada.

```
"refunded": true,
```

Dentro del array “additional” nos encontraremos con la siguiente estructura, la cual nos indica que monto de la transacción se ha reembolsado

```
{
  "merchantCode": "int",
  "terminalNumber": "string",
  "bin": "int",
  "_wcTransactionId_": "int",
  "amountRefunded": int }
```

## 27. INFORMACIÓN RELEVANTE

### 27.1. FORMATO DE PLANTILLAS DE RESPUESTA

Las plantillas de respuesta son formatos informativos para el usuario final con respecto a su pago, por lo cual es importante mostrar los datos relevantes en las plantillas; deben de estar libres de errores ortográficos, de codificación de caracteres y sean consistentes como se describen a continuación:

- Fecha y hora de transacción.
- Valor o monto de la transacción: Tener en cuenta que deben presentarse en formato decimal a dos dígitos junto con el tipo de moneda (USD 938,99)
- IVU (Estatul, Municipal y Reducido): Valor cobrado del impuesto aplicado con el tipo de moneda (USD 25,93)
- Estado de la transacción: Los cuales son: Aprobada, Rechazada y Fallida. (El sistema responde con los estados en inglés, se debe traducir al idioma que predomine en la página).
- Razón y Motivo: Es el mensaje de error o motivo de declinación emitido por la entidad financiera.
- Franquicia: Nombre de la marca de la tarjeta con la cual se realizó la transacción.
- Banco: Es la entidad a la cual pertenece la tarjeta o la cuenta de la transacción
- Autorización/CUS: Es el código único de seguimiento o el # de autorización emitido por la entidad financiera.
- Recibo: Consecutivo generado por la red, emitido por Evertec Placetopay.
- Referencia: Es la referencia de pago generada por cada comercio y debe ser única para cada transacción.
- Descripción: Debe indicar de manera real el concepto o la descripción del pago.
- Dirección IP: Se debe mostrar la dirección IP del equipo donde el usuario final está realizando la transacción.
- Nombre del comprador o cliente: nombre y apellidos del comprador o cliente.

- Consulta: Teléfono, Email, o enlace a formulario de consulta, donde el usuario pueda obtener información adicional de su transacción.

Nota: el comercio deberá definir la forma y el orden para mostrar los datos, pero son obligatorias las etiquetas y la estructura de los datos. A continuación, se presentan ejemplos de aplicación para la página de respuesta en el sitio:

| Nombre                 | Información  |
|------------------------|--|
| Fecha y Hora           | p2p.get.payment[date]  |
| Estado                 | "Transacción" + Resultado de la transacción - Aprobada/Rechazada/Pendiente/Fallida |
| Descripción del pago.  | p2p.get.Description  |
| Motivo                 | p2p.get.ErrorCode() + "-" + p2p.ErrorMessage()                                     |
| Autorizac/CUS          | p2p.get.authorization()  |
| Tipo de moneda y Valor | p2p.getCurrency() + p2p.getTotalAmount()   |
| Iva                    | p2p.getCurrency() + p2p.getTaxAmount()   |

- Ejemplo de la plantilla de respuesta (Transacción aprobada):


**USD \$33.18**

Aprobada

**Fecha:** 2018-02-05 22:17:11  
**Total pagado:** USD \$33.18  
**Autorización / CUS:** 000000  
**Recibo:** 1449217016  
**Referencia:** 192837465  
**Estado:** Aprobada  
**Código Respuesta:** 00

- Ejemplo de la plantilla de respuesta (Transacción rechazada):

**USD \$33.18**

**Rechazada**

**Fecha:** 2018-02-05 22:17:11

**Total pagado:** USD \$33.18

**Autorización / CUS:** 000000

**Recibo:** 1449217016

**Referencia:** 192837465

**Estado:** Rechazada

**Motivo:** Fondos insuficientes

**Código Respuesta:** 05

## 27.2. TARJETAS Y BANCOS DE PRUEBA PARA REALIZAR TRANSACCIONES:

Por normas PCI no podemos incluir tarjetas de crédito e información adjunta en correos, sin embargo, a través del siguiente enlace pueden visualizar las tarjetas para realizar las pruebas pertinentes: [Números de tarjeta de pruebas - Placetopay Docs](#)

Nota: Para todas las franquicias:

- Código de verificación: 123
- Fecha de vencimiento de la tarjeta: Seleccione una fecha vigente
- AVS: 55555

## 27.3. CONSIDERACIONES

Esta información entregada junto a la evaluación de peritaje que se realiza del sitio es fundamental, dado que son tenidos en cuenta para los checklists de pruebas y si todos los puntos no se encuentran OK, el comercio NO podrá salir a producción.

Para el proceso de certificación se debe de enviar la información al analista asignado de Placetopay Evertec con los siguientes datos:



- **Url de pruebas:** El sitio habilitado para realizar la revisión y certificación
- **Usuario y clave:** Datos de acceso para el ingreso y simulación del pago.

## 28. PROCESAMIENTO CON CUENTAS BANCARIAS (ACH)

Para procesar transacciones utilizando como instrumento de pago una cuenta bancaria se requiere implementar el instrumento de pago account que permite definir los datos de la cuenta a utilizar, así como los mecanismos para hacer validación de la cuenta utilizando el método: Validate an existing Account. Ver documentación: [Account Validator Docs](#)

Es importante mencionar que para integrar el procesamiento con cuentas bancarias debe integrarse el validador de cuentas que es un proceso adicional para verificar la veracidad y disponibilidad de las cuentas, validando información como:

- El estado de la cuenta, es decir si la cuenta se encuentra activa o no.
- El monto disponible en la cuenta para identificar si es posible realizar la transacción por el monto indicado.

Este proceso se realiza antes de procesar la transacción, [Placetopay Docs](#)

## 29. Webhook Devoluciones ACH (PR Opcional)

Este ítem aplica cuando el comercio hace uso del medio de pago ACH. En este caso, debe contar con un Webhook que le permita controlar y parametrizar las devoluciones asociadas a este medio de pago.

El comercio debe proporcionar una URL/URI pública donde pueda recibir las notificaciones enviadas por Placetopay. Esta URL debe estar habilitada para aceptar solicitudes HTTP tipo POST con estructura en formato JSON, como se muestra a continuación:

Body:

```
{
  "time": "2024-11-14T05:50:15-05:00",
  "type": "chargeback.created",
  "data": {
    "status": {
      "status": "APPROVED",
      "reason": "R01",
      "message": "Fondos insuficientes",
      "date": "2024-07-03T22:59:00-05:00"
    },
    "date": "2024-07-03T22:59:00-05:00",
    "transactionDate": "2024-07-03T22:59:00-05:00",
    "internalReference": 2,
    "reference": "9123418",
    "paymentMethod": "EBACH",
    "franchise": "ach",
    "franchiseName": "Ebus ACH",
    "issuerName": null,
    "amount": {
      "taxes": [
        {
          "kind": "valueAddedTax",
          "amount": 0,
          "base": 0
        }
      ],
      "currency": "USD",
      "total": 20000
    },
    "conversion": {
      "from": {
        "currency": "USD",
        "total": 20000
      },
      "to": {
        "currency": "USD",
```

```
"total": 20000

},
  "factor": 1
},
  "authorization": "10000123",
  "receipt": null,

"type": "CHARGEBACK",
  "refunded": false,
  "lastDigits": null,
  "provider": null,
  "discount": null,
  "processorFields": {
    "id": "b66f02ffff79b79ea9587b3cd3507a50",
    "b24": "R01"
  },
  "additional": {
    "merchantCode": "4549106521651",
    "terminalNumber": "19371021",
    "bankName": "Test Bank",
    "accountNumber": "6789"
  }
}
```

### 29.1. Validar la firma

Para garantizar la autenticidad de cada notificación, Placetopay incluye en el encabezado de la solicitud HTTP el campo X-Signature, Puedes validar esta firma con un hash HMAC SHA-256 utilizando el contenido del cuerpo de la notificación (body) y la llave de transacción (tranKey) de tu sitio.

```
const crypto = require('crypto');

// Body de la solicitud y firma recibida
const body = JSON.stringify(notificationBody);
const receivedSignature = headers['X-Signature'];

const tranKey = 'YOUR_SITE_TRANKEY';

// Generar la firma localmente
const generatedSignature = crypto
  .createHmac('sha256', tranKey)
  .update(body)
  .digest('hex');

// Validar la firma
if (generatedSignature === receivedSignature) {
  console.log("La notificación es auténtica.");
} else {
  console.log("Firma inválida: la notificación no es auténtica.");
}
```

Se envía una notificación HTTPS al momento de generarse una devolución ACH. [Webhooks - Placetopay Docs](#)



[evertecinc.com](https://evertecinc.com)

