

MANUAL TÉCNICO DE INTEGRACIÓN



Alignet

GUÍA TÉCNICA DE INTEGRACIÓN

PAYME MODAL - PHP

VERSIÓN 5.5.0

Contenido

1. Requisitos y consideraciones técnicas necesarias	3
2. Generación y administración de claves SHA-2 para Wallet y V-POS2	5
3. Proceso de Envío y Recepción de Parámetros a Wallet	8
3.1 Procedimiento de Integración a Wallet	8
3.2 Consideraciones y recomendaciones	8
3.3 Parámetros de envío y respuesta	10
3.4 Ejemplo envío y recepción de parámetros	12
4. Proceso de Envío y Recepción de Parámetros con V-POS2.....	14
4.1 Procedimiento de Integración a V-POS2.....	14
4.2 Consideraciones y recomendaciones	14
4.3 Parámetros de envío y respuesta	16
4.4 Ejemplo envío y recepción de parámetros	22
4.5 Personalización del Formulario de Pagos	26
5. Proceso de Envío y Recepción de Parámetros para Otros Medios de Pago	27
6. Anexo 1: Set de pruebas para la certificación en el ambiente de Integración.....	29
7. Anexo 2: Set de pruebas para la certificación en el ambiente de Producción.	32
8. Anexo 3: Tarjetas de pruebas para ambiente de Integración y Producción.	34
9. Anexo 4: Consideraciones para el ambiente de Integración.....	35

1. Requisitos y consideraciones técnicas necesarias

Para poder integrarse bajo el lenguaje de programación PHP, será necesario tener instaladas las siguientes librerías:

- ✓ PHP5
 - ✓ OpenSSL 0.9.7 en adelante.
- **Comprobación de PHP para ver si posee las librerías instaladas y funcionando correctamente**
Se debe generar una página que contenga la siguiente sentencia de PHP:

```
phpinfo();
```

Lo cual genera una página como esta:

PHP Version 5.6.8 	
System	Windows NT ALGDES028 6.1 build 7601 (Windows 7 Business Edition Service Pack 1) i586
Build Date	Apr 15 2015 15:00:54
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\86\instantclient_12_1\sdk,shared" "--enable-object-out-dir=.\obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler

Véase lo resaltado para notar que el PHP actual posee las características pedidas. Ahora se buscará si es que el PHP posee correctamente los módulos necesarios, para eso hay que buscar si es que en la misma página de información del PHP se encuentran los apartados siguientes

- ✓ HASH
- ✓ OPENSSL
- ✓ XML
- ✓ SOAP

hash

hash support	enabled
Hashing Engines	md2 md4 md5 sha1 sha224 sha256 sha384 sha512 ripemd128 ripemd160 ripemd256 ripemd320 whirlpool tiger128,3 tiger160,3 tiger192,3 tiger128,4 tiger160,4 tiger192,4 snfru snfru256 gost gost-crypto adler32 crc32 crc32b fnv132 fnv1a32 fnv164 fnv1a64 joaat haval128,3 haval160,3 haval192,3 haval224,3 haval256,3 haval128,4 haval160,4 haval192,4 haval224,4 haval256,4 haval128,5 haval160,5 haval192,5 haval224,5 haval256,5

openssl

OpenSSL support	enabled
OpenSSL Library Version	OpenSSL 1.0.1j 15 Jan 2015
OpenSSL Header Version	OpenSSL 1.0.1m 19 Mar 2015

xml

XML Support	active
XML Namespace Support	active
libxml2 Version	2.9.2

soap

Soap Client	enabled
Soap Server	enabled

De esta forma se puede notar que el PHP ya está habilitado para poder usar el script compilado de PHP.

▪ **Compatibilidad de Pay-me con dispositivos y navegadores**

Así mismo se confirma que Pay-me Modal es compatible con los siguientes dispositivos, navegadores y sus versiones mayores a las detalladas a continuación:

- ✓ PC - Chrome v55.0.2883.87
- ✓ PC - Firefox v45.0
- ✓ PC - Internet Explorer v11
- ✓ PC - Internet Explorer v10
- ✓ PC - Edge
- ✓ Dispositivo móvil Android - Chrome v55.0.2883.91
- ✓ Tablet Android - Chrome v40.0.2214.109
- ✓ iPhone 6 - IOS v10.2 - Safari v10
- ✓ iPad Mini 4 - IOS v10.2 - Safari v10
- ✓ MacBookPro Retina 15 - macOS Sierra v10.12.2 - Safari v10.12.2

2. Generación y administración de claves SHA-2 para Wallet y V-POS2

Con la finalidad de que la transmisión de información entre el comercio y Pay-me se realice de forma segura, guardando los tres principios de seguridad: protección, integridad y autenticidad de datos, el comercio generará un par de claves SHA-2 para generar una firma digital con los parámetros que se envíen a ambos módulos de Pay-me: Wallet y V-POS2.

Las claves SHA-2 son obtenidas accediendo al sistema V-Payment, en la opción Llave Públicas/Privadas del menú Administración:

Ambiente	Dirección URL
Integración	https://integracion.alignetsac.com/vpaymentweb/index.jsp
Producción	https://vpayment.verifika.com/vpaymentweb/index.jsp

Es responsabilidad del comercio el almacenamiento de las claves en un entorno seguro.

Detalle del formato de las claves SHA-2:

Ambiente	Nombre	Modulo
Integración	PASSWORD_COM_YYYY_WALLET_AAAAAAAAAAAAAA.txt	Wallet
	PASSWORD_COM_XXXX_PASARELA_BBBBBBBBBBBBBB.txt	V-POS2
Producción	PASSWORD_COM_YYYY_WALLET_AAAAAAAAAAAAAA.txt	Wallet
	PASSWORD_COM_XXXX_PASARELA_BBBBBBBBBBBBBB.txt	V-POS2

A continuación, se detalla el flujo para la generación de las claves SHA-2:

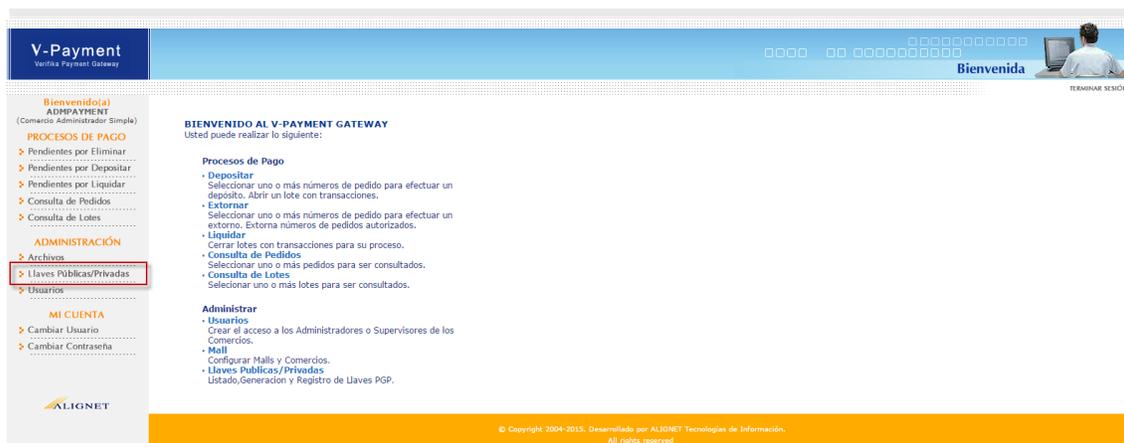


Figura 1. Página Inicio V-Payment



Figura 2. Registro de Claves SHA-2 V-Payment



Figura 3. Registro y descargar de Claves SHA-2 V-Payment

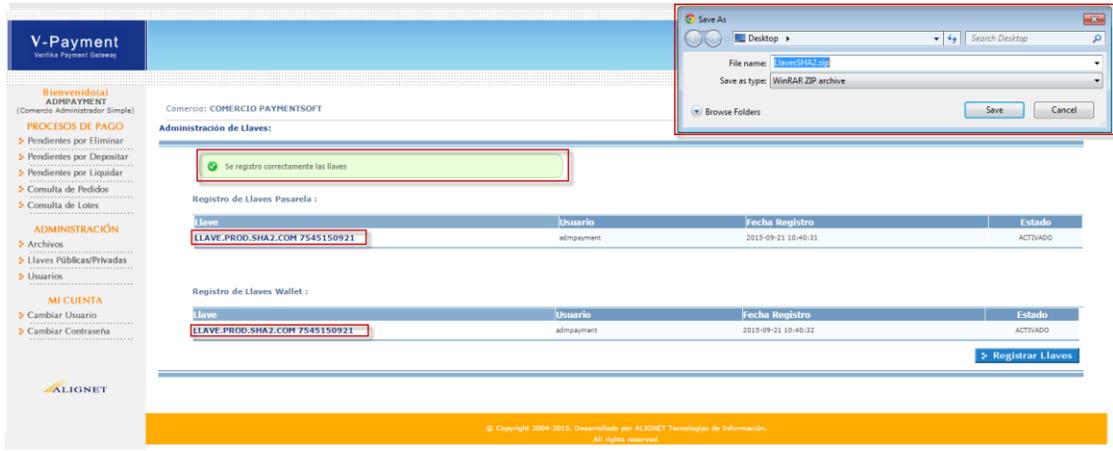


Figura 4. Registro y descargar de Claves SHA-2 V-Payment

3. Proceso de Envío y Recepción de Parámetros a Wallet

3.1 Procedimiento de Integración a Wallet

La forma de integración utilizada entre el comercio y Wallet es a través de servicios web, que incorpora como protocolo de seguridad la técnica criptografía SHA-2. En el web service de cada ambiente se encontrará el método RegisterCardHolder.

Ambiente	Dirección URL
Integración	https://integracion.alignetsac.com/WALLETWS/services/WalletCommerce?wsdl
Producción	https://www.pay-me.pe/WALLETWS/services/WalletCommerce?wsdl

3.2 Consideraciones y recomendaciones

- Ponemos a disposición del comercio una aplicación de demostración y guía sobre el consumo del servicio Wallet ubicado dentro del kit de integración.
- Considerar que ALIGNET enviará al comercio el ID de Wallet.
- Las claves SHA-2 necesarias para el envío de información son las siguientes:
(Detalle: Donde YYYY es el ID de comercio en la pasarela y AAAAAAAAAAAAAA es la fecha de emisión de la clave SHA-2.)

Ambiente	Nombre
Integración	PASSWORD_COM_YYYY_WALLET_AAAAAAAAAAAAAA.txt
Produccion	PASSWORD_COM_YYYY_WALLET_AAAAAAAAAAAAAA.txt

- d. Considerar que se podrán utilizar los métodos “openssl_digest” o “hash”, propios de PHP, para generar la firma cifrada, lo anterior dependiente de la versión PHP del ambiente tecnológico del comercio:

Versión PHP	Algoritmo
Mayor igual a PHP 5.3	<code>openssl_digest(\$idEntCommerce . \$codCardHolderCommerce . \$mail . \$claveSecreta, 'sha512');</code>
Menor a PHP 5.3	<code>hash('sha512', \$idEntCommerce . \$codCardHolderCommerce . \$mail . \$claveSecreta);</code>

3.3 Parámetros de envío y respuesta

- **Parámetros de envío**

A continuación, se detalla la lista de parámetros que el comercio debe enviar en el proceso de consumo del servicio web de Wallet:

Campo	Tipo	Ancho máximo	Descripción
idEntCommerce	Numérico	4	Es el código de servicio designado para el Comercio. Será entregado por ALIGNET.
codCardHolderCommerce	Alfanumérico	20	Código del tarjetahabiente (manejado por el comercio). Este valor se envía al V-POS2 en el parámetro userCommerce.
names	Alfanumérico	30	Primer nombre del tarjetahabiente
lastNames	Alfanumérico	30	Primer apellido del tarjetahabiente
mail	Alfanumérico	50	Correo del Tarjetahabiente
registerVerification	Alfanumérico	(Longitud no fija.)	Firma generada utilizando el algoritmo de cifrado SHA-2 en base a los parámetros enviados a Wallet.

El campo registerVerification contiene el valor cifrado de los campos idEntCommerce, codCardHolderCommerce, mail y la clave SHA-2 para Wallet descargada del sistema V-Payment. (PASSWORD_COM_XXXX_WALLET_XXXXXXXXXXXX.txt).

▪ **Parámetros de respuesta**

A continuación, se detalla la lista de parámetros que el comercio recibirá del consumo del servicio web de Wallet:

Campo	Tipo	Ancho máximo	Descripción
ansCode	Numérico	3	Código de respuesta de la operación solicitada.
ansDescription	Alfanumérico	30	Descripción del código de respuesta.
codAsoCardHolderWallet	Alfanumérico	30	Código único del tarjetahabiente asignado por Wallet. Este valor se envía al V-POS2 en el parámetro userCodePayme.
date	Alfanumérico	8	Fecha de operación
hour	Alfanumérico	8	Hora de la operación

3.4 Ejemplo envío y recepción de parámetros

- Ejemplo de envío de parámetros

A continuación, se mostrará un ejemplo técnico de la conexión a Wallet utilizando PHP.

```
//Se definen todos los parametros obligatorios.  
$idEntCommerce = '510';  
$codCardHolderCommerce = 'CLI001';  
$names = 'Juan';  
$lastNames = 'Perez';  
$mail = 'juan.perez@test.com';  
$reserved1 = '';  
$reserved2 = '';  
$reserved3 = '';
```

La clave SHA-2 será ingresada de forma escrita en el mismo código:

```
//Clave SHA-2.  
$claveSHA2 = 'frepFfNABxuASrdrmmS55695532889';
```

Para poder generar la firma cifrada utilizando los parámetros de envío a Wallet y la clave SHA-2, hay que invocar la función `openssl_digest`. Lo anterior generará la firma cifrada que será enviada a Wallet en el parámetro `registerVerification`.

```
$registerVerification =  
openssl_digest($idEntCommerce.$codCardHolderCommerce.$mail.$claveSecreta, 'sha512');
```

Finalmente se hará referencia al servicio web de Wallet, y se utilizará el método **RegisterCardHolder** para enviar los parámetros del tarjetahabiente:

```
//Referencia al servicio Web de Wallet
$wsdl='https://integracion.alignetsac.com/WALLETWS/services/WalletCommerce?wsdl';
$client = new SoapClient($wsdl);

//Creación de Arreglo para el almacenamiento y envío de parametros.
$params = array(
    'idEntCommerce'=>$idEntCommerce,
    'codCardHolderCommerce'=>$codCardHolderCommerce,
    'names'=>$names,
    'lastNames'=>$lastNames,
    'mail'=>$mail,
    'reserved1'=>$reserved1,
    'reserved2'=>$reserved2,
    'reserved3'=>$reserved3,
    'registerVerification'=>$registerVerification
);

//Consumo del metodo RegisterCardHolder
$result = $client->RegisterCardHolder($params);
```

- **Ejemplo de recepción de parámetros**

A continuación, se muestra un ejemplo de código implementado en PHP para la recepción e interpretación de los datos:

```
//Consumo del metodo RegisterCardHolder realizado en el último paso del //punto 3.1.
$result = $client->RegisterCardHolder($params);

//Lectura de parametros de respuesta.
echo "Código de Respuesta:" . $result->ansCode . "<br/>";
echo "Descripción: " . $result->ansDescription . "<br/>";

//Token que será enviado en el parametro userCodePayme en V-POS2.
echo "Código de Asociación: " . $result->codAsoCardHolderWallet . "<br/>";
echo "Fecha de Operación: " . $result->date . "<br/>";
echo "Hora de Operación: " . $result->hour . "<br/>";
```

4. Proceso de Envío y Recepción de Parámetros con V-POS2

4.1 Procedimiento de Integración a V-POS2

Para el envío de la solicitud de pago se deberá de generar una solicitud POST HTTPS, usando un formulario HTML, implementado en el lenguaje de programación del comercio o tienda virtual. Dependiendo del ambiente de integración, se deberá definir la url del JavaScript correspondiente:

Ambiente	Dirección URL
Integración	https://integracion.alignetsac.com/VPOS2/js/modalcomercio.js
Produccion	https://vpayment.verifika.com/VPOS2/js/modalcomercio.js

4.2 Consideraciones y recomendaciones

- Ponemos a disposición del comercio una aplicación de demostración y guía sobre el consumo del servicio VPOS2 ubicado dentro del kit de integración.
- Las claves SHA-2 necesarias para el envío de información son las siguientes:
(Detalle: Donde XXXX es el ID de comercio en la pasarela y BBBBBBBBBBBBBB es la fecha de emisión de la clave SHA-2)

Ambiente	Nombre
Integracion	PASSWORD_COM_XXXX_PARARELA_BBBBBBBBBBBBBB.txt
Producción	PASSWORD_COM_XXXX_PASARELA_BBBBBBBBBBBBBB.txt

- Considerar que se podrán utilizar los métodos “openssl_digest” o “hash”, propios de PHP, para generar la firma cifrada, lo anterior dependiente de la versión PHP del ambiente tecnológico del comercio:

Versión PHP	Algoritmo
Mayor igual a PHP 5.3	<code>openssl_digest(\$acquirerId . \$idCommerce . \$purchaseOperationNumber . \$purchaseAmount . \$purchaseCurrencyCode . \$slaveSecreta, 'sha512');</code>
Menor a PHP 5.3	<code>hash('sha512', \$acquirerId . \$idCommerce . \$purchaseOperationNumber . \$purchaseAmount . \$purchaseCurrencyCode . \$slaveSecreta);</code>

- d. La forma de integración entre el comercio y el V-POS2 es a través de javascript, donde este crea la función para invocar el diseño modal para el V-POS2.

```
//Invocar al JavaScript en el Head del Formulario
<head>
<script type="text/javascript"
src="https://integracion.alignetsac.com/VPOS2/js/modalcomercio.js" >
</script>
</head>
```

- e. El comercio en su formulario de envío deberá agregar un tag “class” para identificar los parámetros de envío. **Class=“ alignet-form-vpos2”**

```
//Definir el tag Class en el Form
<form name="f1" id="f1" action="#" method="post" class="alignet-form-vpos2">
```

- f. El comercio en su botón de pago deberá llamar a una función JavaScript llamada “AlignetVPOS2.openModal(Dominio del ambiente)”.

Ambiente	Ejemplo:
Integración	<pre> Comprar</pre> <hr/> <pre><input type="button" onclick="javascript:AlignetVPOS2.openModal('https://integracion.alignetsac.com/', '[TipoDeDiseño]')" value="Comprar"></pre>
Produccion	<pre>Comprar</pre> <hr/> <pre><input type="button" onclick="javascript:AlignetVPOS2.openModal('', '[TipoDeDiseño]')" value="Comprar"></pre>

Nota: Para el ambiente de producción no se deberá indicar en la función JavaScript el dominio. Además, tendrá la opción de seleccionar el tipo de diseño a utilizar. Deberá ingresar el código del diseño (1, 2, o 3) en la función openModal, en la sección “[TipoDeDiseño]”. Puede ubicar el detalle de los diseños disponibles en el punto 4.4.4 de la guía Funcional.

IMPORTANTE: Todos los navegadores **Safari** en sistemas operativos MacOS y iOS, presentan características por las que, para el correcto funcionamiento de la llamada a la pasarela modal, esta debe realizarse desde un bloque javascript accionado directamente por el usuario.

Las llamadas a la pasarela modal que se realicen desde bloques javascript cuya ejecución se desencadena por eventos automáticos como carga de formularios (onload), vencimientos de timeout (setTimeout) o algún otro en el que no exista intervención directa de usuario, presentarán error en navegadores Safari.

```
//Definir el onclick en el boton
<input type="button"
onclick="javascript:AlignetVPOS2.openModal('https://integracion.alignetsac.com/', '1')"
value="Comprar">
```

4.3 Parámetros de envío y respuesta

▪ Parámetros de envío

A continuación, se detalla la lista de parámetros que el comercio debe enviar en el proceso de solicitud de pago:

Campo	Tipo	Ancho máximo	Descripción	Mandatorio
acquirerId	Numérico	4	Código de adquirente proporcionado por la entidad afiliadora.	Si
idCommerce	Numérico	4	Código único de comercio proporcionado por la entidad afiliadora. Valor fijo.	Si
purchaseOperationNumber	Numérico	6	Identificador único por cada transacción, generado por el comercio. Considerar que deberán ser enviados los 6 caracteres obligatoriamente.	Si
purchaseAmount	Numérico	10	Valor total de la compra. (4)	Si
purchaseCurrencyCode	Numérico	3	Moneda según Estándar numérico ISO. Considerar las monedas habilitadas por la entidad afiliadora. Soles: 604 Dólares: 840	Si
language	Alfanumérico	2	Idioma usado: español (SP), inglés (EN). (Valor por defecto Español)	Si
billingFirstName	Alfanumérico	30	Nombre del tarjetahabiente. (como aparece en la tarjeta de crédito) (1).	No

Campo	Tipo	Ancho máximo	Descripción	Mandatorio
billingLastName	Alfanumérico	50	Apellido del tarjetahabiente (como aparece en la tarjeta de crédito) (1).	No
billingEMail	Alfanumérico	50	Dirección electrónica del tarjetahabiente. (1).	No
billingAddress	Alfanumérico	50	Dirección del tarjetahabiente. (1).	No
billingZIP	Alfanumérico	10	Código Postal del tarjetahabiente.	No
billingCity	Alfanumérico	50	Nombre de la ciudad del tarjetahabiente. (1).	No
billingState	Alfanumérico	2	Primeros 2 caracteres del Estado, Departamento o Localidad del tarjetahabiente.	No
billingCountry	Alfanumérico	2	Código ISO del país del tarjetahabiente. (1).	No
billingPhone	Alfanumérico	15	Teléfono del tarjetahabiente.	No
shippingFirstName	Alfanumérico	30	Nombre de la persona que recibirá los bienes.	Si
shippingLastName	Alfanumérico	50	Apellido de la persona que recibirá los bienes.	Si
shippingEmail	Alfanumérico	30	Email de la persona que recibirá los bienes.	Si
shippingAddress	Alfanumérico	50	Dirección de entrega del pedido del tarjetahabiente.	Si
shippingZIP	Alfanumérico	10	Código Postal de la entrega.	Si

Campo	Tipo	Ancho máximo	Descripción	Mandatorio
shippingCity	Alfanumérico	50	Nombre de la ciudad de entrega.	Si
shippingState	Alfanumérico	15	Nombre del estado/región o departamento de entrega.	Si
shippingCountry	Alfanumérico	2	Código ISO del país de entrega.	Si
shippingPhone	Alfanumérico	15	Teléfono del lugar de entrega.	No
shippingDNI	Alfanumérico	10	DNI de la persona que recibe los bienes.	No
HTTPSessionId	Alfanumérico	30	Sesión HTTP solo en el caso que el comercio lo requiera	No
terminalCode	Alfanumérico	12	Código de terminal de la compra	No
userCommerce	Alfanumérico	20	Código de usuario del tarjetahabiente en el comercio. En Wallet el parámetro es codCardHolderCommerce. (3).	Si
userCodePayme	Alfanumérico	30	Código de asociación con Wallet para el usuario. En Wallet el parámetro es codAsoCardHolderWallet. (3)	Si
descriptionProducts	Alfanumérico	30	Descripción del producto ó servicio comprado por el tarjetahabiente. (1)	Si
programmingLanguage	Alfanumérico	15	Estipula el lenguaje de programación utilizado por el Comercio. Ejemplo: JAVA, PHP, VB.NET, PYTHON, RUBY, etc.	Si
purchaseVerification	Alfanumérico	(Longitud no fija).	Firma digital de la trama se solicitud de pago.	Si

Campo	Tipo	Ancho máximo	Descripción	Mandatorio
reserved1 - reserved21	Alfanumérico	30	Campos para datos adicionales no contemplados en el V-POS2. (2)	No
reserved24 - reserved40	Alfanumérico	30	Campos para datos adicionales no contemplados en el V-POS2. (2)	No

- (1) Solo considerar letras, números o espacios, NO enviar caracteres especiales como letras con tilde y ñ.
- (2) Campos enviados por el comercio con información adicional. Estos serán devueltos con el mismo valor al momento de enviar la respuesta al comercio con el resultado del procesamiento de la transacción.
- (3) Campos requeridos para la integración con Wallet.
- (4) Valor que debe cumplir con las consideraciones del formato monto. Debe ir sin separador decimal (Si el monto es 100.30 dólares entonces la cantidad a enviar es 10030).

El campo purchaseVerification contiene el valor cifrado de los campos acquirerId, idCommerce, purchaseOperationNumber, purchaseAmount, purchaseCurrencyCode y la clave SHA-2 para la pasarela descargada del sistema V-Payment. (PASSWORD_COM_XXXX_PASARELA_XXXXXXXXXXXX.txt).

▪ **Parámetros de respuesta**

A continuación, se detalla la lista de parámetros que el comercio recibirá de la solicitud de pago:

Campo	Tipo	Ancho máximo	Descripción
authorizationResult	Numérico	2	<p>Este campo contiene el resultado de la autorización. Tiene tres posibles valores enviados por el V-POS: 00, indica que la transacción ha sido autorizada, 01, indica que la transacción ha sido denegada en el Banco Emisor, y 05, indica que la transacción ha sido rechazada por el V-POS.</p> <p>NOTA IMPORTANTE: El comercio mostrará los mensajes de resultado al tarjetahabiente según estos tres códigos. Por ejemplo: “Operación Autorizada”. “Operación Denegada”. “Operación Rechazada”</p>
authorizationCode	Alfanumérico	6	<p>En caso que la transacción haya sido autorizada por el Banco Emisor, este campo contendrá el código de autorización de la transacción.</p>
errorCode	Alfanumérico	4	<p>En caso que la transacción haya sido denegada o rechazada este campo contendrá el código de error respectivo que indicará el motivo del rechazo. La lista de códigos es dinámica y puede aumentar o disminuir según las mejoras que se realicen al V-POS y/o nuevas especificaciones de las marcas y procesadoras.</p> <p>NOTA IMPORTANTE: Este código de respuesta no debe ser mostrado al tarjetahabiente.</p>
errorMessage	Alfanumérico	-	<p>Este campo contendrá la descripción del código de error en caso de producirse un rechazo.</p> <p>NOTA IMPORTANTE: Este mensaje de error no debe ser mostrado al tarjetahabiente. El Adquirente puede acordar con el comercio para que se muestren grupos de mensajes.</p>
answerCode	Alfanumérico	-	<p>Código de respuesta de la procesadora con la cual se efectuó el pago.</p>
answerMessage	Alfanumérico	-	<p>Mensaje de respuesta que describe el valor del campo answerCode.</p>

Campo	Tipo	Ancho máximo	Descripción
bin	Alfanumérico	6	Este campo contiene los 6 primeros números de la tarjeta de pago, solamente es enviada en caso este valor se obtenga.
brand	Alfanumérico	12	Este campo contiene la descripción de la marca, puede darse los siguientes valores VISA, MC, AMEX o DN.
paymentReferenceCode	Alfanumérico	-	En caso la compra fue realizada con alguna marca de tarjeta, se devolverá el número de tarjeta enmascarada (ejemplo: 414243*****1234). Para otros medios, se devolverá el código respectivo.
purchaseVerification	Alfanumérico	(Longitud no fija).	Firma generada utilizando el algoritmo de cifrado SHA-2 en base a los siguientes parámetros: acquirerId, idCommerce, purchaseOperationNumber, purchaseAmount, purchaseCurrencyCode, authorizationResult y la clave SHA-2 para la pasarela descargada del sistema V-Payment. (PASSWORD_COM_XXXX_PASARELA_XXXXXXXXXX XX.txt) El mismo será utilizado para la validación de los datos en el proceso de respuesta.
reserved1 - reserved21	Alfanumérico	30	Campos para datos adicionales no revisados por el V-POS2.
reserved22	Alfanumérico	30	Este campo retorna el tipo de tarjeta: DEBIT o CREDIT.
reserved23	Alfanumérico	30	Este campo retorna el nombre del Banco Emisor de la Tarjeta utilizada en la transacción.
reserved24 - reserved40	Alfanumérico	30	Campos para datos adicionales no revisados por el V-POS2.

4.4 Ejemplo envió y recepción de parámetros

- Ejemplo de envío de parámetros

A continuación, se mostrará un ejemplo técnico de la conexión a V-POS2 utilizando PHP:

```
//Se definen todos los parametros obligatorios.
```

```
$acquirerId = '144';
```

```
$idCommerce = '7886';
```

```
$purchaseOperationNumber = '123456';
```

```
$purchaseAmount = '10000';
```

```
$purchaseCurrencyCode = '604';
```

La clave SHA-2 será ingresada de forma escrita en el mismo código:

```
//Clave SHA-2.
```

```
$claveSHA2 = 'cuhceSEkyTVvnbqHSc895627234825';
```

Para poder generar la firma cifrada utilizando los parámetros de envío a V-POS2 y la clave SHA-2, hay que invocar la función `openssl_digest`. Lo anterior generará la firma cifrada que será enviada a V-POS2 en el parámetro `purchaseVerification`.

```
$purchaseVerification =
```

```
openssl_digest($acquirerId . $idCommerce . $purchaseOperationNumber . $purchaseAmount .
```

```
$purchaseCurrencyCode . $claveSecreta, 'sha512');
```

Finalmente se muestra un ejemplo completo del formulario de envío a VPOS2, enviando los parámetros correspondientes:

```
<head> <script type="text/javascript"
src="https://integracion.alignetsac.com/VPOS2/js/modalcomercio.js" >
</script> </head>
<form name="f1" id="f1" action="#" method="post" class="alignet-form-vpos2">
  <input type="hidden" name="acquirerId" value="<?php echo $acquirerId; ?>" />
  <input type="hidden" name="idCommerce" value="<?php echo $idCommerce; ?>" />
  <input type="hidden" name="purchaseOperationNumber" value="<?php echo
  $purchaseOperationNumber; ?>" />
  <input type="hidden" name="purchaseAmount" value="<?php echo $purchaseAmount; ?>" />
  <input type="hidden" name="purchaseCurrencyCode" value="<?php echo $purchaseCurrencyCode;
  ?>" />
  <input type="hidden" name="language" value="SP" />
  <input type="hidden" name="shippingFirstName" value="Juan" />
  <input type="hidden" name="shippingLastName" value="Perez" />
  <input type="hidden" name="shippingEmail" value="test@test.com" />
  <input type="hidden" name="shippingAddress" value="Direccion ABC" />
  <input type="hidden" name="shippingZIP" value="ZIP 123" />
  <input type="hidden" name="shippingCity" value="City ABC" />
  <input type="hidden" name="shippingState" value="State ABC" />
  <input type="hidden" name="shippingCountry" value="PE" />
  <!--Parametro que contiene el valor del codCardHolderCommerce.-->
  <input type="hidden" name="userCommerce" value="modal123" />
  <!--Parametro que contiene el valor del codAsoCardHolderWallet.-->
  <input type="hidden" name="userCodePayme" value="1--510--1010" />
  <input type="hidden" name="descriptionProducts" value="Producto ABC" />
  <input type="hidden" name="programmingLanguage" value="PHP" />
  <!--Ejemplo envío campos reservados en parametro reserved1.-->
  <input type="hidden" name="reserved1" value="Valor Reservado ABC" />
  <input type="hidden" name="purchaseVerification" value="<?php echo $purchaseVerification; ?>"
  <input type="button"
onclick="javascript:AlignetVPOS2.openModal('https://integracion.alignetsac.com/')" value="Comprar">
</form>
```

▪ **Ejemplo de recepción de parámetros**

Para recibir la respuesta de pago de Pay-me a través del componente V-POS2 es necesario que el comercio implemente una página o componente dinámico en donde se extraigan los valores de los parámetros obtenidos de la transacción. Además de estos campos, la respuesta de pago, contendrá todos los campos enviados al V-POS2 que se ingresaron en la solicitud de pago y que podrán ser recuperados en la respuesta. A continuación, se muestra un ejemplo de una página de respuesta:

Página de Respuesta

<https://www.paginacomercio.com/paginarespuesta.php>

Con el fin de validar que los datos en el proceso de respuesta no hayan sido alterados, se ha implementado una validación usando el valor del purchaseVerification devuelto por Pay-me y el purchaseVerification creado por el comercio.

Si alguno de los datos fue alterado, se mostrará el mensaje: **“Transacción Invalida. Los datos fueron alterados en el proceso de respuesta.”**

A continuación, se muestra un ejemplo de código implementado en PHP para la recepción e interpretación de los datos:

```
<?php
//Misma clave que se usa para el envio a VPOS2
$claveSecreta = 'LbABXJkbcaFRLJchXCbPO79658268743';

//purchaseVerication que devuelve la Pasarela de Pagos
$purchaseVericationVPOS2 = $_POST['purchaseVerification'];
//purchaseVerication que genera el comercio
$purchaseVericationComercio = openssl_digest($_POST['acquirerId'] . $_POST['idCommerce'] .
$_POST['purchaseOperationNumber'] . $_POST['purchaseAmount'] . $_POST['purchaseCurrencyCode'] .
$_POST['authorizationResult'] . $claveSecreta, 'sha512');

//Si ambos datos son iguales
if ($purchaseVericationVPOS2 == $purchaseVericationComercio || $purchaseVericationVPOS2 == "") {
?>
<table>
    <tr><td>AuthorizationResult</td><td><?php echo $_POST['authorizationResult'];?></td></tr>
    <tr><td>AuthorizationCode</td><td><?php echo $_POST['authorizationCode'];?></td></tr>
    <tr><td>ErrorCode</td><td><?php echo $_POST['errorCode'];?></td></tr>
    <tr><td>ErroMessage</td><td><?php echo $_POST['errorMessage'];?></td></tr>
    <tr><td>Bin</td><td><?php echo $_POST['bin'];?></td></tr>
```

```
<tr><td>Brand</td><td><?php echo $_POST['brand'];?></td></tr>
<tr><td>PaymentReferenceCode</td><td><?php echo
$_POST['paymentReferenceCode'];?></td></tr>

<!--Ejemplo recepción de campos reservados en parametro reserved1-->
<tr><td>Reserved1</td><td><?php echo $_POST['reserved1'];?></td></tr>
<tr><td>Reserved22</td><td><?php echo $_POST['reserved22'];?></td></tr>
<tr><td>Reserved23</td><td><?php echo $_POST['reserved23'];?></td></tr>
<tr><td>Número de Operacion</td><td><?php echo
$_POST['purchaseOperationNumber'];?></td></tr>
<tr><td>Monto</td><td><?php echo "S/. " . $_POST['purchaseAmount']/100;?></td></tr>
</table>
<?php
//Si ambos datos son diferentes
} else {
echo "<h1>Transacción Invalida. Los datos fueron alterados en el proceso de respuesta.</h1>";
}
?>
```

4.5 Personalización del Formulario de Pagos

El registro del logo y los cambios de los colores es realizado por el equipo de integraciones de Pay-me. Para ello el comercio, siguiendo las consideraciones detalladas en la guía funcional, deberá entregar los siguientes puntos:

Parámetro	Valor
Logo	(A completar por el comercio)
Cabecera - Color de Fondo	(A completar por el comercio)
Selector - Color de Fondo	(A completar por el comercio)
Botón Pagar - Color de selección	(A completar por el comercio)
Botón Pagar - Color de Fondo	(A completar por el comercio)
Enlace Retornar - Color	(A completar por el comercio)

Tener en cuenta que el logo deberá tener formato PNG y el valor de colores deberá ser entregado en formato hexadecimal.

5. Proceso de Envío y Recepción de Parámetros para Otros Medios de Pago

Para que un comercio pueda contar con estos medios de pago alternativos, es necesario que se realice lo siguiente:

- Solicitar la habilitación de la marca alternativa de pago.
- Brindar la url de la página de respuesta para pagos alternativos.
- Brindar el tiempo de expiración de la orden o ticket de pago a generar.

Cabe mencionar que a través del tiempo de expiración de la orden se definirá el tiempo en que se podrá efectuar el pago de la misma. Una vez expirada dicha orden, se deberá volver a ingresar a la pasarela y generar una nueva. Es necesario que el comercio defina e indique el tiempo de expiración de la orden de pago (en minutos) al área de integraciones. Para el caso de SafetyPay, por defecto es de 2 horas y como máximo podrá ampliarse hasta 7 días.

▪ Parámetros de envío

A continuación, se detalla la lista de parámetros que el comercio debe enviar si desea habilitar la funcionalidad de Preselección de Otros Medios de Pagos:

Campo	Tipo	Ancho máximo	Descripción
payBrandRedirect	Numérico	2	Este campo permite especificar qué se ejecute el redirect hacia la pantalla de SafetyPay o PagoEfectivo. Puede tener los siguientes valores: 1: Realizar el redirect ya sea SafetyPay o Pago Efectivo. 0: No realiza redirect.
selectedPayType	Alfanumérico	10	Campo opcional para acceder por defecto a Otros Medios de Pago. Se debe enviar el siguiente valor: OTHER: Otros Medios de Pago
selectedPayBrand	Alfanumérico	10	Este campo permite especificar qué medio de pago alternativo específico. Puede tener los siguientes valores: PAEF: Pago Efectivo SFPY: SafetyPay
selectedPayBrandLevel1	Numérico	2	Este campo permite acceder por defecto a la opción que pueda tener el medio de pago alternativo. En este caso podrá tener los valores: 1: Banca por Internet. 2: Pago en Efectivo.

Adicionalmente, cabe mencionar que, para el uso de las marcas alternativas de pago, Payme realizará dos envíos de respuesta al comercio. La primera es al generar la orden de pago y la segunda es al momento de realizar el pago de la orden, ya sea a través del homebanking o físicamente en alguna entidad bancaria. Esto ocurre con el fin de informar al comercio la actualización del estado de la orden.

▪ **Parámetros de respuesta**

A continuación, se detalla la lista de parámetros que el comercio recibirá al hacer un pago con un medio de pago alternativo:

Campo	Tipo	Ancho máximo	Descripción
numeroCip	Alfanumérico	40	Parámetro de retorno exclusivo del medio de pago Pago Efectivo. Contiene el código de la orden que utilizara el usuario para realizar el pago en la entidad financiera correspondiente.
authorizationResult	Numérico	2	Indica el estado de la orden de pago, según se muestra a continuación: 03: Pendiente de Pago 00: Autorizado
brand	Alfanumérico	20	Este campo retorna el medio de pago alternativo utilizado en la transacción. Puede devolver los siguientes valores: SAFETYPAY PAGO EFECTIVO

6. Anexo 1: Set de pruebas para la certificación en el ambiente de Integración.

El propósito de los siguientes casos de pruebas es comprobar que el comercio envíe correctamente los datos de compra a Pay-me y asegurar la correcta recepción de los resultados del procesamiento de una transacción en el ambiente de Integración. Los siguientes valores deberán ser confirmados por el comercio luego de ser ejecutado el caso de prueba:

- ✓ purchaseOperationNumber
- ✓ purchaseAmount
- ✓ authorizationResult
- ✓ errorCode
- ✓ errorMessage

a. Caso de Prueba 1

Descripción: Enviar una transacción a Pay-me, luego hacer clic en el botón Retornar al Comercio. Conectarse previamente a Wallet, generar un código de asociación y enviar los datos userCommerce y userCodePayme a V-POS2.

Valores Esperados	
authorizationResult	05
errorCode	2300
errorMessage	User Cancelled in PASS 1

b. Caso de Prueba 2

Descripción: Enviar una transacción a Pay-me (incluyendo los datos de Wallet userCommerce y userCodePayme previamente generados), ingresar los datos de la tarjeta Visa 485951*****0036, dar clic en el botón Pagar, ingresar la contraseña Verified by Visa y dar clic en Continuar. Registrar la tarjeta en Wallet activando el checkbox “Registrar mi tarjeta en Pay-me”.

Valores Esperados	
authorizationResult	00
errorCode	00
errorMessage	Successful approval/completion
purchaseVerification	(Devuelto por Pay-me)
purchaseVerification	(Creado por el comercio)

c. **Caso de Prueba 3**

Descripción: Enviar una transacción a Pay-me, ingresar los datos de la tarjeta Visa 485951*****0051, dar clic en el botón Pagar.

Valores Esperados	
authorizationResult	00
errorCode	00
errorMessage	Successful approval/completion

d. **Caso de Prueba 4**

Descripción: Enviar una transacción a Pay-me, seleccionar la tarjeta Visa 485951*****0036 registrada, dar clic en el botón Pagar, y al solicitarse la contraseña Verified by Visa dar clic en Cancelar.

Valores Esperados	
authorizationResult	05
errorCode	2401
errorMessage	Pre Authentication rules not approved

e. **Caso de Prueba 5**

Descripción: Enviar una transacción con un monto mayor a 1000.00. Ingresar los datos de la tarjeta Visa 485951*****0036.

Valores Esperados	
authorizationResult	00
errorCode	00
errorMessage	Successful approval/completion

f. **Caso de Prueba 6**

Descripción: Enviar una transacción con un monto menor a uno. Por ejemplo, envíe 75 para que llegue 0.75. Ingresar los datos de la tarjeta Visa 485951*****0051.

Valores Esperados	
authorizationResult	00
errorCode	00
errorMessage	Successful approval/completion

g. Caso de Prueba 7

Descripción: Enviar una transacción a Pay-me, ingresar los datos de la tarjeta Visa 411111*****1111, dar clic en el botón Pagar.

Valores Esperados	
authorizationResult	01
errorCode	05
errorMessage	Do not honor

7. Anexo 2: Set de pruebas para la certificación en el ambiente de Producción.

El propósito de los siguientes casos de pruebas es comprobar que el comercio envíe correctamente los datos de compra al V-POS2 y asegurar la correcta recepción de los resultados del procesamiento de una transacción en el ambiente de Producción. Los siguientes valores deberán ser confirmados por el comercio luego de ser ejecutado el caso de prueba:

- ✓ purchaseOperationNumber
- ✓ purchaseAmount
- ✓ authorizationResult
- ✓ errorCode
- ✓ errorMessage

a. Caso de Prueba 1

Descripción: Enviar una transacción a Pay-me, luego hacer clic en el botón Regresar al Comercio.

Valores Esperados	
authorizationResult	05
errorCode	2300
errorMessage	User Cancelled in PASS 1

b. Caso de Prueba 2

Descripción: Enviar una transacción a Pay-me (incluyendo los datos de Wallet userCommerce y userCodePayme previamente generados), ingresar los datos de la tarjeta Visa 411111*****1111, dar clic en el botón Pagar.

Valores Esperados	
authorizationResult	01
errorCode	05
errorMessage	No such issuer

c. **Caso de Prueba 3**

Descripción: Enviar una transacción con cualquier monto (incluyendo los datos de Wallet userCommerce y userCodePayme previamente generados). Ingresar los datos de la tarjeta MasterCard 503849*****0032, dar clic en el botón Pagar.

Valores Esperados	
authorizationResult	01
errorCode	14
errorMessage	Invalid account number (no such number)

d. **Caso de Prueba 4**

Descripción: Enviar una transacción con cualquier monto (incluyendo los datos de Wallet userCommerce y userCodePayme previamente generados). Ingresar los datos de la tarjeta Amex 376*****006, dar clic en el botón Pagar.

Valores Esperados	
authorizationResult	01
errorCode	-
errorMessage	Punto-Web Secure Code Mensaje

e. **Caso de Prueba 5**

Descripción: Enviar una transacción con cualquier monto (incluyendo los datos de Wallet userCommerce y userCodePayme previamente generados). Ingresar los datos de la tarjeta Diners 362*****379, dar clic en el botón Pagar.

Valores Esperados	
authorizationResult	01
errorCode	05
errorMessage	Do not honor

8. Anexo 3: Tarjetas de pruebas para ambiente de Integración y Producción.

Número de tarjeta VISA	Fecha de Expiración	Código de Seguridad	Contraseña Verified By Visa	Integración	Producción	Tipo
4859510000000036	Dic-20	648	360036	X		Autorizada
4859510000000051	Dic-20	365	Tarjeta no enrolada	X		Autorizada
4111111111111111	Dic-20	648	Tarjeta no enrolada		X	Denegada

Número de tarjeta MASTERCARD	Fecha de Expiración	Código de Seguridad	Contraseña Secure Code	Integración	Producción	Tipo
5038490000000032	Dic-20	517	Tarjeta no enrolada		X	Denegada
5549110920049586	Feb-20	608	Tarjeta no enrolada	X		Autorizada

Número de tarjeta AMEX	Fecha de Expiración	Código de Seguridad	Contraseña SafeKey	Integración	Producción	Tipo
376000000000006	Dic-17	2523	Tarjeta no enrolada		X	Denegada

Número de tarjeta DINERS	Fecha de Expiración	Código de Seguridad	Contraseña	Integración	Producción	Tipo
36236831437379	Oct-18	123	Tarjeta no enrolada		X	Denegada

9. Anexo 4: Consideraciones para el ambiente de Integración

- **Disponibilidad del Ambiente de Pruebas**

El ambiente de pruebas se encuentra disponible las 24 horas del día, de lunes a domingo. El soporte sobre consultas y/o inconvenientes se realiza entre las 09:00am hasta las 06:00pm, solo en días laborables.

- **Análisis de resultados de pruebas**

Los resultados de las pruebas deben ser enviados por correo a los integradores responsables.

- **Consideraciones**

Tener en cuenta que todas las horas indicadas en el presente documento, así como, las indicadas durante la etapa de integración se encuentran en base a la hora Perú (Zona horaria GMT -5)