

**NORMA TÉCNICA - ESTÁNDAR
PARA LA COMUNICACIÓN
CON ADQUIRENTES**

SINPE-TP

SERIE DE NORMAS Y PROCEDIMIENTOS

Público



NT-STP

**NORMA TÉCNICA - ESTÁNDAR
PARA LA COMUNICACIÓN CON
ADQUIRENTES**

SINPE-TP

SERIE DE NORMAS Y PROCEDIMIENTOS

Público



NT-STP

Tabla de contenido

1	Introducción	1
2	Alcance	1
3	Términos empleados	1
4	Documentos aplicables	2
5	Consideraciones generales	2
5.1	Protocolo de comunicación	2
5.2	Aspectos de seguridad	3
5.2.1	Intercambio de llaves	3
5.2.2	Confidencialidad	4
5.2.3	Autenticación	4
6	Servicios de procesamiento	4
6.1	Tramas para el servicio de autorización	4
6.1.1	Estructura de la trama del SCR	5
6.1.2	Estructura de la trama del adquirente	9
6.2	Tramas para el servicio de recuperación de deuda	10
6.2.1	Estructura de la trama del SCR	11
6.2.2	Estructura de la trama del adquirente	13
6.3	Tramas para el servicio de liquidación	13
6.3.1	Estructura de la trama del SCR	13
6.3.2	Estructura de la trama del adquirente	17
6.4	Tramas para el servicio de verificación del código de seguridad	17
6.4.1	Estructura de la trama del SCR	17
6.4.2	Estructura de la trama del adquirente	18
7	Anexos:	19
7.1	Archivos relacionados con la autorización en formato JSON	19
7.1.1	Solicitud de autorización con el adquirente	19
7.1.2	Respuesta de solicitud de autorización del adquirente	20
7.1.3	Solicitud de anulación de transacción	21
7.1.4	Solicitud de reversión de transacción	22
7.1.5	Respuesta de anulaciones o reversiones del adquirente	23
7.2	Archivos relacionados con la liquidación en formato JSON	24
7.2.1	Trama de información para el archivo de liquidación con el adquirente	24
7.2.2	Respuesta de solicitud de liquidación del adquirente	27
7.3	Archivos relacionados con la verificación del código de seguridad	28
7.3.1	Solicitud de verificación del código de seguridad	28
7.3.2	Respuesta de verificación del código de seguridad	29

Sistema Nacional de Pagos Electrónicos

División Sistemas de Pago - BCCR

Año 2021

1 Introducción

El presente documento forma parte de la Serie de Normas y Procedimientos del SINPE y describe los servicios que utilizan los adquirentes para establecer y mantener la comunicación con el Sistema Central de Recaudo (SCR), así como la estructura y contenido de las tramas de información con las cuales se realiza el intercambio electrónico de datos en el Sistema Nacional de Pago Electrónico en el Transporte Público (SINPE-TP).

Dentro de los servicios que se requieren del adquirente, se encuentra el procesamiento de cobro de los viajes realizados por los pasajeros con el uso de los dispositivos de pago admitidos en SINPE-TP. Para estos propósitos, el adquirente debe realizar el procesamiento de solicitudes de autorización, recuperación de deuda, liquidación y reembolso.

Para cada tipo de solicitud de procesamiento se define un protocolo de datos que permite llevar a cabo el intercambio de información en un ambiente tecnológico estándar, seguro y automatizado, con las reglas de procesamiento establecidas por las principales marcas de tarjetas que operan en el país (VISA, MasterCard y American Express), las cuales especifican la forma en que debe autorizarse y liquidarse una transacción *EMV-Contactless* del transporte.

2 Alcance

La presente norma técnica define el estándar electrónico para llevar a cabo la comunicación entre SINPE-TP y los adquirentes. Sus disposiciones, requisitos y estándares son de acatamiento obligatorio para los adquirentes que provean servicios a dicho sistema.

3 Términos empleados

- **API:** siglas de “*Application Programming Interface*” (Interfaz de programación de aplicaciones); es un conjunto de funciones, reglas (códigos), procedimientos y especificaciones, que ofrecen una biblioteca de programación (como capa de abstracción) para que sea utilizada por otro programa informático con el fin de comunicarse entre ellos.
- **HTTPS:** siglas de “*Hyper Text Transfer Protocol Secure*” (Protocolo seguro de transferencia de hipertexto).
- **JSON:** acrónimo de “*JavaScript Object Notation*” (Notación de objeto de JavaScript); es un formato de texto para el intercambio de datos en aplicaciones web.
- **Marca:** acción de aproximar un dispositivo de pago al validador instalado en una unidad de transporte, para validar el dispositivo de pago y generar la trama de información que se envía al SINPE-TP para su procesamiento. En los documentos en idioma inglés a este término se le denomina “TAP” (*Transit Access Pass*).
- **PAN:** siglas de “*Primary Account Number*” (Número de cuenta primario); es un número único que identifica a un dispositivo de pago.
- **Periodo de viaje:** determina el tiempo máximo en el que un cliente puede acumular transacciones del transporte, previo a enviar una tarjeta a liquidar. Usualmente es un día calendario.

- **RESTful**: también conocido como “API REST”; es un estándar de comunicación entre sistemas que usa el protocolo HTTP para obtener datos o generar operaciones sobre esos datos en distintos formatos, como XML y JSON.
- **Sistema Central de Recaudo (SCR)**: componente de SINPE-TP que aplica las reglas de transporte en el procesamiento de pagos. Dentro del SCR se concibe integrada la pasarela de transporte, como componente encargado de aplicar las reglas de pagos agregados.
- **TLS**: siglas de “*Transport Layer Security*” (Seguridad en la capa de transporte); es un protocolo criptográfico que proporciona comunicaciones seguras por una red, comúnmente Internet.

4 Documentos aplicables

Siglas	Nombre del documento
RSP	Reglamento del Sistema de Pagos
NC-STP	Norma Complementaria SINPE-TP

5 Consideraciones generales

5.1 Protocolo de comunicación

Las comunicaciones entre los adquirentes y el SCR para el intercambio de datos se realizan con el uso de los protocolos: HTTPS, mediante el estándar RESTful para el intercambio de peticiones.

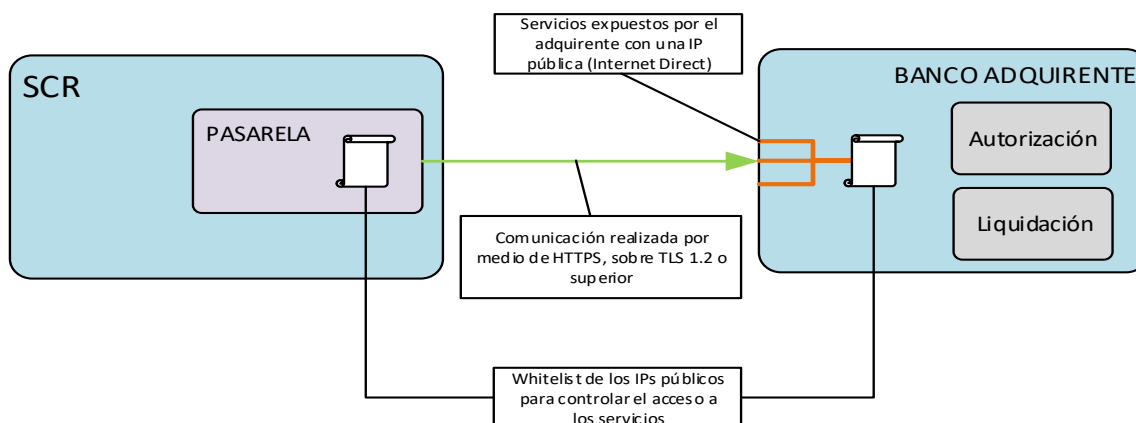


Figura 1. Protocolos de comunicación y aseguramiento entre adquirentes y el SCR.

Para ello se utiliza una conexión host-to-host entre el adquirente y el SCR (pasarela de transporte). El adquirente debe exponer sus servicios con IPs públicas, de manera que la comunicación se realiza con una conexión directa a Internet (Internet Direct). Para consumir los servicios expuestos, las partes deben intercambiar sus IPs públicas, así como los puertos de acceso, de manera que la parte que exponga sus servicios pueda agregar las IPs a sus listas de acceso (whitelist) y permitir el consumo de esos servicios por la otra parte.

Cada uno de los servicios requeridos del adquirente cuenta con una trama de información particular para el intercambio de datos, tanto para el envío de datos realizado por el SCR, como para la respuesta que debe generar el adquirente, especificados en la sección 6.

Esta configuración en la comunicación se utiliza en el ambiente de producción y en los ambientes de desarrollo y de pruebas.

5.2 Aspectos de seguridad

Antes de enviar transacciones, los canales de comunicación deben estar aprovisionados para manejar de forma segura los datos EMV y realizar la criptografía correspondiente. Para ello se utiliza el algoritmo de cifrado AES con una llave de 256 bits como método de cifrado de los datos sensibles (PrimaryAccountNumber, Track2 e iccCommTags), previo a ser enviados a los adquirentes.

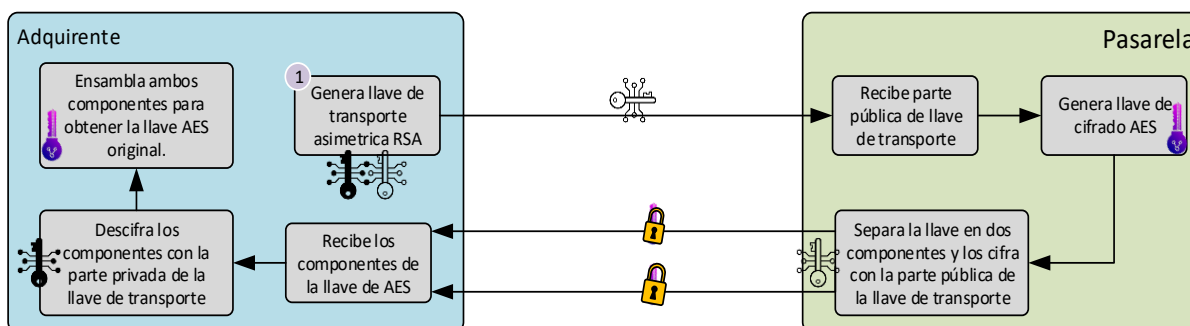
Adicionalmente, el algoritmo AES requiere de un vector de inicialización (IV) para ejecutarse. Este vector es generado de forma dinámica para cada encriptación realizada por la pasarela, por lo que cuando se aplica el algoritmo para la cifra de un bloque de datos, se genera un vector de inicialización único para esa ejecución. El vector es generado por la pasarela y se envía concatenado con el texto cifrado en la forma “vector de inicialización” + “text cifrado”¹, de manera que el adquirente pueda recuperarlo y utilizarlo para el descifrado de los datos.

En el caso en el que un bloque de datos no cumpla con los bytes requeridos como insumo para el algoritmo de cifrado, con el relleno (*padding*) de este bloque de datos se utiliza el estándar PKCS#7.

El formato de los campos cifrados dentro de las tramas de información debe ser en código hexadecimal.

5.2.1 Intercambio de llaves

Como parte de la seguridad requerida para proteger los datos recuperados de la tarjeta, el adquirente debe recibir de parte de la pasarela la llave AES utilizada en la iteración con SINPE-TP, la cual es utilizada como entrada en el algoritmo para cifrar los campos PrimaryAccountNumber, Track2 e iccCommTags en los que viaja la información sensible de la tarjeta.



Para el proceso de intercambio de llaves, el adquirente debe generar primero una llave de transporte asimétrica RSA; la parte pública de esta llave es enviada por correo electrónico a la pasarela. Por su parte, la pasarela genera la llave de cifrado AES para cada adquirente.

¹ Como ejemplo: si se tienen los siguientes datos:

- Texto original en ASCII: 4111111111111111
- Llave de cifrado: 424143435245444F4D415449435452414E53505542424343524B455954455354
- Vector de inicialización: 4261636c6333736a64387a7074396378

Se obtendría como resultado el texto cifrado que se especifica en seguida:

- d6f0f869f0a6f99dedc7c3e179d92160d0bd917977c8bc4c14e70e99b7572951

La pasarela enviaría al adquirente el vector de inicialización y el texto cifrado concatenados de la siguiente manera:

- 4261636c6333736a64387a7074396378d6f0f869f0a6f99dedc7c3e179d92160d0bd917977c8bc4c14e70e99b7572951

La llave de cifrado se parte en dos componentes, y cada componente es cifrado utilizando la llave pública recibida del adquirente. Estos componentes cifrados se envían por medio de dos canales diferentes, a definir con cada adquirente.

Una vez recibidos los componentes, el adquirente los descifra con la parte privada de la llave de transporte, y luego vuelven a ensamblar las partes dentro de su HSM o parte segura de su plataforma, para así obtener la llave de cifrado AES original. Con esta llave el adquirente procede a cifrar los mensajes.

5.2.2 Confidencialidad

Como parte de la seguridad en la transferencia de datos, se utiliza el protocolo seguro HTTPS con el protocolo criptográfico TLS 1.2 o superior, el cual proporciona comunicaciones seguras por una red (en este caso específico, internet).

5.2.3 Autenticación

La autenticación se realiza mediante el uso de tokens, implementando el estándar de autorización o framework llamado OAuth 2.0, el cual es utilizada para tener acceso a servicios HTTPS de terceros (en este caso los bancos adquirentes).

Para lograr lo anterior, los adquirentes generan un token de acceso para la pasarela, el cual debe ser incluido en el encabezado del protocolo HTTPS, con la etiqueta "Authorization" para cada uno de los mensajes enviados. De esta manera, el adquirente puede validar el token garantizando que, efectivamente, fue emitido por él para el consumo del servicio.

Para consumir el token el adquirente debe habilitar un API adicional, utilizando los mismos protocolos de comunicación descritos en esta sección, al cual la pasarela pueda realizar una petición para recibir un token de acceso. El consumo de este API será acordado entre las partes (adquirente y pasarela) de manera segura.

6 Servicios de procesamiento

6.1 Tramas para el servicio de autorización

Dentro del contexto de SINPE-TP se realizan dos tipos de autorizaciones: autorizaciones iniciales y autorizaciones para la confirmación de fondos, así como transacciones de actualización de ATC, las cuales llevan el mismo formato.

- **Autorizaciones iniciales:** tienen como objetivo verificar que la cuenta de los tarjetahabientes sea válida y por lo general se realizan por montos de bajo valor (1 colón), o por un monto cero; ello dependiendo de la marca de la tarjeta.

El adquirente debe procesar la autorización inicial conforme con lo definido en las reglas de las marcas de tarjetas, siendo una verificación de cuenta por un monto cero para VISA y una autorización por un valor nominal de un colón (1 CRC) para tarjetas MasterCard y American Express.

El servicio para autorizaciones iniciales puede ser invocado en dos escenarios:

1. Cuando la tarjeta es utilizada por primera vez durante el periodo de viaje (considerada como "tarjeta nueva" en el ambiente del sistema), el servicio envía una solicitud de autorización inicial que, de resultar exitosa, permite considerarla como "tarjeta conocida" en SINPE-TP.

2. Cuando la tarjeta es retirada de lista de denegación, luego de haberse sometido a un proceso de recuperación de deuda.
- **Autorizaciones para la confirmación de fondos:** tienen como objetivo verificar la suficiencia de fondos para cubrir el monto acumulado durante el presente periodo de viaje y garantizar su pago a la entidad solicitante.

El servicio para autorizaciones puede ser invocado en dos escenarios:

3. Cuando el monto acumulado del día para un dispositivo de pago supere el límite de responsabilidad del emisor: en este caso, el servicio debe enviar una solicitud de autorización al adquirente por el monto acumulado del dispositivo de pago como parte del modelo de riesgos del sistema.
4. Cuando se acabe el periodo de viaje (al final del día), el sistema debe enviar una solicitud de autorización al adquirente por el monto acumulado de cada dispositivo de pago con el que se haya registrado uno o más viajes.
- **Solicitud de actualización de ATC²:** tiene como fin informar al emisor del número actual del ATC que tiene una tarjeta luego de una serie de taps fuera de línea. Este tipo de actualización debe contemplar tres puntos claves:
 - a. El DE 4 (Monto) debe llevar monto 0.
 - b. El DE 55 (Criptograma) debe contener los datos del último “tap” realizado por el tarjetahabiente.
 - c. El DE 61s7 (POS transaction status) debe llevar el valor 6 (ATC update).

El adquirente debe proveer un servicio que cumpla con el estándar RESTful, mediante el cual pueda recibir solicitudes POST en el protocolo HTTPS. Para la invocación del servicio de autorización inicial el adquirente debe proporcionar la siguiente ruta de acceso:

- [https://<host del adquirente>\[:puerto\]/verificacion](https://<host del adquirente>[:puerto]/verificacion)

El servicio de autorización y actualización de ATC es habilitado por el adquirente en la siguiente ruta:

- [https://<host del adquirente>\[:puerto\]/autorizacion](https://<host del adquirente>[:puerto]/autorizacion)

6.1.1 Estructura de la trama del SCR

Estas solicitudes son recibidas en formato JSON, con la trama de información que se especifica en la tabla 1 y la respuesta de la solicitud especificada en la tabla 5.

Tabla 1

Trama de información para las solicitudes de autorización del SCR.

Campo	Data Element	Descripción	Formato	Mandatorio
totalAmount	DE04	Monto total de la transacción. Es el equivalente al campo Amount, transaction del estándar ISO 8583.	Numérico de 10 dígitos, 2 decimales.	Si

² Debido al modelo de liquidación a implementarse para SINPE-TP (Libro XV, Capítulo VI, del Reglamento del Sistema de Pagos), las transacciones para la actualización de ATC no son necesarias para su ejecución. Como tal, este mensaje no será necesario implementarse en la primera versión e integración del sistema. Las mismas se mantienen en el documento como referencia para futuras implementaciones.

Campo	Data Element	Descripción	Formato	Mandatorio
SystemTraceNumber	DE11	Campo generado automáticamente por la terminal y se incrementa por cada transacción realizada. Se requiere en el mensaje de respuesta del host para validar la solicitud enviada.	Alfanumérico de 6 caracteres.	Si
DateTimeLocalTrans	DE12 y DE13	Fecha y hora local del momento en que se realizó la transacción en el validador.	Etiqueta de tiempo de 10 dígitos.	Si
MCC	DE18	Tipo de comercio. Los valores válidos son: 4111: Transporte de pasajeros de cercanías locales y suburbanos, incluidos ferries. 4112: Ferrocarriles de pasajeros. 4131: Líneas de autobús.	Número entero de 4 dígitos.	Si
entryMode	DE22	Indica la forma en que fue leída la información de la tarjeta. Manual, MagStripe, Contact Less, Chip; y las capacidades del lector. Ver tabla 4 para el detalle del campo entryMode y sus posibles valores.	Texto de 3 dígitos. Ver tabla 4 para posibles valores.	Si
CardSequenceNumber	DE23	Número de secuencia de la tarjeta e identifica las tarjetas con un mismo PAN. Es mandatorio si la terminal envía el dato, de otra manera no será incluido.	Número entero de 3 dígitos.	Si
track2	DE35	Información cifrada de la lectura del track de la tarjeta.	Información cifrada.	Si
terminalId	DE41	Identificador único de la terminal.	Alfanumérico de hasta 36 caracteres.	Si
MerchantID	DE42	Identifica de forma exclusiva a un comerciante determinado.	Alfanumérico.	Si
TransactionTypeIdentifier	DE48	El tipo de autorización que debe ser enviado. Este corresponde al DE 48, subelemento 64, subcampo 1.	Número de 2 dígitos.	Si
TransportationMode	DE48	Identifica el tipo transporte en el que se realizó el tap (bus, tren, etc.). Este corresponde al DE 48, subelemento 64, subcampo 2.	Número de 2 dígitos.	Si
Currency	DE49	Moneda.	Según el ISO 4217 en formato numérico.	Si
iccCommTags	DE55	Contiene los datos relacionados con EMV en formato TLV (Tag, Length, Value). Es el equivalente al campo ICC Related Data del estándar ISO 8583. Ver tabla 2 para el detalle de los tags.	Información cifrada.	Si

Campo	Data Element	Descripción	Formato	Mandatorio
PrivateUse	DE63	Campo de uso particular del adquirente.	Archivo tipo JSON.	Si
TerminalCountryCode	N/A	Código de país de la institución adquirente.	Texto de hasta 3 caracteres.	Si
serviceCode	N/A	Código de servicio definido en ISO para el track 1 y track 2.	Alfanumérico de hasta 4 caracteres.	Si
applicationLabel	N/A	Identificador asociado al AID, utilizado en la transacción.	Alfanumérico de hasta 50 caracteres.	Si
transactionType	N/A	Tipo de transacción. Ver tabla 3 para el detalle del campo transactionType y sus posibles valores.	Texto de hasta 3 caracteres.	Si
retrievalReferenceNumber	N/A	Número de referencia de la transacción. Utilizado en este únicamente endpoint al solicitar una Anulación, con el transactionType VOID.	Alfanumérico de hasta 12 caracteres.	Condicional
authorizationNumber	N/A	Número de autorización. Utilizado en este endpoint únicamente al solicitar una Anulación, con el transactionType VOID.	Alfanumérico de hasta 36 caracteres.	Condicional
systemTraceNumber	N/A	Número de seguimiento del sistema. Utilizado en este endpoint únicamente al solicitar una Reversa, con el transactionType REVERSE.	Alfanumérico de 6 caracteres.	Condicional

Tabla 2
Especificación del campo iccCommTags.

Tag	Nombre	Descripción
5F2A	Transaction Currency Code	Tomado de la tabla currency asociada al adquirente.
82	Aplication Interchange Profile	Especifica las funciones de aplicación que es soportada por la tarjeta ejecutando únicamente las soportadas por ICC.
84	Dedicated File Name	Tomado de la aplicación.
95	Terminal Verification Result (TVR)	Resultado de los diferentes procesos ejecutados por el terminal durante el proceso de transacción con la tarjeta.
9A	Transaction Date	Fecha de la transacción tomada de la terminal (YYMMDD).
9C	Transaction Type	Tomado de los datos de la transacción seleccionada.
9F02	Transaction Amount	Se toma de los datos de la transacción. Lleva valor en 0 para tránsito.
9F03	Amount Other	Monto secundario asociado con el monto de una transacción Cash Back.
9F09	Terminal Application Version Number	Tomado de la aplicación.
9F10	Issuer Application Data (IAD)	Obtenido de la tarjeta.
9F1A	Terminal Country Code	Se toma de la tabla de inicialización del terminal.
9F1E	Interface Device Serial Number (IDF)	Número único y permanente de serie asignado al dispositivo de interfaz del fabricante.
9F26	Application Cryptogram (AC)	Usado para aprobar transacciones offline.

Tag	Nombre	Descripción
9F27	Cryptogram Information Data	Usado para aprobar transacciones offline.
9F34	Card Verification Result Method	Resultado del último CVM.
9F35	Terminal Type	Especifica el tipo de terminal.
9F36	Application Transaction Counter (ATC)	Tomado desde la tarjeta.
9F37	Unpredictable Number	Valor para proporcionar viabilidad y la singularidad de la generación del criptograma.
9F41	Transaction Sequence Counter	Contador mantenido por la terminal al que es incrementado por cada transacción.
9F53	Transaction Category Code/ Merchant Category Code	Usualmente dado por el adquirente.
9F07	App Usage Control	Dato generado por el validador.

Tabla 3
Especificación del campo transactionType

Tipo de transacción	Valor	Descripción
Autorización	AUTHORIZATION	Retención de fondos de una tarjeta. Es utilizada para autorizaciones con el monto final.
Verificación	VERIFICATION	Verificación de la tarjeta. Es utilizada para denotar una verificación de cuenta o una autorización nominal.
Devolución	REFUND	Reembolso de fondos a una tarjeta. La devolución se realiza de forma offline, utilizando los datos de la autorización original.
Actualización ATC	ATC_UPDATE	Transacción de actualización de contadores ATC.
Echo Test	ECHO_TEST	Test de conexión con el sistema.
Anulación	VOID	Anulación de transacciones en caso de que se haya recibido respuesta aprobada, pero desea hacer una anulación. En el caso de anulaciones se envían únicamente los campos RetrievalReferenceNumber, authorizationNumber.
Liquidación	SETTLEMENT	Cierre del lote de una terminal.
Reenvío	RESUBMISSION	Reenvío de una autorización previamente declinada, como parte del proceso de recuperación de deuda.
Reversa	REVERSE	Anulación luego de un timeout, cuando no se recibió una respuesta por parte del adquirente. Después de 30 segundos de no recibir respuesta por parte del adquirente, el SCR puede enviar una anulación de este tipo. La transacción lleva únicamente los campos obligatoriamente terminalID, merchantID y systemTraceNumber de la autorización original.

Tabla 4
Especificación del campo entryMode.

Valor	Descripción
MNL	Digitando los datos de la cuenta (Manual entry).
CLC	Captura de los datos del chip de la tarjeta utilizando un dispositivo EMV sin contacto sin capacidad de PIN.

6.1.2 Estructura de la trama del adquirente

Una vez enviada la solicitud de autorización, el adquirente devuelve una respuesta con los campos especificados en la tabla 5.

Tabla 5

Respuesta de las solicitudes de autorización del adquirente.

Campo	Descripción	Formato	Mandatorio
authorizationNumber	Número de autorización.	Alfanumérico de hasta 36 caracteres.	Si
hostDate	Fecha de la transacción.	Etiqueta de tiempo de 10 dígitos.	Si
hostTime	Hora en que se realizó la transacción.	Etiqueta de tiempo de 10 dígitos.	Si
PAR	Identificador que hace referencia a múltiples métodos de pago de un cliente. Opcional para uso futuro.	Alfanumérico de 29 caracteres.	No
F_PAN	PAN embozado en tarjeta física. Opcional para uso futuro.	Número entero de hasta 19 dígitos.	No
retrievalReferenceNumber	Número de referencia de la transacción. Utilizado por el BAC Credomatic para hacer el match entre una autorización y su liquidación, así como entre la autorización y una devolución.	Alfanumérico de hasta 12 caracteres.	Si
responseCode	Código de respuesta de la transacción. Los posibles valores se pueden ver en la tabla 6.	Número entero de 2 dígitos.	Si
responseCodeDescription	Descripción de la respuesta. Los posibles valores se pueden ver en la tabla 6.	Alfanumérico de hasta 100 caracteres.	Si
salesAmount	Monto de la transacción.	Numérico de 10 dígitos, 2 decimales.	Si
systemTraceNumber	Número de seguimiento del sistema.	Alfanumérico de 6 caracteres.	Si
POSDData	Hace referencia al DE61 de MasterCard o al DE60 de VISA. Utilizado por el Banco Nacional para hacer el match entre una autorización y su liquidación, así como entre la autorización y una devolución.	Alfanumérico de 25 caracteres.	BN: Si Otros: No
additionalData	Hace referencia al DE63 de ambas marcas. Utilizado por el Banco Nacional para hacer el match entre una autorización y su liquidación, así como entre la autorización y una devolución.	Alfanumérico de 15 caracteres.	BN: Si Otros: No

Tabla 6

Códigos de respuesta de las transacciones.

Código	Descripción	Código	Descripción
00	Approved or complete successfully.	62	Restricted card.
01	Refer to card issuer.	63	Security violation.

Código	Descripción	Código	Descripción
03	Invalid merchant.	65	Exceeds withdrawal count limit.
04	Capture card.	70	Contact card issuer.
05	Do not honor.	71	PIN not changed.
08	Honor with ID.	75	Allowable number of PIN tries exceeded.
10	Partial Approval.	76	Invalid/nonexistent to account specified.
12	Invalid transaction.	77	Invalid/nonexistent from account specified.
13	Invalid amount.	78	Invalid/nonexistent account specified (general).
14	Invalid card number.	84	Invalid authorization life cycle.
15	Invalid issuer.	85	Not declined Valid for all zero amount transactions.
30	Forma error.	86	PIN validation no possible.
41	Lost Card.	87	Purchase amount only.
43	Stolen card.	88	Cryptographic failure.
51	Insufficient funds/over credit limit.	89	Unacceptable PIN—Transaction declined.
54	Expired card.	91	Authorization platform or issuer system inoperative.
55	Invalid PIN.	92	Unable to route transaction.
57	Transaction not permitted to issuer/cardholder.	94	Duplicate transmission detected.
58	Transaction not permitted to acquirer/terminal.	96	System error. Utilizado para timeouts.
61	Exceeds withdrawal amount limit.	R0	Stop payment order.
R1	Revocation of authorization order.	R3	Revocation of all authorization.

6.2 Tramas para el servicio de recuperación de deuda

El proceso de recuperación de deuda inicia cuando una tarjeta es ingresada a la lista gris (luego de obtener una solicitud de autorización declinada), lo que significa que el monto acumulado para la tarjeta no podrá ser cobrado (liquidado), o que el pago fue asumido por el emisor en aplicación del modelo de riesgos.

En estos casos se crea un registro para recuperación de deuda, a efectos de activar el proceso que se encarga de reintentar la autorización de los montos que no recibieron una respuesta exitosa en solicitudes de autorización previas, con el fin de liquidar el monto pendiente de cobro y poder retirar la tarjeta de la lista gris, de manera que el pasajero pueda seguir utilizando la tarjeta como dispositivo de pago en SINPE-TP.

El servicio para recuperación de deuda puede ser invocado de tres maneras:

- **Por el SCR de forma calendarizada:** se hace un reenvío de la autorización original, con ciertos cambios en sus valores. Para lograr esto debe realizarse una autorización denominada “Transacción Iniciada por Comerciante” o MIT (por sus siglas en inglés). Al realizar la MIT, debe identificarse la transacción original que se está reenviando.

- **Por una marca del cliente:** al intentar viajar con una tarjeta que se encuentre en lista gris, se acciona el proceso de recuperación de deuda al llegar a SINPE-TP. En este caso se crea una solicitud de autorización nueva a partir de la marca entrante.
- **Por solicitud del cliente:** el cliente solicita la activación del proceso, ya sea por medio del portal web o mediante un agente de servicios, y se ejecuta una solicitud de autorización de “Tarjeta no Presente” o CNP (por sus siglas en inglés).

Las solicitudes de autorización para los diferentes inicializadores de recuperación de deuda son autorizaciones en línea, por lo que la respuesta se recibe de forma inmediata. En el caso de recibir una respuesta exitosa, el valor de la deuda se actualiza con “saldo cero” y se excluye el dispositivo de pago de la lista gris, por lo que el usuario podrá volver a utilizarlo para viajar en el transporte público.

El servicio de recuperación de deuda proporcionado por el adquirente debe cumplir con el estándar RESTful, con el cual pueda recibir solicitudes POST mediante el protocolo HTTPS. Además, el servicio es habilitado por el adquirente en la siguiente la ruta:

- [https://<host del adquirente>\[:puerto\]/recuperacion-deuda](https://<host del adquirente>[:puerto]/recuperacion-deuda)

6.2.1 Estructura de la trama del SCR

Tomando en cuenta lo anterior, la tabla 7 especifica los campos clave que deben tener las solicitudes de autorización para recuperación de deuda inicializada por el SCR; dependiendo del inicializador de la solicitud, los valores de algunos de sus campos podrían variar. Los demás campos son iguales a la autorización original.

Tabla 7

Trama de información para las solicitudes de autorización MIT

Campo	Data Element	Descripción	Formato	Mandatorio
totalAmount	DE04	Monto total de la transacción.	Número con 10 dígitos, 2 decimales.	Si
SystemTraceNumber	DE11	Campo generado automáticamente por la terminal y se incrementa por cada transacción realizada. Se requiere en el mensaje de respuesta del host para validar la solicitud enviada.	Alfanumérico de 6 caracteres.	Si
DateTimeLocalTrans	DE12 y DE13	Fecha y hora local del momento en que se realizó la transacción en el validador.	Etiqueta de tiempo de 10 dígitos.	Si
MCC	DE18	Tipo de comercio. Los valores válidos son: 4111: Transporte de pasajeros de cercanías locales y suburbanos, incluidos ferries. 4112: Ferrocarriles de pasajeros. 4131: Líneas de autobús.	Número entero de 4 dígitos.	Si
entryMode	DE22	Indica la forma en que fue leída la información de la tarjeta. Manual, MagStripe, Contact Less, Chip. Ver tabla 3 para el detalle del campo entryMode y sus posibles valores.	Texto de 3 dígitos. Ver tabla 3 para posibles valores.	Si

Campo	Data Element	Descripción	Formato	Mandatorio
CardSequenceNumber	DE23	Número de secuencia de la tarjeta e identifica las tarjetas con un mismo DE002 (Número de tarjeta). Es mandatorio si la terminal envía el dato, de otra manera no es necesario.	Número entero de 3 dígitos.	Si
track2	DE35	Información cifrada de la lectura del track de la tarjeta. El campo es enviado cuando se tiene una recuperación de deuda inicializada por un tap. En otros casos no es mandatorio.	Información cifrada.	Condicional
terminalId	DE41	Identificador único de la terminal.	Alfanumérico de hasta 36 caracteres.	Si
MerchantID	DE42	Identifica de forma exclusiva a un comerciante determinado.	Alfanumérico de hasta 36 caracteres.	Si
TransactionTypeIdentifier	DE48	El tipo de autorización que debe ser enviado. Este corresponde al DE 48, subelemento 64, subcampo 1. Mandatorio únicamente para transacciones de MasterCard.	Número de 2 dígitos.	Condicional
TransportationMode	DE48	Identifica el tipo transporte en el que se realizó el tap (autobús, tren, etc.). Este corresponde al DE 48, subelemento 64, subcampo 2. Mandatorio únicamente para transacciones de MasterCard.	Número de 2 dígitos.	Condicional
Currency	DE49	Moneda.	Según el ISO 4217 en formato numérico.	Si
iccCommTags	DE55	Contiene los datos relacionados con EMV en formato TLV (Tag, Length, Value). Es el equivalente al campo ICC Related Data del estándar ISO 8583.	Información cifrada.	Si
PrivateUse	DE63	Campo de uso particular del adquirente.	Objeto de tipo JSON.	Si
PrimaryAccountNumber	N/A	El número de cuenta primario (PAN), contiene el número de cuenta de la tarjeta, el cual es representado por un número entero de hasta 19 dígitos, en caso de que el dispositivo de pago sea emulado se envía el F-PAN. Incluido cuando el track 2 no está presente.	Información cifrada.	Condicional
transactionType	N/A	Tipo de transacción. Ver tabla 3 para el detalle del campo transactionType y sus posibles valores. Para esta autorización se utiliza el valor de Reenvío.	Alfanumérico. Ver tabla 3 para posibles valores.	Si
TerminalCountryCode	N/A	Código de país de la institución adquirente	Texto de hasta 3 caracteres.	Si
taxAmount	N/A	Monto de impuestos aplicados a la	Número de 10 dígitos,	Si

Campo	Data Element	Descripción	Formato	Mandatorio
		transacción.	2 decimales.	
serviceCode	N/A	Código de servicio definido en ISO para el track 1 y track 2.	Alfanumérico de hasta 4 caracteres.	Si
applicationLabel	N/A	Identificador asociado al AID, utilizado en la transacción.	Alfanumérico de hasta 50 caracteres.	Si
ExpirationDate	N/A	Esta es la fecha de vencimiento del PAN y es incluida cuando el track I y /o track II no están presentes.	Número de 4 dígitos, en formato YYMM (año y mes).	Condicional

6.2.2 Estructura de la trama del adquirente

Una vez enviada la solicitud de autorización, el adquirente devuelve una respuesta con los campos especificados en la tabla 5.

6.3 Tramas para el servicio de liquidación

Para la liquidación el adquirente debe habilitar un servicio RESTful, donde se le envíe el detalle de las transacciones a liquidar, por los montos autorizados durante el día y los montos cubiertos por la responsabilidad del emisor. Este endpoint puede ser invocado en diferentes momentos del día para distribuir la carga del procesamiento del mensaje. Se envía a liquidar un dispositivo de pago en tres escenarios:

1. Cuando se acabe el periodo de viaje.
2. Cuando la tarjeta alcance el límite de responsabilidad del emisor.
3. Al realizar una devolución a un dispositivo de pago, la cual se aplica en forma offline utilizando los datos de la autorización original.

El adquirente realiza la liquidación de los montos especificados en el mensaje de liquidación; ello para tramitar el débito del dinero de la cuenta del cliente mediante la entidad emisora y acreditarlo posteriormente al BCCR. Asimismo, el adquirente debe procesar solicitudes de liquidación de acuerdo con los modelos transaccionales definidos por las principales marcas que operan en el país (VISA, MasterCard y American Express).

El servicio RESTful donde se envía la trama de Liquidación debe ser habilitado por el adquirente en la siguiente dirección:

- [https://<host del adquirente>\[:puerto\]/settlement](https://<host del adquirente>[:puerto]/settlement)

6.3.1 Estructura de la trama del SCR

Los mensajes de liquidación siguen un formato JSON. La trama consta de un encabezado, el cual es un resumen de todas las transacciones realizadas durante el día (Tabla 8), y de un listado con el detalle de dichas transacciones (Tabla 8.1).

Tabla 8
Trama de información del archivo de liquidación.

Campo	Descripción	Formato	Mandatorio
SettlementID	Identificador único de liquidación.	Alfanumérico de hasta 36 caracteres.	Si

Campo	Descripción	Formato	Mandatorio
transactionType	Tipo de transacción. Para el resumen de liquidación se utiliza el valor para Liquidación.	SETTLEMENT.	Si
Date	Fecha y hora del envío de la liquidación.	Etiqueta de tiempo de 10 dígitos.	Si
DebitTransactionsQuantity	Cantidad de transacciones de débito.	Entero de 7 dígitos.	Si
DebitTransactionsAmount	Monto de transacciones de débito.	Número de 10 dígitos, 2 decimales.	Si
DebitTransactionsCommission	Monto de comisiones de débito.	Número de 10 dígitos, 2 decimales.	Si
CreditTransactionsQuantity	Cantidad de transacciones de crédito (devoluciones o reembolsos).	Entero de 7 dígitos.	Si
CreditTransactionsAmount	Monto de transacciones de crédito (devoluciones o reembolsos).	Número de 10 dígitos, 2 decimales.	Si
CreditTransactionsCommission	Monto total de comisiones de comisiones de crédito (devoluciones o reembolsos).	Número de 10 dígitos, 2 decimales.	Si
NetAmount	Monto neto.	Número de 10 dígitos, 2 decimales.	Si
terminalId	Identificador único de la terminal que realiza la liquidación.	Alfanumérico de hasta 36 caracteres.	Si
Transactions	Listado de transacciones en firme Ver tabla 8.1 para el detalle de cada transacción.	Arreglo de objetos JSON.	Si

Los campos de datos que lleva cada transacción del campo Transactions en la lista de la trama, se especifican en la tabla 8.1.

Tabla 8.1

Detalle de los campos presentes en cada transacción, incluido en el campo Transactions del encabezado de la Trama.

Campo	Data Element	Descripción	Formato	Mandatorio
Consecutive	N/A	Número consecutivo de la transacción para la liquidación presente. Es utilizado para llevar un orden en las transacciones enviadas a liquidar.	Entero de 6 dígitos.	Si
totalAmount	DE04	Monto total de la transacción. Es el equivalente al campo Amount, transaction del estándar ISO 8583.	Numérico de 10 dígitos, 2 decimales.	Si
SystemTraceNumber	DE11	El campo STAN es generado automáticamente por la terminal y se incrementa por cada transacción realizada. Se requiere en el mensaje de respuesta del host para validar la solicitud enviada.	Alfanumérico de 6 caracteres.	Si

Campo	Data Element	Descripción	Formato	Mandatorio
MCC	DE18	Tipo de comercio. Los valores válidos son: 4111: Transporte de pasajeros de cercanías locales y suburbanos, incluidos ferries. 4112: Ferrocarriles de pasajeros. 4131: Líneas de autobús.	Número entero de 4 dígitos.	Si
entryMode	DE22	Indica la forma en que fue leída la información de la tarjeta. Manual, MagStripe, Contact Less, Chip. Ver tabla 3 para el detalle del campo entryMode y sus posibles valores.	Texto de 3 dígitos. Ver tabla 4 para posibles valores.	Si
CardSequenceNumber	DE23	Número de secuencia de la tarjeta e identifica las tarjetas con un mismo DE002 (Número de tarjeta). Es obligatorio si la terminal envía el dato, de otra manera no es necesario.	Número entero de 3 dígitos.	No
terminalId	DE41	Identificador único de la terminal.	Alfanumérico de hasta 36 caracteres.	Si
MerchantID	DE42	Cuando se concatena con el identificador del adquirente, identifica de forma exclusiva a un comerciante determinado.	Alfanumérico de hasta 36 caracteres.	Si
TransactionTypeIdentifier	DE48	El tipo de autorización que debe ser enviado. Este corresponde al DE 48, subelemento 64, subcampo 1.	Número de 2 dígitos.	Si
TransportationMode	DE48	Identifica el tipo transporte en el que se realizó el tap (bus, tren, etc). Este corresponde al DE 48, subelemento 64, subcampo 2.	Número de 2 dígitos.	Si
Currency	DE49	Moneda.	Según el ISO 4217 en formato numérico.	Si
PrimaryAccountNumber	N/A	El número de cuenta primario (PAN), contiene el número de cuenta de la tarjeta. Esta información va cifrada en la solicitud.	Número entero de hasta 19 dígitos.	Si
retrievalReferenceNumber	N/A	Número de referencia de la transacción. Utilizado por el BAC Credomatic para hacer el match entre una autorización y su liquidación, así como entre la autorización y una devolución.	Alfanumérico de hasta 12 caracteres.	Si
authorizationNumber	N/A	Número de autorización.	Alfanumérico de hasta 36 caracteres.	Si
DateTimeFirstLocalTrans	N/A	Fecha y hora local del momento en que	Etiqueta de tiempo	Si

Campo	Data Element	Descripción	Formato	Mandatorio
		se realizó la primera transacción en el validador, para el presente periodo de viaje.	de 10 dígitos.	
DateTimeLastLocalTrans	N/A	Fecha y hora local del momento en que se realizó la última transacción en el validador, para el presente periodo de viaje.	Etiqueta de tiempo de 10 dígitos.	Si
transactionType	N/A	Tipo de transacción. Ver tabla 3 para el detalle del campo transactionType y sus posibles valores.	Alfanumérico. Ver tabla 3 para posibles valores.	Si
TerminalCountryCode	N/A	Código de país de la institución adquirente.	Texto de hasta 3 caracteres.	Si
serviceCode	N/A	Código de servicio definido en ISO para el track 1 y track 2.	Alfanumérico de hasta 36 caracteres.	Si
applicationLabel	N/A	Identificador asociado al AID utilizado en la transacción.	Alfanumérico de hasta 50 caracteres.	Si
Commission	N/A	La comisión que va a tener cada transacción de acuerdo al reglamento.	Número de 10 dígitos, 2 decimales.	Si
TransactionObjective	N/A	Es la finalidad (crédito o débito) con el cual se realiza la transacción. Los posibles valores se definen en el cuadro 8.2.	Alfanumérico de hasta 6 caracteres.	Si
ResponseCode	FD-38	Código de respuesta de la transacción respectiva. En caso de VISA, tendrá el valor VFT000 para transacciones liquidadas bajo responsabilidad de emisor.	00 o VFT000.	Si
POSDData	DE-61/ DE-60	Hace referencia al DE61 de MasterCard o al DE60 de VISA. Utilizado por el BN para hacer el match entre una autorización y su liquidación, así como entre la autorización y una devolución.	Alfanumérico de 25 caracteres.	BN: Si Otros: No
additionalData	DE-63	Hace referencia al DE63 de ambas marcas. Utilizado por el BN para hacer el match entre una autorización y su liquidación, así como entre la autorización y una devolución.	Alfanumérico de 15 caracteres.	BN: Si Otros: No
SettlementDate	DE-15	Fecha de la liquidación, enviado únicamente para las transacciones con MasterCard.	Número de 4 dígitos, en formato MMDD (mes y día).	Condicional
iccCommTags	DE55	Contiene los datos relacionados con EMV en formato TLV (Tag, Length, Value). Es el equivalente al campo ICC Related Data del estándar ISO 8583.	Información cifrada.	BN: Si Otros: No

Tabla 8.2

Posibles valores para el objetivo de las transacciones (TransactionObjective)

Objetivo de la transacción	Valor	Descripción
Débito	debit	Utilizado cuando la liquidación corresponde a un débito a la cuenta del dispositivo de pago.
Crédito	credit	Utilizado cuando la liquidación corresponde un crédito a la cuenta del dispositivo de pago.

6.3.2 Estructura de la trama del adquirente

Una vez enviada la solicitud de liquidación, el adquirente devuelve una respuesta con los campos especificados en la tabla 9.

Tabla 9

Respuesta de las solicitudes de liquidación del adquirente.

Campo	Descripción	Formato	Mandatorio
SettlementID	Identificador único de liquidación.	Alfanumérico de hasta 36 caracteres.	Si
responseCode	Código de respuesta del resultado de procesar el mensaje. Los valores posibles se encuentran en la tabla 6.	Número entero de 3 dígitos.	Si
responseCodeDescription	Descripción de la respuesta.	Alfanumérico de hasta 100 caracteres.	Si

6.4 Tramas para el servicio de verificación del código de seguridad³

La verificación del código de seguridad es un mensaje utilizado para transacciones de tarjetas no presentes, realizadas con una entrada manual de datos. Con este servicio el usuario accede a un portal web o aplicación móvil e ingresa los datos de su tarjeta, para registrarla en su cuenta de usuario. El objetivo de esta transacción es validar que los datos que ingrese el usuario son correctos, que la tarjeta es genuina y que la cuenta asociada se encuentra activa.

El servicio de verificación del código de seguridad proporcionado por el adquirente debe cumplir con el estándar RESTful, con el cual pueda recibir solicitudes POST mediante el protocolo HTTPS. Además, debe ser habilitado por el adquirente en la siguiente la ruta:

- [https://<host del adquirente>\[:puerto\]/verificacion-cvv](https://<host del adquirente>[:puerto]/verificacion-cvv)

6.4.1 Estructura de la trama del SCR

La tabla 10 especifica los campos clave que deben tener las solicitudes de verificación del código de seguridad inicializadas por el SCR.

³ Las transacciones para la verificación del código de seguridad es una transacción que se utiliza para el registro de medios de pago en canales web o móviles del usuario. Como tal no es parte de las certificaciones L3 de transporte, por lo que este mensaje no será necesario de implementar en la primer versión e integración del sistema. Las mismas se mantienen en el documento como referencia para futuras implementaciones.

Tabla 10

Trama de información para las solicitudes de verificación del código de seguridad

Campo	Descripción	Formato	Mandatorio
DateTime	Fecha y hora local del momento en que se realiza la solicitud.	Etiqueta de tiempo de 10 dígitos.	Si
entryMode	Indica la forma en que fue leída la información de la tarjeta. En la tabla 3 se detallan los posibles valores.	Texto de 3 dígitos.	Si
PrimaryAccountNumber	El número de cuenta primario (PAN), contiene el número de cuenta de la tarjeta, el cual es representado por un número entero de hasta 19 dígitos.	Información cifrada.	Si
ExpirationDate	Esta es la fecha de vencimiento del PAN, en formato YYMM (año y mes).	Númerico en formato YYMM (año y mes).	Si
CVV	Código de seguridad de la tarjeta. Número de hasta 4 dígitos.	Información cifrada.	Si
CardholderName	Nombre del tarjetahabiente a como se encuentra impreso en la tarjeta.	Alfanumérico de hasta 50 caracteres.	Si

6.4.2 Estructura de la trama del adquirente

Luego de enviada la solicitud de verificación de código de seguridad, el adquirente devuelve una respuesta con los campos especificados en la tabla 11.

Tabla 11

Respuesta de las solicitudes de verificación del código de seguridad del adquirente

Campo	Descripción	Formato	Mandatorio
responseCode	Código de respuesta de la transacción. Los posibles valores se pueden ver en la tabla 6.	Número entero de 2 dígitos.	Si
responseCodeDescription	Descripción de la respuesta. Los posibles valores se pueden ver en la tabla 6.	Alfanumérico de hasta 100 caracteres.	Si

7 Anexos:

7.1 Archivos relacionados con la autorización en formato JSON

7.1.1 Solicitud de autorización con el adquirente

```
{
  "totalAmount": 110.00,
  "SystemTraceNumber": "ABC123",
  "DateTimeLocalTrans": "1612453379",
  "MCC": 4111,
  "entryMode": "CLC",
  "CardSequenceNumber": 111,
  "track2": "6CF2FC4F21 ... F0CB",
  "terminalId": "c2c78c7f-4fd9-4453-8ced-95e2fa7c146d",
  "MerchantID": "BCCR",
  "TransportationTypeIdentifier": "01",
  "TransportationMode": "04",
  "Currency": 188,
  "iccCommTags": "5F2A",
  "PrivateUse": {...},
  "TerminalCountryCode": "CRC",
  "serviceCode": "702F",
  "applicationLabel": "Banco Marca",
  "transactionType": "AUTHORIZATION",
}
```

* track2 y iccCommTags van cifrados bajo el algoritmo AES para el envío de las autorizaciones.

7.1.2 Respuesta de solicitud de autorización del adquirente

```
{  
  "authorizationNumber": "af2744ec-65c4-4d45-9bda-697b6c941639",  
  "hostDate": "1612453379",  
  "hostTime": "1612453379",  
  "retrievalReferenceNumber": "ABCDEF123456",  
  "responseCode": 00,  
  "responseCodeDescription": "Approved successfully",  
  "salesAmount": 110.00,  
  "systemTraceNumber": "ABC123",  
  "POSData": "abcde-fhhijdfghjklqwertyu",  
  "AdditionalData": "abcdefghjklqwer"  
}
```

7.1.3 Solicitud de anulación de transacción

```
{  
  "totalAmount": 110.00,  
  "SystemTraceNumber": "ABC123",  
  "DateTimeLocalTrans": "1612453379",  
  "MCC": 4111,  
  "entryMode": "CLC",  
  "CardSequenceNumber": 111,  
  "track2": "6CF2FC4F21 ... F0CB",  
  "terminalId": "c2c78c7f-4fd9-4453-8ced-95e2fa7c146d",  
  "MerchantID": "BCCR",  
  "TransportationTypeIdentifier": "01",  
  "TransportationMode": "04",  
  "Currency": 188,  
  "iccCommTags": "5F2A",  
  "PrivateUse": {...},  
  "TerminalCountryCode": "CRC",  
  "serviceCode": "702F",  
  "applicationLabel": "Banco Marca",  
  "transactionType": "VOID",  
  "authorizationNumber": "af2744ec-65c4-4d45-9bda-697b6c941639",  
  "retrievalReferenceNumber": "ABCDEF123456"  
}
```

7.1.4 Solicitud de reversión de transacción

```
{  
  "totalAmount": 110.00,  
  "DateTimeLocalTrans": "1612453379",  
  "MCC": 4111,  
  "entryMode": "CLC",  
  "CardSequenceNumber": 111,  
  "track2": "6CF2FC4F21 ... F0CB",  
  "TransportationTypeIdentifier": "01",  
  "TransportationMode": "04",  
  "Currency": 188,  
  "iccCommTags": "5F2A",  
  "PrivateUse": {...},  
  "TerminalCountryCode": "CRC",  
  "serviceCode": "702F",  
  "applicationLabel": "Banco Marca",  
  "SystemTraceNumber": "ABC123",  
  "terminalId": "c2c78c7f-4fd9-4453-8ced-95e2fa7c146d",  
  "MerchantID": "BCCR",  
  "transactionType": "REVERSE"  
}
```

7.1.5 Respuesta de anulaciones o reversiones del adquirente

```
{  
  "systemTraceNumber": "ABC123",  
  "responseCode": 00,  
  "responseCodeDescription": "Completed successfully",  
  "hostDate": "1612453379",  
  "hostTime": "1612453379",  
}
```

7.2 Archivos relacionados con la liquidación en formato JSON

7.2.1 Trama de información para el archivo de liquidación con el adquirente

```
{
  "SettlementID": "af2744ec-65c4-4d45-9bda-697b6c941639",
  "transactionType": "SETTLEMENT",
  "Date": "1612453400",
  "DebitTransactionQuantity": 010,
  "DebitTransactionsAmount": 12000.00,
  "DebitTransactionsCommission": 120.00,
  "CreditTransactionQuantity": 001,
  "CreditTransactionsAmount": 500.00,
  "CreditTransactionsCommission": 5.00,
  "NetAmount": 12375.00,
  "Transactions": [
    {
      "Consecutive": 1,
      "totalAmount": 110.00,
      "SystemTraceNumber": "ABC123",
      "MCC": 4111,
      "entryMode": "CLC",
      "CardSequenceNumber": "111",
      "terminalId": "c2c78c7f-4fd9-4453-8ced-95e2fa7c146d",
      "MerchantID": "BCCR",
      "TransactionTypeIdentifier": "01",
      "TransportationMode": "04",
      "Currency": 188,
      "PrimaryAccountNumber": "Ao7qxNpGI- ... z20JFUWA",
      "transactionID": "ed1564ec-65c4-4d45-9bda-697b6c941639",
      "retrievalReferenceNumber": "ABCD1234",
      "authorizationNumber": "af2744ec-65c4-4d45-9bda-697b6c941639",
      "DateTimeFirstLocalTrans": "1612453379",
      "DateTimeLastLocalTrans": "1612453379",
      "transactionType": "AUTHORIZATION",
      "TerminalCountryCode": "CRC",
      "serviceCode": "702F",
      "applicationLabel": "Banco Marca",
      "Commission": 1.10,
      "TransactionObjective": "debit",
      "ResponseCode": "00",
      "POSDData": "abcde-fhhijdfghjklqwertyu",
      "AdditionalData": "abcdefghjklqwer"
    }
  ],
}
```

```
{
  "Consecutive": 2,
  "totalAmount": 500.00,
  "SystemTraceNumber": "ABC123",
  "MCC": 4111,
  "entryMode": "CLC",
  "CardSequenceNumber": "111",
  "terminalId": "c2c78c7f-4fd9-4453-8ced-95e2fa7c146d",
  "MerchantID": "BCCR",
  "TransactionTypeIdentifier": "01",
  "TransportationMode": "04",
  "Currency": 188,
  "PrimaryAccountNumber": "Ao7qxNpGI- ... z20JFUWA",
  "transactionID": "ed1564ec-65c4-4d45-9bda-697b6c941098",
  "retrievalReferenceNumber": "ABCD1256",
  "authorizationNumber": "af2744ec-65c4-4d45-9bda-697b6c941098",
  "DateTimeFirstLocalTrans": "1612453380",
  "DateTimeLastLocalTrans": "1612453380",
  "transactionType": "AUTHORIZATION",
  "TerminalCountryCode": "CRC",
  "serviceCode": "702F",
  "applicationLabel": "Banco Marca",
  "Commission": 5.00,
  "TransactionObjective": "debit",
  "ResponseCode": "VFT000",
  "POSDData": "afgrtd-grasdfghjklqwertyu",
  "AdditionalData": "grasdfghjklqwer"
},
```

```

{
  "Consecutive": 3,
  "totalAmount": 200.00,
  "SystemTraceNumber": "ABCQW12378",
  "MCC": 4111,
  "entryMode": "CLC",
  "CardSequenceNumber": "111",
  "terminalId": "c2c78c7f-4fd9-4453-8ced-95e2fa7c146d",
  "MerchantID": "BCCR",
  "TransactionTypeIdentifier": "01",
  "TransportationMode": "04",
  "Currency": 188,
  "PrimaryAccountNumber": "Ao7qxNpGI- ... z20JFUWA",
  "transactionID": "ed1564ec-65c4-4d45-9bda-697b6c941639",
  "retrievalReferenceNumber": "PBCD9234",
  "authorizationNumber": "af2744ec-65c4-4d45-9bda-697b6c941639",
  "DateTimeFirstLocalTrans": "1612453379",
  "DateTimeLastLocalTrans": "1612453379",
  "transactionType": "REFUND",
  "TerminalCountryCode": "CRC",
  "serviceCode": "702F",
  "applicationLabel": "Banco Marca"
  "Commission": 2.00,
  "TransactionObjective": "credit",
  "ResponseCode": "00"
  "POSDData": "abcde-fhhijdfghjklqwertyu",
  "AdditionalData": "abcdefghjklqwer"
},
...
]
}

```

* PrimaryAccountNumber va cifrado bajo el algoritmo AES para el envío de las liquidaciones.

7.2.2 Respuesta de solicitud de liquidación del adquirente

```
{  
  "SettlementID": "af2744ec-65c4-4d45-9bda-697b6c941639",  
  "responseCode": 00,  
  "responseCodeDescription": "Complete successfully",  
}
```

7.3 Archivos relacionados con la verificación del código de seguridad

7.3.1 Solicitud de verificación del código de seguridad

```
{  
  "DateTime": "1612453379",  
  "entryMode": "CLC",  
  "PrimaryAccountNumber": "4261636c63364387a7074396...4e70e99b7572951",  
  "ExpirationDate": "2507",  
  "CVV": "4261636c63364387a7074396...4e70a940c032942d",  
  "CardholderName": "Juan Perez P."  
}
```

7.3.2 Respuesta de verificación del código de seguridad

```
{  
  "responseCode": 00,  
  "responseCodeDescription": "Completed successfully"  
}
```