Guía de Comercio Electrónico API v2.6

Integración Simplificada con 3DS

15 septiembre 2022

Contenido

Bitácora de Modificaciones

Versión del Documento	Observaciones	Fecha de Publicación
1.0	Versión original	25 septiembre 2021
2.0	Borrador final	10 diciembre 2021
2.1	Se agregó *PowerTranz-GatewayKey* a la Sección 4 Se agregó numeración a todo el documento Se descartaron *PowerTranzId* y *PowerTranzPassword* en la Sección 7.3	24 diciembre 2021
2.2	Correcciones adicionales	10 febrero 2022
2.3	Correcciones adicionales: gramática y contenido	23 marzo 2022
2.4	- Clarificación del Indicador de Tokenización (Tokenize flag) en la sección 5 - Se agregó el indicador *TokenType* a la sección 5 - Se agregó límite de tiempo de 5 minutos al *SPiToken* en la sección 2.2, punto 1.7 - Se agregó clarificación al *Payment Completion Header* (Encabezamiento de Finalización de Pago) en la sección 7.3 - Se agregó clarificación al *Approved flag* (indicador de aprobación) en la sección 6 - Se agregó clarificación al IsoResponseCode SP4 (Código ISO de Respuesta) en la sección 2.2 - Se agregó clarificación sobre *TBD* (por ser determinado) en la sección 2.3 - Se agregó clarificación sobre capturas parciales en la sección 7.4 - Se agregaron casos de prueba Amex en la sección 10 - Se agregó aclaración sobre caracteres prohibidos (ver. §1, Introducción).	25 marzo 2022
2.5	- Actualizaciones a los códigos de respuesta de Powertranz e información sobre los errores, incluyendo una aclaración sobre el formato permitido. - Mejoras a la § 9.1 relacionadas con la decomisión por parte de las marcas de 3DSV1 - Se añadieron los campos *AuthenticationIndicator* y *MessageCategory* a la § 5 - Se añadió la § 9.5 “Tokenización” - Se añadieron ejemplos 7.7, 7.8 y 7.9 a la § sobre tokenización - Se añadió el campo *TaxAmount* a la § 5 - Se agregó aclaración a la § 8.3 sobre *AuthenticationStatus* - Se añadió la § 5.2 - Se eliminó el campo *ExternalIdentifier* de los ejemplos	

	- Se actualizó el resultado de autenticación en el caso M1-01-YA - Se actualizó la § 8.4 - Se actualizó la § 8.5	
2.6	- Se agregó ThreeDSecure.ResponseCode a la §6 - Se agregó FraudCheck a la §6 - Se agregó el Apéndix 3 para FraudCheck - Se agregaron las § 7.10 y 7.11 (ejemplos de FraudCheck) - Se agregó la § 9.6 Fraud Check - Se actualizó el Apéndice 1, Códigos de Respuesta con los códigos de Fraud Check	15 septiembre

1. Introducción

Este documento sirve de guía para desarrolladores que integran su sitio web con la pasarela de pagos PowerTranz de First Atlantic Commerce. Esta guía explica el método sencillo de integración para transacciones de comercio electrónico que utilizan el método de autenticación 3DSecure, ya sea mediante una página alojada (HPP) o de manera convencional.

Advertencia

Los campos en los mensajes que el comercio envía a Powertranz solo aceptan caracteres del alfabeto inglés, es decir, no permiten caracteres del castellano como los acentos o las tildes (Á, á, É, é, Í, í, Ó, ó, Ú, ú, Ü, ü,) ni la letra eñe (Ñ, ñ). De la misma manera, el uso de puntuación está limitado al guion (-) y al punto (.) El sistema tampoco permite el símbolo &, conocido como *ampersand* en inglés, ni los dos puntos (:) ni el punto y coma (;). Presencia de cualquier de estos caracteres en un mensaje pueden causar que PowerTranz lo rechace con un error.)

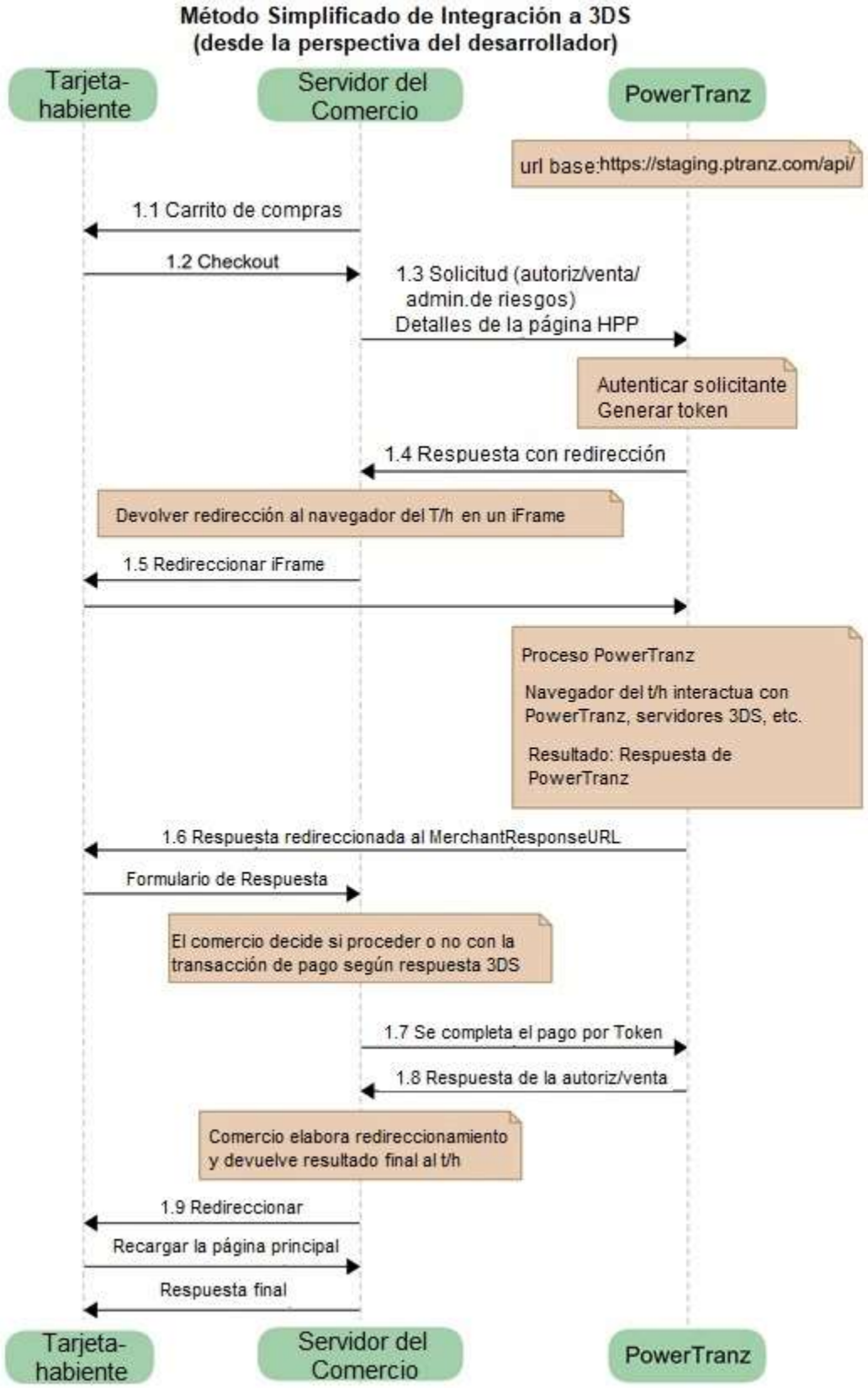
2. Resumen: Comercio Electrónico con Autenticación 3D-Secure

La pasarela de pagos PowerTranz apoya autenticación 3D-Secure versión 2.x con retroceso a 3DS versión 1.0, y envía solicitudes de carácter financiero (autorización, venta, reembolso o anulación) a las redes de pago (MasterCard, Visa, American Express, etc.) para autorizar toda transacción.

La solicitud de autenticación 3D-Secure utiliza los métodos de API “Auth” (autorización), “Sale”(venta) o “RiskMgmt” (manejo de riesgos) que llevan el indicador 3D-Secure habilitado. PowerTranz determina cuál versión de 3D-Secure utilizar basado en la cuenta de tarjeta y las capacidades del banco emisor. El método simplificado de integración 3D-Secure se encarga de las interacciones necesarias para obtener una autenticación 3DS versión 2.0 de una manera fluida, que incluye las “huellas digitales” (características del dispositivo.) Este método maneja el flujo de interrogaciones realizadas por el emisor, e incluye la capacidad de retroceder a la versión 1.0 en aquellos casos donde el emisor no maneja versión 2.0 de 3DSecure.

Cuando se emplea este método de integración, primero ocurre una pre-autenticación y acto seguido una finalización del pago, según el resultado de dicha pre-autenticación. Los datos del pago provienen o bien directamente de la página de pago del comercio o de la Página Alojada PowerTranz. El servidor de PowerTranz procesa la transacción y notifica al servidor del comercio los resultados de la autenticación 3DSecure. Acto seguido, el comercio decide si procede o no con la solicitud de autorización.

2.1 Diagrama de la Integración con 3DS Simplificada



2.2 Integración con 3DS Simplificada – Flujo de Alto Nivel

1.1 El servidor web del comercio despliega en la pantalla del tarjetahabiente (t/h) el contenido final del carrito de compras.

1.2 El t/h efectúa el proceso de pago.

1.3 Según el método de integración que se emplea:

a. El comercio recolecta los datos del pago del t/h y envía una solicitud (Autorización, Venta o Gestión de Riesgos) al servidor de PowerTranz. La solicitud incluye datos pertinentes de la tarjeta y detalles del pago, con el indicador 3DS habilitado; o bien

b. El comercio envía una solicitud (Autorización, Venta o Manejo de Riesgos) al servidor de PowerTranz. La solicitud incluye el nombre y juego de la página alojada (*Hosted Page Set* y *Hosted Page Name*). La página alojada se encarga de recolectar los datos pertinentes de la tarjeta y detalles del pago.

1.4 PowerTranz realiza la autenticación de la solicitud enviada por el comercio, genera un *SPIToken*, y contesta al servidor del comercio con datos de redirección. Si la solicitud satisface requerimientos de validación, PowerTranz devuelve el valor SP4 en el campo IsoResponseCode.

1.5 Los datos de redirección se ubican dentro de la respuesta a la solicitud de Autorización, Venta o Gestión de Manejo de Riesgos enviada por el *endpoint*. La respuesta contiene un formulario HTML con JavaScript embebido. Cuando este formulario se inyecta en un iFrame, se despliega o bien la página alojada (HPP) o un flujo de interrogaciones bajo el control del emisor. Durante esta etapa, el iFrame desplegado en el navegador del t/h interactúa con PowerTranz y con los servidores 3DS necesarios, de acuerdo con el tipo de autenticación 3DS que haga falta. Esto pudiera ocurrir como un flujo fluído desde la perspectiva del t/h. Por otra parte, el t/h pudiera recibir una serie de interrogaciones realizadas por el emisor. Al concluir esta etapa, el iFrame se re direcciona al url indicado en el *MerchantResponseUrl*, y el control regresa al aplicativo del sitio (o app móvil) del comercio. Por favor consulte el Apéndice 2 donde se muestran ejemplos de codificación.

1.6 PowerTranz envía el resultado de la autenticación 3DS al servidor del comercio mediante el navegador del t/h. No se trata de una transacción de carácter financiero, sino sencillamente el resultado de una autenticación 3DS.

1.7 El comercio determina si desea proceder a finalizar el pago, basado en el resultado de la autenticación 3DS. Si el comercio procede a completar el pago, el comercio entonces envía una transacción de finalización de pago que incluye el *SpiToken*. El comercio tiene un marco de 5 minutos dentro del cual enviar la transacción de finalización de pago. Una vez que ha vencido este intervalo, el *SpiToken* deja de estar disponible. A continuación, PowerTranz envía una solicitud de autorización al procesador del emisor.

1.8 PowerTranz devuelve la respuesta de la solicitud de autorización o venta al servidor del comercio.

1.9 El servidor del comercio despliega el resultado en el navegador del tarjetahabiente. Si el comercio realizó una transacción de venta, la transacción queda finalizada y una vez que el ciclo diario de cierre ejecute (controlado por PowerTranz) la cuenta del t/h será cargada por el emisor y la cuenta bancaria del comercio será abonada por el adquirente. Si por otra parte, el comercio realizó una solicitud de autorización, el emisor reducirá el disponible de la tarjeta. Sin embargo, para completar el ciclo de liquidación, será necesario que el comercio transmita una operación de captura.

2.3 Llamadas al API – Detalles Adicionales

En el proceso simplificado de integración 3DS versión 2.0, el sistema del comercio realizará varias llamadas a los *endpoints* en el API de PowerTranz. La primera solicitud (ya sea Autorización, Venta o Gestión de Riesgos) dispara el proceso de autenticación y devuelve un *token* de autorización, el cual se utiliza en las solicitudes siguientes . A continuación, solicitudes opcionales pueden ser enviadas a los *endpoints* "Payment" (Pago), "Capture" (Captura), "Void" (Anulación) y "Refund" (Reembolso), con el propósito de cancelar o finalizar la transacción, según sea necesario.

El comercio dispara una solicitud de autenticación 3D-Secure por medio de los *endpoints* tipo REST "Auth/Sale/RiskMgmt" con el indicador 3DS habilitado.

- Se invoca el *endpoint* "/Auth" (Autorización) o "/Sale" (Venta) cuando el comercio desea efectuar una solicitud de carácter financiero *on line* tras una autenticación 3DS. Si el pago se finaliza con éxito, la autorización requiere que una operación de captura sea enviada a continuación, para finalizar la transacción. Una operación de Venta se encarga de solicitar autorización y marcar la transacción para su captura, sin necesidad de realizar una transacción adicional.

- Una solicitud al *endpoint* "/RiskMgmt" (Manejo de Riesgos) de carácter no financiero se efectúa únicamente cuando el comercio desea autenticar al t/h, es decir, solo Autenticación 3DS 2.0.

Si el comercio decide proceder con una solicitud de autorización (para solicitudes de carácter financiero), la transacción de pago se dispara por medio de una llamada a la función "/Payment".

Notas:

- Durante una llamada de Autorización, Venta o Gestión de Riesgos, el comercio deberá suministrar el "MerchantResponseURL", el cual representa el *endpoint* del servidor del comercio, al cual PowerTranz enviará el resultado final de la transacción.

- Llamadas al API de PowerTranz API se realizan mediante el uso de REST con JSON por encima de HTTPS como protocolo de transporte.

- Los URLs base de los *endpoints* de PowerTranz SPI/HPP, que brindan acceso externo, son como sigue:

Ambiente de Prueba: https://staging.ptranz.com/api/spi/<endpoint>

Producción: https://***TBD***.ptranz.com/api/spi/<endpoint>

- Los comercios pueden hacer llamados "/Capture" (Captura), "/Void" (Anulación) o "/Refund" (Reembolso) para una transacción que haya sido autorizada con éxito. Los URLs base para estos *endpoints* son como siguen:

Ambiente de Prueba: https://staging.ptranz.com/api/<endpoint>

Producción: https://***TBD***.ptranz.com/api/<endpoint>

TBD (por determinarse) – El url de producción será suministrado al comercio una vez que FAC verifique resultados satisfactorios en las transacciones en el ambiente de prueba.

3. *Endpoints* y Operaciones de la Pasarela de Pagos PowerTranz

PowerTranz brinda un juego de *endpoints* de carácter financiero y no financiero para el procesamiento de transacciones. La tabla a continuación muestra cada *endpoint,* con una breve descripción del uso y sus URLs.

Endpoint	Descripción	Tipo	Método	URL
Alive	Status de la pasarela	No financiero	GET	<API Root>/api/alive
Auth (Autorización)	Realizar una autorización SPI, reservando fondos para posterior captura.	Financiero	POST	<API Root>/api/spi/auth
Sale (Venta)	Realizar una autorización SPI con captura.	Financiero		<API Root>/api/spi/sale
RiskMgmt (Manejo de Riesgos)	Transacción de carácter no financiero. Empléese para pre-autenticar transacción tipo solo 3DS.	Financiero	POST	<API Root>/api/spi/riskmgmt
Payment (Pago)	Finalización de pago para una venta pre-autenticada con 3DS o una solicitud de autorización	Financiero	POST	<API Root>/api/spi/payment
Capture (Captura)	Capturar transacción previamente autorizada	Financiero	POST	<API Root>/api/capture
Refund (Reembolso)	Reembolsar transacción previamente autorizada	Financiero	POST	<API Root>/api/refund
Void (Anulación)	Anular una autorización.	Financiero	POST	<API Root>/api/void

El portal "Swagger" para el API de PowerTranz API incluye detalles de los parámetros en formato JSON.

https://staging.ptranz.com/api/swagger/index.html

4. Requerimientos del Encabezamiento de Solicitud bajo PowerTranz

Todas las solicitudes a *endpoints* deberán ser de tipo HTTP POST sobre TLS con contenido JSON. Es obligatorio que el encabezamiento http incluya los parámetros de autenticación del comercio (por ejemplo, PowerTranzId y contraseña). Los comercios deberán llamar a los *endpoints* del API de PowerTranz mediante una solicitud HTTP POST y enviar los parámetros de la solicitud en formato JSON.

Nombre del Campo	Mandatorio o Condicional	Formato	Longitud Máx/Valor	Notas
PowerTranz-PowerTranzId	M	AN	25	Identificador del Comercio para la cuenta PowerTranz del comercio. Ejemplo: 99901066
PowerTranz-PowerTranzPassword	M	AN	100	La contraseña de procesamiento definida para el comercio. Ejemplo: m9mOPK@vpUM
PowerTranz-GatewayKey	C	GUID (trama)	36	Additional *token* assigned by Powertranz No enviar hasta que PowerTranz suministre valor

5. Detalles de los Parámetros del Mensaje de Solicitud: Autorización, Venta, Control de Riesgos

(M)andatorio, (O)pcional, (C)ondicional

Parámetro	M/O/C	Formato	Longitud Máx/Valor	Descripción
TransactionIdentifier	M	GUID (trama)	36	Identificador único asignado por el aplicativo del comercio Ejemplo : f62c3e58-1983-4165-8535-fe5bb6ba6127
TotalAmount	M	DEC	18,3	Monto total según autenticación
TaxAmount	O	DEC	18,3	Monto de imspuestos. Si se envía en una solicitud de autorización, es mismo moto deberá también ser enviado en la solicitud de captura.)
CurrencyCode	M	N	4	(Código de moneda) Deberá utilizarse el código numérico (ISO 4217)
ThreeDSecure	M	BOOL		
Tokenize	C	BOOL		Este indicador hace falta solo para solicitudes RiskMgmt (Manejo de Riesgos). El sistema devuelve el PanToken si Tokenize se ha indicado como *true* (verdadero)
Source				(Fuente) Objeto interior requerido (consultar Subjuego de Datos abajo)
CardPan	M	N	19	No. de cuenta de la tarjeta
CardCvv	O	N	4	CVV (Card verification value)
CardExpiration	M	N	4	Fecha exp. Formato: AAMM
CardholderName	M	AN	2-45	Nombre del tarjetahabiente – mandatorio para transacciones 3DS
Token	O	AN	100	PanToken devuelto en respuesta anterior
Token Type	O	AN		El tipo de token por utilizar. “PG2” debe ser enviado únicamente para tokens de FAC
OrderIdentifier	M	AN	**255**	No. de Pedido asignado por el comercio
BillingAddress				Objeto interior requerido (consultar Subjuego de Datos abajo)
FirstName	O	AN	30	Nombre (Para autenticación con 3DS, el campo CardholderName deberá estar presente en el objeto fuente)
LastName	O	AN	30	Apellido (Para autenticación con 3DS, el campo CardholderName deberá estar presente en el objeto fuente)
Line1	O	AN	30	Domicilio – Línea 1 (mandatorio para AVS)
Line2	O	AN	50	Domicilio – Línea 2
City	O	AN	25	Ciudad
County	O	AN	25	País
State	O	AN	25	Estado/Provincia. Si se suministra deberá indicar el código de subdivisión del país, según el standard ISO 3166-2.

				Para estados en EE.UU. debe utilizarse la abreviatura correcta (CA, FL, GA, NY, etc.)
PostalCode	O	AN	10	Código Postal (mandatorio para AVS) Deberá consistir únicamente de caracteres alfanuméricos.
CountryCode	C	AN	3	Código numérico de país según ISO 3166. Debe estar presente si se indica Estado.
EmailAddress	O	AN	50	Dirección email
PhoneNumber	O	AN	20	Teléfono. Deberá incluir el código del país. Ejemplos: 35301176543210 01176543210 Solo deberá consistir de dígitos y guiones. Otros caracteres están prohibidos.
PhoneNumber2	O	AN	20	Teléfono móvil (ver reglas de validación del campo PhoneNumber arriba)
PhoneNumber3	O	AN	20	Teléfono del trabajo (ver reglas de validación del campo PhoneNumber arriba)
ShippingAddress				Objeto opcional interior al cuerpo del mensaje (consulte subjuego de datos abajo). Note que las validaciones de Billing-Address aplican)
FirstName	O	AN	30	Nombre (para autenticaciones 3DS, CardholderName debe estar presente en el objeto fuente)
LastName	O	AN	30	Apellido (para autenticaciones 3DS, CardholderName debe estar presente en el objeto fuente)
Line1	O	AN	30	Línea 1 del domicilio (requerida para AVS) No se permite el uso de ciertos caracteres (ejemplos: æ, á, é, ñ, *, +, &, :, ;). Sugerimos se evite todo símbolo, aunque puntuación básica sí es permitida (. y -).
Line2	O	AN	50	Línea 2 del domicilio.
City	O	AN	25	Ciudad
County	O	AN	25	País
State	O	AN	25	Estado o provincia
PostalCode	O	AN	10	Código postal (requerido para AVS)
CountryCode	O	AN	3	Deberá consistir del código numérico del país ISO 4217
EmailAddress	O	AN	50	Dirección email
PhoneNumber	O	AN	20	Teléfono (ver reglas de validación del campo PhoneNumber arriba)
PhoneNumber2	O	AN	20	Teléfono móvil (ver reglas de validación del campo PhoneNumber arriba)
PhoneNumber3	O	AN	20	Teléfono (trabajo) (ver reglas de validación del campo PhoneNumber arriba)

AddressMatch	O	BOOL		'true' (verdadero) si domicilio de envío concuerda con domicilio en el estado de cuenta
ExtendedData				Objeto interior requerido
ThreeDSecure				Objeto interior requerido (consultar Subjuego de Datos abajo)
ChallengeWindowSize	M	AN	1	Dimensiones del panel de solicitud 3DS que se le presenta al tarjetahabiente 1 – 250 x 400 2 – 390x400 3 – 500x600 4 – 600x400 5 – 100%
MerchantResponseURL	M	AN	255	URL de Respuesta definido por el comercio
ChallengeIndicator	O	N	2	Valor condicional (si se apoya) 01 = Sin preferencia 02 = No se solicita cuestionar al t/h 03 = Preferencia del solicitante re. cuestionar al t/h por 3DS 04 = Se solicita cuestionar al t/h: por defecto se interpreta como 01 (sin preferencia).
AuthenticationIndicator	O	N	2	01=Transacción de pago 04=Añadir una tarjeta 05=Conservar la tarjeta
MessageCategory	O	N	2	01=PA (Autenticación del pago) 02=NPA (No Autenticación del pago)
HostedPage				Objeto mandatorio interno a ExtendedData (ver subjuego de datos abajo) si se utiliza una HPP
PageSet	O	AN	50	PageSet de la Página Alojada
PageName	O	AN	50	PageName de la Página Alojada

6. Parámetros de la Respuesta (todos tipos de transacción)

(P)resente, (C)ondicional

Parámetro	P/C	Formato	Longitud Max/Valor	Description
TransactionType	P	numérico	2	Tipo de Transacción (1-Autorización, 2-Venta, 3-Captura, 4-Anulación, 5-Reembolso)
Approved	P	BOOL		Status de la transacción La fase de autenticación de la transacción devuelve el valor “false”. En la finalización del pago, este indicador muestra el resultado de la autorización, o sea, “True” o “False”
AuthorizationCode	C	AN	6	Código de autorización
TransactionIdentifier	P	GUID (trama)	36	Identificador único asignado por el aplicativo del comercio Ejemplo: f62c3e58-1983-4165-8535-fe5bb6ba6127
TotalAmount	P	DEC	18,3	Monto de la transacción procesada
CurrencyCode	P	N	3	Código de moneda de transacción
CardBrand	P	AN	255	Marca de la tarjeta (propósito: información)
IsoResponseCode	P	AN	3	Código de respuesta ISO que indica aprobación, denegación o falla
ResponseMessage	P	AN	255	Mensaje de respuesta: descripción de la respuesta según el Código ISO de Respuesta
RRN	P	string	12	No. de Rastreo
OriginalTrxnIdentifier	C	GUID (trama)	36	Identificador de la transacción original comunicado en la respuesta a Captura, Reembolso o Anulación
RiskManagement				Gestión de Riesgo
CvvResponseCode	C			Resultado de verificación del CVV2
ThreeDSecure	P	BOOL		
ECI	C	AN	2	Status de la Autenticación: Y o A
CAVV	C	AN	100	Se indica si Status de la Autenticación es Y o A
Xid	P	AN	100	Identificador de la transacción 3DS
AuthenticationStatus	P	AN	1	Status de autenticación: Consulte el siguiente enlace: 3DS Authentication Results
RedirectData	C	Formulario HTML		Contiene el formulario de redirección enviado al navegador del t/h con estos códigos de respuesta 3D4,3D5,3D6
AuthenticateUrl	C	AN	100	Mandatorio para Autenticaciones 3DS2 cuando se utiliza “device fingerprinting” (datos del dispositivo)
CardEnrolled	P	AN	1	Status del proceso de inscripción de la tarjeta
ProtocolVersion	P	AN	8	Versión del protocolo 3DS que acepta el emisor

FingerprintIndicator	C	AN	1	Status de identificación del dispositivo. Valores posibles: U, Y o N
StatusReason	C	AN	2	Indica la razón por la cual el campo AuthenticationStatus contiene N, U o R. Consulte el siguiente enlace: StatusReason
DsTransID	P	AN	36	Identificador universal único asignado por el servidor de directorio que identifica transacciones individuales.
ResponseCode	P	AN	3	Código de respuesta 3DS que muestra el status de la solicitud 3DS
CardholderInfo	C	AN	255	Datos adicionales opcionalmente suministrados por el emisor al t/h
FraudCheck	C			
FcProvider	C	AN	255	Proveedor de control de frauds. Ejemplo: Kount
ResponseCode	C	AN	3	Código de respuesta del chequeo de fraudes que muestra el status de la solicitud de Kount
FcResponseCode	C	AN	1	Resultado de Kount A – Aprobado D – Declinado R – Revisar E – Referir al superintendente
FcScore	C	N		Puntaje de Kount
FcTransId	C	AN	12	No. de identidad de la transacción asignado por Kount
FcDetails	C			Datos enviados por Kount. Detalles disponibles en el Apéndice 3.
PanToken	C			*Token* del PAN
OrderIdentifier	P	AN	255	Identificador del pedido indicado en la solicitud
SpiToken	C			*Token* SPI
Errors	C			Errores
Code	C	AN	2	Código de error
Message	C	AN	255	Texto que describe el código de error
BillingAddress	C	AN		Objeto interno con datos sobre el domicilio de entrega indicado en la solicitud

7. PowerTranz con 3DS2: Ejemplos de Solicitudes

Autorización, Venta, Gestión de Riesgos

Las solicitudes de Autorización, Venta, y Gestión de Riesgos todas heredan la misma base y comparten los mismos parámetros.

Nota: Algunos parámetros podrán o deberán ser excluidos, según el tipo de solicitud.

A continuación, un ejemplo JSON del flujo de Autorización-Pago-Captura que un comercio pudiera emplear mediante su propia página de pago o una página alojada (HPP).

7.1 Solicitud de Autorización – Página de Pago del Comercio

Solicitud de Autorización

```
POST #AuthUrl# HTTP/1.1
Accept: application/json
PowerTranz-PowerTranzId: #PowerTranzPasswordId#
PowerTranz-PowerTranzPassword: #PowerTranzPassword#
Content-Type: application/json; charset=utf-8
Host: staging.ptranz.com
Content-Length: TBD
Expect: 100-continue
Connection: Keep-Alive

{
  "TransactionIdentifier": "5ee7d7c1-af78-4d7e-9386-
abb280822b73",
  "TotalAmount": 1,
  "CurrencyCode": "978",
  "ThreeDSecure": true,
  "Source": {
    "CardPan": "5115010000000001",
    "CardCvv": "",
    "CardExpiration": "2512",
    "CardholderName": "John Doe"
  },
  "OrderIdentifier": "INT-95e75078-7d58-40e8-8053-
c3d488f05f59-Orc 3569",
  "BillingAddress": {
    "FirstName": "John",
    "LastName": "Smith",
    "Line1": "1200 Whitewall Blvd.",
    "Line2": "Unit 15",
    "City": "Boston",
    "State": "MA",
    "PostalCode": "02116",
    "CountryCode": "840",
    "EmailAddress": "john.smith@gmail.com",
    "PhoneNumber": "617-345-6790"
  },
  "AddressMatch": false,
  "ExtendedData": {
    "ThreeDSecure": {
      "ChallengeWindowSize": 4,
      "ChallengeIndicator": "01"
    },
  "ComercioRespuestaUrl":
"https://localhost:5001/Final"
  }
}
```

Respuesta

```
{
  "TransactionType": 1,
  "Approved": false,
  "TransactionIdentifier": "5ee7d7c1-af78-4d7e-9386-
abb280822b73",
  "IsoResponseCode": "SP4",
  "ResponseMessage": "SPI Preprocessing complete",
  "OrderIdentifier": "INT-95e75078-7d58-40e8-8053-
c3d488f05f59-Orc 3569",
  "RedirectData": "[HTML FORM DATA TRUNCATED FOR
BREVITY]",
  "SpiToken":
"vlf80fset61e73ml9toqu2kqtn5sddelqk9r7kao51kut6h3o-
iseenw5eb"
   }
```

Observaciones:

El script resaltado se auto postea. Es un script presente en la respuesta de Gestión de Riesgo, Autorización y Venta.

- Será necesario desplegar el script resaltado en el navegador del tarjetahabiente.

- Se recomienda incluir el script arriba señalado dentro de un iFrame.

iFrame	**Respuesta de Autenticación**

iFrame
 	
iFrame – Redirect From Server to MerchantResponseURL
	{
	"TransactionType": 1,
	"Approved": false,
	"TransactionIdentifier": "5ee7d7c1-af78-4d7e-9386-abb280822b73",
	"TotalAmount": 1.00,
	"CurrencyCode": "978",
	"CardBrand": "MasterCard",
	"IsoResponseCode": "3D0",
	"ResponseMessage": "3D-Secure complete",
	"RiskManagement": {
	"ThreeDSecure": {
	"Eci": "02",
	"Cavv": " kBMAAAAAnEYBUwH06nACcJeBRfOZ",
	"Xid": " 7cac2981-3732-4ae9-a7c9-8d07ec6726f7",
	"AuthenticationStatus": "Y",
	"CardEnrolled": "Y",
	"ProtocolVersion": "2.1.0",
	"ResponseCode": "3D0"
	}
	},
	"PanToken": "1ra0yl1pp1uo9b98fqkf16d93rgw629x01rm2cpq58s82e8u03",
	"OrderIdentifier": "INT-95e75078-7d58-40e8-8053-c3d488f05f59-Orc 3569",
	"SpiToken": "vlf80fset61e73ml9toqu2kqtn5sddelqk9r7kao51kut6h3o-iseenw5eb",
	"BillingAddress": {
	"FirstName": "John",
	"LastName": "Smith",
	"Line1": "1200 Whitewall Blvd.",
	"Line2": "Unit 15",
	"City": "Boston",
	"State": "MA",
	"PostalCode": "02116",
	"CountryCode": "840",
	"EmailAddress": "john.smith@gmail.com",
	"PhoneNumber": "617-345-6790"
	}
	}

7.2 Solicitud de Autorización – Página Alojada (HPP)

Solicitud de Autorización	**Respuesta**

POST #AuthUrl# HTTP/1.1
Accept: application/json
PowerTranz-PowerTranzId: #PowerTranzPasswordId#
PowerTranz-PowerTranzPassword: #PowerTranzPassword#
Content-Type: application/json; charset=utf-8
Host: staging.ptranz.com
Content-Length: TBD
Expect: 100-continue
Connection: Keep-Alive
 	
{
"TransactionIdentifier": "89876ff5-a44a-4e1f-bf71-8f224823c439",
"TotalAmount": 1,
"CurrencyCode": "978",
"ThreeDSecure": true,
"Source": {
},
"OrderIdentifier": "INT-245d0301-5170-406c-abb7-750aadce9173-Orc 3570",
"BillingAddress": {
"FirstName": "John",
"LastName": "Smith",
"Line1": "1200 Whitewall Blvd.",
"Line2": "Unit 15",
"City": "Boston",
"State": "MA",
”PostalCode”:”02116”,
"CountryCode": "840",
"EmailAddress": "john.smith@gmail.com",
"PhoneNumber": "617-345-6790"
},
"AddressMatch": false,
"ExtendedData": {
"ThreeDSecure": {
"ChallengeWindowSize": 4,
"ChallengeIndicator": "01"
},
"MerchantResponseUrl": "https://localhost:5001/Final",
"HostedPage": {
"PageSet": "GFRHPP",
"PageName": "HPPBilling1"
}
}
}
	{
	"TransactionType": 1,
	"Approved": false,
	"TransactionIdentifier": "89876ff5-a44a-4e1f-bf71-8f224823c439",
	"IsoResponseCode": "SP4",
	"ResponseMessage": "SPI Preprocessing complete",
	"OrderIdentifier": "INT-245d0301-5170-406c-abb7-750aadce9173-Orc 3570",
	"RedirectData": "[HTML FORM DATA TRUNCATED FOR BREVITY]",
	"SpiToken": "cq8gqlirt6ce2tmmphf09x5kxhndvh2zi25y7owm3m60fhy2l-iseenw5eb"
	}
	Observaciones:
	
	El script resaltado se auto postea. Es un script presente en la respuesta de Gestión de Riesgo, Autorización y Venta.
	
	• Será necesario desplegar el script resaltado en el navegador del tarjetahabiente.
	• Se recomienda incluir el script señalado arriba dentro de un iFrame.
	• Si el comercio utiliza la solución Página Alojada (HPP), será necesario incluir el nódulo de la página alojada. Si la solucuión HPP no se utiliza entonces se excluye el nódulo HPP.

7.3 Finalización del Pago

Para finalizar la etapa de pago de la transacción, los comercios deberán hacer un llamado a "/payment" pasando el *token* tipo SPI en una solicitud HTTP POST. PowerTranz enviará la transacción a la red de pagos adecuada y enviará respuesta al comercio. A continuación, se muestra ejemplo de un mensaje de respuesta JSON elaborado por PowerTranz. Tome en cuenta que la autorización (y por ende, la reducción del disponible en la cuenta del tarjetahabiente) no ocurre hasta que no se envíe el mensaje de finalización de pago. El resultado de la finalización del pago puede ser o bien un aprobado, un denegado o un error..

Solicitud	**Respuesta**

POST https://dev.ptranz.com/Api/spi/Payment HTTP/1.1
Host: staging.ptranz.com
Accept: text/plain
Solicitud-Id: |8f9d8e1f-482cd3595d7a08db.
Content-Type: application/json-patch+json
Content-Length: TBD
 	
"vftpo8xbb4l36v9d63wx74uejlsfui5btkjw4yv6v4ojbcw8k-iseenw5eb"
 	
Observaciones:
 	
En contenido del mensaje de solicitud consiste sencillamente del valor del SpiToken y no de JSON.
	{
	"TransactionType": 1,
	"Approved": true,
	"AuthorizationCode": "123456",
	"TransactionIdentifier": "12c37d56-07fe-4941-be69-026981fc1dc3",
	"TotalAmount": 1,
	"CurrencyCode": "978",
	"RRN": "125315159423",
	"CardBrand": "Visa",
	"IsoResponseCode": "00",
	"ResponseMessage": "Transacción is approved.",
	"PanToken": "1d3qljq1yt4dk6vagncxd07usvjr6p6sqeo78b36bed9ebh7u8",
	"OrderIdentifier": " 912b-43ef-a2ee-2c83d4bd59d4"
	}

7.4 Solicitud de Captura

Si la solicitud original fue enviada al *endpoint* de ventas y la transacción de finalización de pago devolvió aprobación (Código ISO de respuesta: "00"), entonces la transacción será procesada para su liquidación. Si por otra parte, la transacción fue enviada al *endpoint* de autorizaciones, entonces será necesario capturar la transacción para completar la venta y generar un cobro (por parte del emisor) al tarjetahabiente. Tenga en cuenta que existen *endpoints* adicionales de "Transaction Modification" los cuales pueden ser empleados para efectuar reembolsos y anulaciones.

Capture Solicitud	**Capture Respuesta**

POST https://dev.ptranz.com/Api/capture HTTP/1.1
Host: staging.ptranz.com
Accept: text/plain
PowerTranz-PowerTranzId: #PowerTranzPasswordId#
PowerTranz-PowerTranzPassword: #PowerTranzPassword#
Request-Id: |8f9d8e1f-482cd3595d7a08db.
Content-Type: application/json-patch+json
Content-Length: TBD
 	
{
"TransacciónIdentifier": "4f3fae73-b43a-4016-ae93-24f88d98e079",
"TotalAmount": 1,
 	
}
	{
	"OriginalTrxnIdentifier": "4f3fae73-b43a-4016-ae93-24f88d98e079",
	"TransactionType": 3,
	"Approved": true,
	"TransactionIdentifier": "4f3fae73-b43a-4016-ae93-24f88d98e079",
	"TotalAmount": 1,
	"CurrencyCode": "978",
	"RRN": "127011162582",
	"IsoResponseCode": "00",
	"ResponseMessage": "Transaction is approved",
	}

7.5 Solicitud de Reembolso

Solicitud

```
POST https://dev.ptranz.com/Api/refund HTTP/1.1
Host: dev.ptranz.com
Accept: text/plain
PowerTranz-PowerTranzId: #PowerTranzPasswordId#
PowerTranz-PowerTranzPassword: #PowerTranzPassword#
Solicitud-Id: |8f9d8e1f-482cd3595d7a08db.
Content-Type: application/json-patch+json
Content-Length: TBD

{
  "Refund": true,
  "TransactionIdentifier": "cab173a7-f75e-444b-ac42-
cc6a367b8b6b",
  "TotalAmount": 1,
  "CurrencyCode": "978",
  "Source": {
    "CardPresent": false,
    "CardEmvFallback": false,
    "ManualEntry": false,
    "Debit": false,
    "Contactless": false,
    "CardPan": "",
    "MaskedPan": ""
  },
  "TerminalCode": "",
  "TerminalSerialNumber": "",
  "AddressMatch": false
}
```

Respuesta

```
{
  "OriginalTrxnIdentifier": "cab173a7-f75e-444b-
ac42-cc6a367b8b6b",
  "TransactionType": 5,
  "Approved": true,
  "TransactionIdentifier": "0446a902-311d-4868-8247-
e9dfbd8ea0a6",
  "TotalAmount": 1,
  "CurrencyCode": "978",
  "RRN": "127013162598",
  "IsoResponseCode": "00",
  "ResponseMessage": "Transaction is approved",
  }
```

7.6 Solicitud de Anulación

Solicitud

```
POST https://dev.ptranz.com/Api/void HTTP/1.1
Host: dev.ptranz.com
Accept: text/plain
PowerTranz-PowerTranzId: #PowerTranzPasswordId#
PowerTranz-PowerTranzPassword: #PowerTranzPassword#
Request-Id: |8f9d8e1f-482cd3595d7a08db.
Content-Type: application/json-patch+json
Content-Length: TBD

{
  "TransactionIdentifier": "67a7689d-efe0-4a21-a3c3-
cd8b55d7825f",
  "ExternalIdentifier": "#ComercioGenerated#",
  "TerminalCode": "",
  "TerminalSerialNumber": "",
  "AutoReversal": false
}
```

Respuesta

```
{
  "OriginalTrxnIdentifier": "67a7689d-efe0-4a21-
a3c3-cd8b55d7825f",
  "TransactionType": 4,
  "Approved": true,
  "TransactionIdentifier": "67a7689d-efe0-4a21-a3c3-
cd8b55d7825f",
  "TotalAmount": 1,
  "CurrencyCode": "978",
  "RRN": "127011162583",
  "IsoResponseCode": "00",
  "ResponseMessage": "Transaction is approved",
  }
```

7.7 Solicitud de Tokenización

Solicitud	**Respuesta**

POST https://staging.ptranz.com/Api/RiskMgmt
HTTP/1.1
Accept: text/plain
PowerTranz-PowerTranzId: #PowerTranzPasswordId#
PowerTranz-PowerTranzPassword: #PowerTranzPassword#
Request-Id: |8f9d8e1f-482cd3595d7a08db.
Content-Type: application/json-patch+json
Content-Length: TBD
{
"TransactionIdentifier": "7b689a53-cc82-4456-98d6-5eb9faa1b0f0",
"TotalAmount": 0,
"CurrencyCode": "840",
"Tokenize": true,
"ThreeDSecure": false,
"Source": {
"CardPan": "5115010000000001",
"CardCvv": "123",
"CardExpiration": "2512",
"CardholderName": "John Doe"
},
"OrderIdentifier": "INT-95e75078-7d58-40e8-8053-c3d488f05f59-Orc 3569"
}
	{
	
	"TransactionType": 8,
	"Approved": false,
	"TransactionIdentifier": "7b689a53-cc82-4456-98d6-5eb9faa1b0f0”,
	"TotalAmount": 0.0,
	"CurrencyCode": "840",
	"CardBrand": " MasterCard",
	"IsoResponseCode": "TK0",
	"ResponseMessage": "Tokenize complete",
	"PanToken":
	"28zezcdudowtoepj685759opnt96g6eavzkgjetrg6czcl8ywn"
	,
	"OrderIdentifier": "INT-95e75078-7d58-40e8-8053-c3d488f05f59-Orc 3569"
	
	}

7.8 Solicitud de autorización con empleo de un token de Powertranz

Solicitud	**Respuesta**

POST #AuthUrl# HTTP/1.1
Accept: application/json
PowerTranz-PowerTranzId: #PowerTranzPasswordId#
PowerTranz-PowerTranzPassword: #PowerTranzPassword#
Content-Type: application/json; charset=utf-8
Host: staging.ptranz.com
Content-Length: TBD
Expect: 100-continue
Connection: Keep-Alive
{
"TransactionIdentifier": "5ee7d7c1-af78-4d7e-9386-abb280822b73",
"TotalAmount": 1,
"CurrencyCode": "978",
"ThreeDSecure": true,
"Source": {
"Token": "28zezcdudowtoepj685759opnt96g6eavzkgjetrg6czcl8ywn",
"CardCvv": "123",
"CardExpiration": "2512",
"CardholderName": "John Doe"
},
"OrderIdentifier": "INT-95e75078-7d58-40e8-8053-c3d488f05f59-Orc 3569",
"BillingAddress": {
"FirstName": "John",
"LastName": "Smith",
"Line1": "2608 Bergenline Ave.",
"Line2": "Unit 31",
"City": "Union City",
"State": "NJ",
"PostalCode": "07087",
"CountryCode": "840",
"EmailAddress": "john.smith@gmail.com",
"PhoneNumber": "201-869-0103"
},
"AddressMatch": false,
"ExtendedData": {
"ThreeDSecure": {
"ChallengeWindowSize": 4,
"ChallengeIndicator": "01"
},
"MerchantResponseUrl": https://localhost:5001/Final
}
}
	{
	"TransactionType": 1,
	"Approved": false,
	"TransactionIdentifier": "5ee7d7c1-af78-4d7e-9386-abb280822b73",
	"IsoResponseCode": "SP4",
	"ResponseMessage": "SPI Preprocessing complete",
	"OrderIdentifier": "INT-95e75078-7d58-40e8-8053-c3d488f05f59-Orc 3569",
	"RedirectData": "[FORMULARIO DE DATOS HTML RECORTADOS DEBIDO A ESPACIO LIMITADO]",
	"SpiToken": "vlf80fset61e73ml9toqu2kqtn5sddelqk9r7kao51kut6h3o-iseenw5eb"
	}
	Notas:
	El script que se resalta es de tipo que se “auto postea”, y se trata de un script que el sistema devuelve con las respuestas tipo **RiskMgmt, Auth** y **Sale.**
	• El script que se resalta deberá ser renderizado en el navegador del tarjetahabiente.
	• Se recomienda incluir el script en un iFrame.

7.9 Solicitud de autorización con empleo de un token de Sentry

Solicitud	**Respuesta**

POST #AuthUrl# HTTP/1.1
Accept: application/json
PowerTranz-PowerTranzId: #PowerTranzPasswordId#
PowerTranz-PowerTranzPassword: #PowerTranzPassword#
Content-Type: application/json; charset=utf-8
Host: staging.ptranz.com
Content-Length: TBD
Expect: 100-continue
Connection: Keep-Alive
{
"TransactionIdentifier": "5ee7d7c1-af78-4d7e-9386-abb280822b73",
"TotalAmount": 1,
"CurrencyCode": "978",
"ThreeDSecure": true,
"Source": {
"Token": "411111_000021111",
"TokenType": "PG2",
"CardCvv": "123",
"CardExpiration": "2512",
"CardholderName": "John Doe"
},
"OrderIdentifier": "INT-95e75078-7d58-40e8-8053-c3d488f05f59-Orc 3569",
"BillingAddress": {
"FirstName": "John",
"LastName": "Smith",
"Line1": "4200 Grant Ave.",
"Line2": "Unit 22",
"City": "Union City",
"State": "NJ",
"PostalCode": "07087",
"CountryCode": "840",
"EmailAddress": "john.smith@gmail.com",
"PhoneNumber": "201-864-6790"
},
"AddressMatch": false,
"ExtendedData": {
"ThreeDSecure": {
"ChallengeWindowSize": 4,
"ChallengeIndicator": "01"
},
"MerchantResponseUrl": https://localhost:5001/Final
}
}
	{
	"TransactionType": 1,
	"Approved": false,
	"TransactionIdentifier": "5ee7d7c1-af78-4d7e-9386-abb280822b73",
	"IsoResponseCode": "SP4",
	"ResponseMessage": "SPI Preprocessing complete",
	"OrderIdentifier": "INT-95e75078-7d58-40e8-8053-c3d488f05f59-Orc 3569",
	"RedirectData": "[HTML FORM DATA TRUNCATED FOR BREVITY]",
	"SpiToken": "vlf80fset61e73ml9toqu2kqtn5sddelqk9r7kao51kut6h3o-iseenw5eb"
	}
	Notas:
	El script resaltado se “auto postea” y el sistema lo devuelve con los mensajes RiskMgmt, Auth y Sale.
	• El script resaltado deberá ser renderizado en el navegador del tarjetahabiente.
	• Se recomienda incluir el script en un iFrame.

7.10 Solicitud de autorización y respuesta – FraudCheck y 3DS

Solicitud	**Respuesta**

POST #AuthUrl# HTTP/1.1
Accept: application/json
PowerTranz-PowerTranzId: #PowerTranzPasswordId#
PowerTranz-PowerTranzPassword: #PowerTranzPassword#
Content-Type: application/json; charset=utf-8
Host: staging.ptranz.com
Content-Length: TBD
Expect: 100-continue
Connection: Keep-Alive
{
"TransactionIdentifier": "5ee7d7c1-af78-4d7e-9386-abb280822b73",
"TotalAmount": 1.05,
"CurrencyCode": "978",
"ThreeDSecure": true,
"FraudCheck": true,
"Source": {
"CardPan": "5115010000000001",
"CardCvv": "",
"CardExpiration": "2512",
"CardholderName": "John Doe"
},
"OrderIdentifier": "INT-95e75078-7d58-40e8-8053-c3d488f05f59-Orc 3569",
"BillingAddress": {
"FirstName": "John",
"LastName": "Smith",
"Line1": "1200 Whitewall Blvd.",
"Line2": "Unit 15",
"City": "North Bergen",
"State": "NJ",
"PostalCode": "07047",
"CountryCode": "840",
"EmailAddress": "john.smith@gmail.com",
"PhoneNumber": "201-864-1234"
},
"AddressMatch": false,
"ExtendedData": {
"ThreeDSecure": {
"ChallengeWindowSize": 4,
"ChallengeIndicator": "01"
},
"MerchantResponseUrl": https://localhost:5001/Final
}
}
	{
	"TransactionType": 1,
	"Approved": false,
	"TransactionIdentifier": "5ee7d7c1-af78-4d7e-9386-abb280822b73",
	"IsoResponseCode": "SP4",
	"ResponseMessage": "SPI Preprocessing complete",
	"OrderIdentifier": "INT-95e75078-7d58-40e8-8053-c3d488f05f59-Orc 3569",
	"RedirectData": "[HTML FORM DATA TRUNCATED FOR BREVITY]",
	"SpiToken": "vlf80fset61e73ml9toqu2kqtn5sddelqk9r7kao51kut6h3o-iseenw5eb"
	}
	
	Notas:
	El script resaltado se “auto postea” y el sistema lo devuelve con los mensajes RiskMgmt, Auth y Sale.
	• El script resaltado deberá ser renderizado en el navegador del tarjetahabiente.
	• Se recomienda incluir el script en un iFrame.

Respuesta final a la autorización – FraudCheck y 3DS

Solicitud	**Respuesta**
	{ "TransactionType": 1, "Approved": false, "TransactionIdentifier": "5ee7d7c1-af78-4d7e-9386-abb280822b73", "TotalAmount": 1.05, "CurrencyCode": "978", "CardBrand": "MasterCard", "IsoResponseCode": "3D0", "ResponseMessage": "3DS complete", "RiskManagement": { "ThreeDSecure": { "Eci": "02", "Xid": "f6e851ee-b3d8-4d7d-98cb-62f0eec39e42", "Cavv": "AJkBCQIGIlYplVGQaQaIAAAAAAA=", "AuthenticationStatus": "Y", "ProtocolVersion": "2.1.0", "FingerprintIndicator": "U", "DsTransId": "94c7d18b-b18a-4fdb-810f-bcbe513d9b25", "ResponseCode": "3D0" }, "FraudCheck": { "FcProvider": "Kount", "ResponseCode": "FC0", "FcResponseCode": "A", "FcScore": "33", "FcTransId": "K9WC08BB7J9W", "FcDetails": { "ErrorCode": "0", "Version": "0695", "Mode": "Q", "TransactionId": "K9WC08BB7J9W", "MerchantId": "240000", "SessionId": "bccd03e020704e5fbda6f8d4abb29aeb", "OrderNumber": "INT-95e75078-7d58-40e8-8053-c3d4", "Auto": "R", "Score": "33", "Geox": "US", "Brand": "MSTR", "Velo": "0", "Vmax": "0", "Network": "A", "Kaptcha": "Y", "Proxy": "N", "Emails": "1", "HttpCountry": "US", "TimeZone": "180", "Cards": "1", "PcRemote": "N", "Devices": "1", "DeviceLayers": "2D5332442A..23EA1C3E4B.88292C253E.DB16B1D428", "MobileForwarder": "N", "VoiceDevice": "N", "LocalTime": "2022-09-16 10:48", "FingerPrint":"89E3933F0D384718B1FE447AD311E34B",

	Powertranz Simplified 3DS Integration v2.6
	27
	"Flash": "N",
	"Language": "EN",
	"Country": "BM",
	"Cookies": "Y",
	"MobileDevice": "N",
	"Site": "DEFAULT",
	"IPAddress": "199.172.239.242",
	"IPAddressLatitude": "32.3201",
	"IPAddressLongitude": "-64.7376",
	"IPAddressCountry": "BM",
	"IPAddressRegion": "Hamilton",
	"IPAddressCity": "Hamilton",
	"IPAddressOrganization": "Internet Bermuda Limited",
	"DateDeviceFirstSeen": "2022-09-15",
	"UserAgentString": "Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36",
	"DeviceScreenResolution": "1080x1920",
	"OS": "Windows 8"
	}
	}
	},
	"PanToken": "140k2o9m2rztv8hw61vi43qxqc6nccn0fnaazi78fvmtsukliv",
	"OrderIdentifier": "INT-95e75078-7d58-40e8-8053-c3d488f05f59-Orc 3569",
	"SpiToken": "23rawin3ot3w882np3wdlafzrlykgigs8dq20xskhyo1d47v0e-iseenw5eb"
	};

7.11 Solicitud y respuesta de la verificación de fraude *Fraud Check*

Solicitud de Administración de Riesgo	**Respuesta inicial**

POST https://staging.ptranz.com/Api/RiskMgmt
HTTP/1.1
Accept: application/json
PowerTranz-PowerTranzId: #PowerTranzPasswordId#
PowerTranz-PowerTranzPassword: #PowerTranzPassword#
Content-Type: application/json; charset=utf-8
Host: staging.ptranz.com
Content-Length: TBD
Expect: 100-continue
Connection: Keep-Alive
{
"TransactionIdentifier": "5ee7d7c1-af78-4d7e-9386-abb280822b73",
"TotalAmount": 10.50,
"CurrencyCode": "978",
"ThreeDSecure": false,
"FraudCheck": true,
"Source": {
"CardPan": "5115010000000001",
"CardCvv": "",
"CardExpiration": "2512",
"CardholderName": "John Doe"
},
"OrderIdentifier": "INT-95e75078-7d58-40e8-8053-c3d488f05f59-Orc 3569",
"BillingAddress": {
"FirstName": "John",
"LastName": "Smith",
"Line1": "1166 Ave. of the Americas",
"Line2": "Suite 915",
"City": "NY",
"State": "NY",
"PostalCode": "10036",
"CountryCode": "840",
"EmailAddress": "john.smith@gmail.com",
"PhoneNumber": "212-395-5000"
},
"AddressMatch": false,
"ExtendedData": {
"ThreeDSecure": {
"ChallengeWindowSize": 4,
"ChallengeIndicator": "01"
},
"MerchantResponseUrl": "https://localhost:5001/Final"
	{
	"TransactionType": 8,
	"Approved": false,
	"TransactionIdentifier": "5ee7d7c1-af78-4d7e-9386-abb280822b73",
	"IsoResponseCode": "SP4",
	"ResponseMessage": "SPI Preprocessing complete",
	"OrderIdentifier": "INT-95e75078-7d58-40e8-8053-c3d488f05f59-Orc 3569",
	"RedirectData": "[HTML FORM DATA TRUNCATED FOR BREVITY]",
	"SpiToken": "vlf80fset61e73ml9toqu2kqtn5sddelqk9r7kao51kut6h3o-iseenw5eb"
	}
	Notas:
	El script resaltado se “auto postea” y el sistema lo devuelve con los mensajes RiskMgmt, Auth y Sale.
	• El script resaltado deberá ser renderizado en el navegador del tarjetahabiente.
	• Se recomienda incluir el script en un iFrame.

Respuesta de la verificación de fraude *Fraud Check*

Solicitud de Administración de Riesgo	**Respuesta final**

	{
	"TransactionType": 8,
	"Approved": false,
	"TransactionIdentifier": "5ee7d7c1-af78-4d7e-9386-abb280822b73",
	"TotalAmount": 10.50,
	"CurrencyCode": "978",
	"CardBrand": "MasterCard",
	"IsoResponseCode": "FC0",
	"ResponseMessage": "Fraud check complete",
	"RiskManagement": {
	"FraudCheck": {
	"FcProvider": "Kount",
	"ResponseCode": "FC0",
	"FcResponseCode": "R",
	"FcScore": "31",
	"FcTransId": "K9WC0LWXW0K1",
	"FcDetails": {
	"ErrorCode": "0",
	"Version": "0695",
	"Mode": "Q",
	"TransactionId": "K9WC0LWXW0K1",
	"MerchantId": "240000",
	"SessionId": "7b475c5776ad43fab448046d1c712a05",
	"OrderNumber": "INT-95e75078-7d58-40e8-8053-c3d4)",
	"Auto": "R",
	"Score": "31",
	"Geox": "US",
	"Brand": "MSTR",
	"Velo": "0",
	"Vmax": "0",
	"Network": "A",
	"Kaptcha": "Y",
	"Proxy": "N",
	"Emails": "1",
	"HttpCountry": "US",
	"TimeZone": "180",
	"Cards": "1",
	"PcRemote": "N",
	"Devices": "1",
	"DeviceLayers": "2D5332442A..23EA1C3E4B.88292C253E.DB16B1D428",
	"MobileForwarder": "N",
	"VoiceDevice": "N",
	"LocalTime": "2022-09-16 10:57",
	"FingerPrint":"89E3933F0D384718B1FE447AD311E34B",
	"Flash": "N",
	"Language": "EN",
	"Country": "BM",
	"Cookies": "Y",
	"MobileDevice": "N",
	"Site": "DEFAULT",
	"IPAddress": "199.172.239.242",
	"IPAddressLatitude": "32.3201",
	"IPAddressLongitude": "-64.7376",
	"IPAddressCountry": "BM",

	"IPAddressRegion": "Hamilton",
	"IPAddressCity": "Hamilton",
	"IPAddressOrganization": "Internet Bermuda Limited",
	"DateDeviceFirstSeen": "2022-09-15",
	"UserAgentString": "Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36",
	"DeviceScreenResolution": "1080x1920",
	"OS": "Windows 8"
	}
	}
	}
	"OrderIdentifier": " INT-95e75078-7d58-40e8-8053-c3d488f05f59-Orc 3569)",
	"SpiToken":
	"2t2jkdww6vzpxed77wbnxqrufvigxuyuyfu8ightt7cjit0qeh-iseenw5eb"
	};

8. Parámetros del Mensaje de Respuesta de PowerTranz

Como mostrado en los ejemplos anteriores, existen dos juegos de códigos de respuesta que el comercio deberá analizar para determinar sus próximos pasos.

La respuesta inicial a la solicitud de Autorización, Venta o Gestión de Riesgo devuelve al comercio el resultado de la autenticación 3DS .

8.1 Códigos de Respuesta de Autenticación 3DS

PowerTranz genera el código de respuesta 3DS que indica el status de la autenticación 3DS.
Note que “3D0” indica que el proceso concluyó con éxito sin embargo es necesario analizar los resultados detalladamente, para decidir si enviar o no la finalización del pago. Además, existen reglas que cada comercio define para determinar si se efectúa una finalización del pago según en los resultados de la autenticación 3DS.

Código de Respuesta	Respuesta 3DS	Descripción	Observaciones
3D0	Autenticación completada	3DS completado	Procesos 3DS1 y 3DS2 completados
3D1	Autenticación no disponible	No se apoya 3DS para este tipo de tarjeta	Proceso de Pre-autenticación completado
3D3	Error de autenticación	Error 3DS	Error 3DS1 o 3DS2

Ejemplo dentro de la respuesta de autenticación:

```
"IsoRespuestaCode": "3D0",
  "RespuestaMessage": "3D-Secure complete",
```

8.2 Resultado de una Autenticación 3DS

El objeto interno ThreeDSecure en la respuesta de autenticación muestra el resultado de una autenticación 3DS. Los comercios deberán interpretar el valor de campos importantes y decidir si proceder o no a la finalización del pago.

8.3 Status de una Autenticación 3DS

La tabla a continuación muestra los valores posibles generados por una autenticación y sus significados. Si el status de la autenticación es N (no autenticado) el sistema no permitirá finalización de pago.

Nota. Los campos AuthenticationStatus, ECI Indicator y IsoResponseCode indican el resultado de la autenticación.

Valor	Descripción
Y	Autenticación o verificación de cuenta fructífera
A	Se intentó realizar autenticación
N	No se autenticó/la cuenta no se verificó; transacción denegada
U	No se pudo procesar la autenticación/verificación de cuenta debido a problemas técnicos o de otro tipo
R	Autenticación/ verificación de cuenta rechazada por el emisor, el cual solicita no se efectúe solicitud de autorización

Cuando se cuestiona al tarjetahabiente la respuesta solamente indicará Y (Sí) o N (No.)

8.4 Valores del Campo ECI

El valor que lleva el campo ECI (Electronic Commerce Indicator) lo definen las redes de las marcas e indica el resultado de una solicitud de autenticación 3DS.

a) Esto son los valores indicados por American Express y Visa:
   - ECI 05: Autenticación 3DS fructífera.
   - ECI 06: Se intentó realizar autenticación 3DS.
   - ECI 07: La autenticación 3DS fracasó o no estaba disponible. La transacción se considera no 3DS.

b) A continuación, los valores indicados por MasterCard:
   - ECI 02: Autenticación 3DS fructífera.
   - ECI 01: Se intentó realizar autenticación 3DS.
   - ECI 00: La autenticación 3DS fracasó o no estaba disponible. La transacción se considera no 3DS.
   - ECI N2: La autenticación 3DS fue fructífera para una transacción tipo NPA
   - ECI N0: La autenticación 3DS fracasó para una transacción tipo NPA

Advertencia. El campo ECI no siempre indicará un valor. Todo depende del resultado de la autenticación.

8.5 Resultados de Transacción *Status Reason*

En casos donde la autenticación 3DS fracasa (status N), es posible que el comercio reciba informes adicionales en el campo StatusReason.

Valor	Descripción	Valor	Descripción
01	Autenticación de la tarjeta fracasó	**11**	Se sospecha fraude
02	Dispositivo desconocido	**12**	Transacción no permitida al tarjetahabiente
03	Dispositivo no apoyado	**13**	Tarjetahabiente no inscrito al servicio
04	Excede límite de frecuencia de autenticación	**17**	Alto nivel de confianza
05	Tarjeta caducada	**18**	Muy alto nivel de confianza
06	Número de tarjeta inválido	**19**	Excede no. máximo de interrogaciones
07	Transacción inválida	**20**	No se apoya transacción no relacionada con un pago
08	No existe registro para la tarjeta	**21**	No se apoya transacción 3RI
09	Fracaso de seguridad	**19**	Exceeds ACS maximum challenges
10	Tarjeta robada	**22-79**	Reservados para uso futuro: estos valores se consideran inválidos hasta que EMVCo los habilite.

9. Consideraciones Especiales

9.1 Marcas de Tarjetas no aptas para 3DS

Transacciones con marcas que en la actualidad no apoyan 3DS (JCB, Discover, Diners) pueden fluir de la misma forma que aquellas que sí lo apoyan mediante el Método Simplificado de Integración, ya sea a través de la página alojada (HPP) o del esquema convencional. En lugar de recibir el resultado 3DS, el comercio recibirá la respuesta “3D1”, lo cual indica que 3DS no se apoya. El comercio entonces puede decidir si avanzar o no a finalización del pago.

Como alternativa, se pueden enviar solicitudes para estas marcas como “no 3DS” mediante el siguiente *endpoint* del método completo en vez del método simplificado:

https://*TBD*.ptranz.com/api/<endpoint>

Nota. El código 3D1 también será enviado como respuesta en los siguientes casos:

- Cuando el adquirente no soporta 3DS2 para la marca de la tarjeta
- Si 3DS1 no se soporta para la tarjeta

9.2 Identificadores de Transacciones y Pedidos/Órdenes

PowerTranz requiere que toda transacción generada por el comercio lleve valores únicos en los campos **TransacciónIdentifier** y **OrderIdentifier**.

El campo **TransactonIdentifier** tiene formato GUID (*Global Unique Identifier* o Identificador Único Universal) y representa el número de identidad único de PowerTranz.

El campo **OrderIdentifier** es uno de los valores utilizados en los reportes del Portal de Administración del Comercio, y deberá llevar un valor único para cada transacción aprobada.

9.3 Datos de Tarjetahabiente ante 3DS 2

Aunque solo el nombre del tarjetahabiente es mandatorio para las transacciones 3DS2, se recomienda que el comercio incluya tantos elementos como sea posibles relacionados con el domicilio donde el tarjetahabiente recibe su estado de cuenta.

El servidor de autenticación del emisor decide si cuestionar o no al tarjetahabiente, basado en varios factores que incluyen datos suministrados en el mensaje de solicitud. Información adicional suministrada por el comercio sin duda asiste a un manejo más fluido de la solicitud de autenticación.

Vale la pena recalcar que para transacciones 3DS2, el nombre del comercio indicado en el mensaje de solicitud deberá corresponder exactamente al nombre que se indica en la solicitud de autorización.

Para transacciones solo de autenticación 3DS, donde la solicitud de autorización se envía posteriormente por separado, el comercio está a cargo de enviar su nombre de forma consistente en los dos mensajes.

9.4 Validación de Datos

El protocolo 3DS para EMV (tarjetas con chip) emplea el juego de caracteres ISO 8859. Si los parámetros de una solicitud de autenticación 3DS (como por ejemplo nombre o domicilio del tarjetahabiente) se elaboran de acuerdo a un juego de caracteres no soportado, la solicitud de autenticación fracasará.

Juego de Caracteres Comunes

La tabla a continuación muestra los caracteres comunes dentro de la especificación ISO/IEC 8859.

				b8	0	0	0	0	0	0	0	0
				b7	0	0	0	0	1	1	1	1
				b6	0	0	1	1	0	0	1	1
				b5	0	1	0	1	0	1	0	1
b4	b3	b2	b1		00	01	02	03	04	05	06	07
0	0	0	0	00			SP	0	@	P	`	p
0	0	0	1	01			!	1	A	Q	a	q
0	0	1	0	02			"	2	B	R	b	r
0	0	1	1	03			#	3	C	S	c	s
0	1	0	0	04			$	4	D	T	d	t
0	1	0	1	05			%	5	E	U	e	u
0	1	1	0	06			&	6	F	V	f	v
0	1	1	1	07			'	7	G	W	g	w
1	0	0	0	08			(	8	H	X	h	x
1	0	0	1	09			)	9	I	Y	i	y
1	0	1	0	10			*	:	J	Z	j	z
1	0	1	1	11			+	;	K	[	k	{
1	1	0	0	12			,	<	L	\	l	|
1	1	0	1	13			-	=	M	]	m	}
1	1	0	0	14			.	>	N	^	n	~
1	1	1	1	15			/	?	O	_	o	

9.5 Tokenización

Se emplea el *endpoint* de *Risk Management* (Manejo de Riesgos) para obtener el token que corresponde a la tarjeta. Este token puede emplearse para efectuar transacciones de carácter financiero.
Si la tarjeta ha caducado, es necesario efectuar una nueva solicitud de token para actualizar la fecha de expiración de la tarjeta.

Es necesario utilizar *TokenType* solo en aquellos casos cuando se emplea un token originalmente definido via Sentry, es decir, la versión antigua de la pasarela FAC. En casos así, Ud. deberá enviar un valor de "PG2" en el campo *TokenType*.

Un token también será incluido en el mensaje de respuesta de transacciones de carácter financiero si así lo desea el comercio. Por favor contacte al equipo de soporte de FAC (BACSoporte@fac.bm) para obtener información sobre cómp habilitar la presencia de un token en los mensajes de respuesta de transacciones de carácter financiero.

Tenga en cuenta que es posible efectuar una autenticación 3DSecure como parte de la solicitud inicial de un token. Esto se obtiene si se emplea el *endpoint* de Manejo de Riesgos (*RiskMgmt*) y se coloca el valor *true* al indicador *ThreeDSecure*, como por ejemplo, cuando Ud. agrega una tarjeta al monedero y efectúa una autenticación 3DSecure:

"TotalAmount": 0.0,
"ChallengeIndicator": "04",
"AuthenticationIndicator":"04",
"MessageCategory":"02" (Si no se indica MessageCAtegory, por defecto tomará el valor "02" si TotalAmount es cero o no se incluye.

MessageCategory 02 se emplea en transacciones tipo NPA (autenticación no relacionada con un pago).

Esto no constituye una transacción de pago. Se trata de una transacción que solo efectuará una validación del status de la tarjeta.

9.6 Verificación de Fraude

La función Verificación de Fraude de Powertranz utiliza Kount™, una solución de prevención de fraudes de una empresa externa que cuenta con las más altas calificaciones en la industria de medios de pago. Para emplear Kount, es necesario que además de su cuenta con Powertranz, el comercio tenga una cuenta con Kount. Por favor contactar al grupo de soporte de Powertranz si Ud. desea obtener el servicio.

Verificación de Fraude ofrece la siguiente Funcionalidad:

- La solicitud a Kount puede enviarse independientemente, mediante el *endpoint* spi/RiskMgmt, o puede formar parte de una transacción de carácter financiero mediante los *endpoints* spi/auth o spi/sale.
- Se puede combinar la solicitud a Kount con una solicitud 3DS, colocando 'true' en los indicadores ThreeDSecure y FraudCheck en una solicitud dirigida al *endpoint* de Administración de Riesgos, o como parte de una transacción de caráter financiero dirigida hacia el *endpoint* spi/auth o spi/sale.
- Se puede enviar la solicitud a Kount desde unba página alojada (HPP) con o sin autenticación 3DS.

El código de respuesta en el objeto FraudCheck (Verificación de Fraude) muestra el resultado de la solicitud Kount. Una solicitud de Kount completada tendrá una respuesta de FC0. Si ocurren un error por exceso de tiempo, esto será reflejado en FraudCheck.ResponseCode así como en la tabla de errores titualda Errors.o en general durante el proceso de Kount, vendrán reflejados en el campo FraudCheck.ResponseCode y en la matriz de detalles Errors.

La autenticación 3DS se lleva a cabo si el campo FCResponseCode no indica D (Denegada) y el indicador ThreeDSecure en la petición inicial porta el valor 'true'. El resultado de la autenticación determina si es posible avanzar a la finalización de pago (si la solicitud inicial se envió a los *endpoints* spi/auth o spi/sale). Los posibles resultados de la autenticación se detallan en la Sección 8.

Si la solicitud de Kount se realizó combinada con una solicitud 3DS pero el proceso de Kount expiró o generó error, la autenticación 3DS será procesada, y el resultado de la misma estará disponible en el objeto ThreeDSecure.

Cabe mencionar que errores debidos a exceso de tiempo ("time out") son posibles en las respuestas ThreeDSecure y FraudCheck.

Si se ha completado una evaluación de Kount, el objeto FcDetails devolverá información más detallada sobre la transacción. Esta información también está disponible al comercio en el portal de Kount.

10. Cuentas y Casos de Prueba

Existen dos flujos de proceso 3DS: **fluido** y **con desafío**. En el proceso fluido, no ocurre cuando un diálogo con el tarjetahabiente durante la autenticación. El proceso con desafío conlleva una redirección del navegador del tarjetahabiente al servidor del emisor, para permitir que se efectúen los cuestionamientos necesarios para completar la autenticación.

El servidor del emisor de la tarjeta establece si verificación del dispositivo del tarjetahabiente es necesaria. Esta verificación es conocida como *fingerprinting* en inglés. En la gran mayoría de los casos, el dispositivo es el navegador del tarjetahabiente durante la sesión de compra ecommerce. Esta verificación puede ocurrir como parte de ambos flujos de procesamiento, es decir fluido y con desafío.

Las cuentas de tarjetas de pruebas generan resultados preestablecidos de autenticación y autorización. **Note que el uso de tarjetas marcadas "con desafío" requiere el ingreso de la contraseña indicada en la tabla.**

Advertencia: Estas cuentas no funcionan en el ambiente productivo.

Caso	Cuenta de tarjeta	Versión 3DS	Contra seña	Observaciones
Los siguientes casos producen transacciones aprobadas				
V2-01-YA	4012000000020071	2.1.0		Flujo fluido, Authentication Status=Y
V2-02-AA	4012000000020089	2.1.0		Flujo fluido, Authentication Status=A
M2-01-YA	5100270000000023	2.1.0		Flujo fluido, Authentication Status=Y
M2-02-RA	5100270000000072	2.1.0		Flujo fluido, Authentication Status=R
V2-03-YA	4012000000020006	2.1.0	3ds2	Con desafío, Authentication Status=Y
M2-03-YA	5100270000000031	2.1.0	3ds2	Con desafío, Authentication Status=Y
V2-04-YA	4012010000020070	2.1.0		Flujo fluido, Fingerprinting, Authentication Status=Y
V2-05-AA	4012010000020088	2.1.0		Flujo fluido, Fingerprinting, Auth. Status=A
M2-04-YA	5100271000000120	2.1.0		Flujo fluido, Fingerprinting, Auth. Status=Y
V2-06-YA	4012010000020005	2.1.0	3ds2	Con desafío, Fingerprinting, Auth. Status=Y
V2-07-YA	4012000000020071	2.1.0	3ds2	Con desafío, incluye ChallengeIndicator = 03
A2-01-YA *	341111000000009	2.1.0		Flujo fluido, Status=Y
A2-02-AA	341111000000011	2.1.0		Flujo fluido, Authentication Status=A
A2-03-YA	341112000000001	2.1.0	3ds2	Con desafío, Fingerprinting, Authentication Status=Y
A2-04-YA	341111000000037	2.1.0	3ds2	Con desafío, Authentication Status=Y
A2-05-YA	341112000008012	2.1.0		Flujo fluido, Fingerprinting, Authentication Status=Y
DS-01-0A	6011111111111111	n/a		Discover
JC-01-0A	3528111111111108	n/a		JCB
M1-01-YA	5115010000000018	1.0.2		Authentication Status=U, 3DS1 con retroceso

Los siguientes casos producen denegaciones				
V2-01-ND	4012000000020121	2.1.0		Flujo fluido, Authentication Status=N, Finalización del Pago no permitida (código de respuesta 12)
M2-01-ND	5100270000000098	2.1.0		Flujo fluido, Authentication Status=N, Finalización del Pago no permitida (código de respuesta 12)
M2-02-ND	5100270000000056	2.1.0		Con desafío, Authentication Status=N, Finalización del Pago no permitida (código de respuesta 12)
V2-02-AD	4666666666662222	2.1.0		Flujo fluido, Status = A, Código de Respuesta ISO = 05, Respuesta CVV = N
M2-03-UD	5555666666662222	2.1.0		Flujo fluido, Authentication Status=U, Código de Respuesta ISO = 05
V2-03-AD	4111111111119999	2.1.0		Flujo fluido, Status = A, Código de Respuesta ISO = 98
M2-04-AD	5111111111113333	2.1.0		Flujo fluido, Status = A, Código de Respuesta ISO = 05
V2-04-YD	4111111111110000	2.1.0	3ds2	Con desafío, Status =Y, Código ISO de Respuesta = 91
M2-05-YD	5111111111110000	2.10	3ds2	Con desafío, Status =Y, Código ISO de Respuesta = 91
A2-01-ND	341111000000029	2.1.0		Flujo fluido, Authentication Status=N
DS-01-0D	6011111111111152	n/a		Discover
JC-01-0D	3528111111111157	n/a		JCB

* Por favor confirme con un representante de Soporte PowerTranz si AMEX 3DS se apoya para su cuenta.

Apéndice 1 – Códigos de Respuesta

Códigos de Respuesta PowerTranz e Información de Errores

Transacciones aprobadas o transacciones completadas

Cód. Resp.s ISO	Mensaje de Respuesta	Detalles Adicionales
00	Aprobación	Se devuelve para transacciones de carácter financiero
3D0	Autenticación 3DSecure completada	Se completó la transacción sin errores
3D1	No se soporta 3DS	Los métodos de autenticación 3DS1 o 3DS2 no se soportan para esta tarjeta
HP0	Preprocesamiento para página alojada completo	
TK0	Tokenización completada	
SP4	Prepocesamiento SP4 completado	
FC0	Proceso Fraud Check completado	El proceso completó sin errores

Mensajes de error

Cuando el mensaje de respuesta indica un campo inválido, Ud. deberá revisar la Sección 5 para determinar el formato permitido de ese campo. Por ejemplo, el campo “CardholderName” (nombre del tarjetahabiente) solo permite los caracteres indicados en la Sección 9.4.

Código ISO de Respuesta	Código de Respuesta	Mensaje de Respuesta	Detalles del Error
FC3		Error en Fraud Check	Error en el proceso de Fraud Check
03	310	Comercio inválido	
05	22	Transacción denegada	Denegación genérica
12	75	Error SPI	Error SPI
12	76	Transacción Inválida	Transacción SPI Inválida
12	315	Tarjeta o moneda inválida	Tarjeta o moneda inválida
12	320	Transacción Inválida	Transacción de prueba Inválida
12	321	Error de procesamiento	Error de procesamiento
12	326	Transacción inválida	Campo inválido del interfaz con el Host: {nombre del campo}
12	330	Transacción inválida	No se permite {nombre del campo}
12	343	Transacción inválida	Comercio inválido
12	344	Transacción inválida	Comercio cerrado/cancelado
12	345	Transacción inválida	Parámetros de pago deshabilitados
12	354	Transacción inválida	Error criptográfico
12	361	Transacción Inválida	Invalid transacción
12	362	Transacción Inválida	Invalid transacción
12	370	Transacción no concuerda	Transacción no concuerda en el simulador de pruebas
12	380	Transacción inválida	Autorización original inválida
12	381	Transacción inválida	No se encontró autorización original
12	382	Transacción inválida	Monto inválido de la autorización original
12	383	Transacción inválida	Monto inválido
12	384	Transacción inválida	Reembolso inválido

Código ISO de Respuesta	Código de Respuesta	Mensaje de Respuesta	Detalles del Error
12	386	Transacción inválida	Transacción clausurada
12	387	Transacción duplicada	No. de ID de la transacción duplicado
12	426	Transacción Inválida	Campo inválido del interfaz con el Host: {nombre del campo}
12	546	Error 3DS1	Retroceso a 3D1 no permitido
12	757	Transacción Inválida	No se encontró Página Alojada
12	758	Error en la Página Alojada	Página Alojada Inválida
3D0		3D-Secure finalizado	
3D1		No soporta 3DS	No se soporta 3DS para este tipo de tarjeta
3D3	519	Error 3DS1	Error en el resultado de verificación: {nombre del campo}
3D3	611	Error del sistema	Preautenticación fracasó
3D3	618	Error sistema 3DS1	Error de verificación de inscripción
3D3	619	Error sistema 3DS1	Error de verificación de resultado
3D3	540	Error 3DS2	Error de autenticación
3D3	640	Error sistema 3DS2	Error de autenticación
3D3	518	Error 3DS1	Error en la verificación de inscripción: {Nombre del Campo}
3D3	520	Error 3DS1	No se pudo armar el PAREq
3D3	511	3DS error	Preautenticación fracasó
3D3	532	3DS error	Autenticación fracasó
3D3	444	Error sistema 3DS2	Error general 3DS
3D3	541	Error 3DS2	Error en el custionamiento
3D3	641	Error sistema 3DS2	Error en el custionamiento
3D3	542	Error 3DS2	Error en el resultado
3D3	642	Error sistema 3DS2	Error en el resultado
3D3	543	Error 3DS2	Error en la notificación
3D3	643	Error sistema 3DS2	Error 3DS2 en la notificación
3D3	544	Error sistema 3DS2	Error 3DS2 ID del dispositivo
3D3	550	Error 3DS2	Error DS
3D3	548	Error 3DS	Error de comunicación DS
3D3	551	Error 3DS2	Servidor 3DS inalcanzable
3D3	549	Error 3DS	Error de Cache
3D3	649	Error sistema 3DS2	Error de Cache
3D3	510	Error 3DS	Parámetro 3DS inválido: {Nombre del Campo
57	316	Tipo de tarjeta inválido	Tipo de tarjeta inválido
89	312	Autenticación fracasó	Credenciales inválidas
91	329	Host comms error	Host not available
91	391	*Timeout* del Host	Tiempo de respuesta se agotó
91	392	Error de comunicación del Host	Error de comunicación del Host
96	424	Error de sistema	Error de comunicación interno
96	44	Error de sistema	Error general del GateApi

Código ISO de Respuesta	Código de Respuesta	Mensaje de Respuesta	Detalles del Error
96	432	Error de sistema	Acción no indicada: {Nombre del campo }
96	459	Error de sistema	Error de persistencia
96	460	Error de sistema	Mapeo de la tarjeta
96	85	Error de sistema	Error de sistema SPI
96	850	Error de sistema	Error de sistema HPP
96	325	Error de procesamiento del host	Error de procesamiento del host
96	332	Error de sistema	Ruta no indicada
96	317	Error de sistema	“Timeout” interno
96	353	Error de sistema	“TLV parse” fracasó
96	332	Error de sistema	Ruta no indicada
96	49	Error de sistema	Error no determinado: {Nombre del Campo
96	610	3DS Error de sistema	Falta parámetro 3DS: {Nombre del Campo
96	456	Error de sistema	Gestión de Riesgos no disponible
96	457	Error de sistema	Error general: Gestión de Riesgos
96	458	Error de sistema	Ruta inválida
96	45	Error de sistema	Error de API general
96	450	Error de sistema	Error de puerto general
96	451	Error de sistema	Error general del procesador
96	452	Error de sistema	General processor error
96	453	Error de sistema	“TLV parse” fracasó
96	455	Error de sistema	El API no funciona
96	417	Error de sistema	“Timeout” interno
96	42	Error de sistema	Puerto indisponible
96	421	Error de sistemas	Errores múltiples
96	422	Error de procesamiento del Host	Error en el interfaz del host
96	425	Error de procesamiento del Host	Error de procesamiento del Host
96	43	Error de sistema	Error de ruta interno
96	431	Error de sistema	Error de una regla
96	433	Error de sistema	Ruta inválida
97	36	Solicitud fracasó validación	Solicitud inválida
97	37	Solicitud fracasó validación	Campo(s) falta(n): {Nombre del Campo
97	38	Solicitud fracasó validación	Campo inválido: {Nombre del Campo
97	57	Solicitud fracasó validación	Campo 3DS falta: {Nombre del Campo
97	58	Solicitud fracasó validación	Campo 3DS inválido: {Nombre del Campo
98	428	Error de sistema	Error del interfaz del host
99	441	Error de sistema	Error de código de respuesta
99	490	Error general	Error general
99	390	Error general	Error general
99	327	Error comunicación del host	Error PL

Códigos de Respuesta ISO

Código de Respuesta y Descripción	Código de Respuesta y Descripción
00 Approbada	53 Cuenta de ahorro no existe
01 Referir al emisor	54 Tarjeta caducada
02 Referir al emisor (caso especial)	55 PIN Incorrecto
03 Comercio inválido	56 No existe regitro de la tarjeta
04 Retenga tarjeta	57 Transacción no permitida a la tarjeta
05 No honre/no acepte	58 Transacción no permitida a la tarjeta
06 Error	59 Sospecha de fraude
07 Retenga tarjeta (caso especial)	60 Comercio debe contactar adquirente
08 Acepte con confirmación de la identidad del t/h	61 Excede límite de retiro
09 Solicitud en marcha	62 Tarjeta restringida
10 Aprobada para monto parcial	63 Violación de seguridad
11 Aprobación VIP	64 Monto original incorrecto
12 Transacción inválida	65 Excedió conteo límite de actividad
13 Monto inválido	66 Comercio debe contactar adquirente
14 No. de cuenta no existe	67 Retenga tarjeta en cajero automático
15 Emisor no existe	68 Respuesta se recibió demasiado tarde
16 Approbada, actualice pista # 3	75 Intentos con PIN incorrecto excedió límite
17 Cancelación por parte del cliente	76 No se ubicó mensaje anterior
18 Disputa del cliente	77 Datos no concuerdan con mensaje original
19 Re-ingrese transacción	80 Fecha inválida
20 Respuesta inválida	81 Error de criptografía en el PIN
21 No se tomó acción ninguna	82 CVV Incorrecto
22 Se sospecha mal funcionamiento	83 Imposible verificar el PIN
23 Cargo por transacción no se acepta	84 Ciclo de autorización inválida
24 Receptor no soporta actualización de archivo	85 No hay razón para denegar
25 Imposible ubicar registro	86 Imposible validar PIN
26 Registro actualización de archivo duplicado	88 Fracasó proceso criptográfico
27 Error en un campo al actualizar archivo	89 Fracaso de Autenticación
28 Archivo temporalmente indisponible	90 Proceso de cierre en marcha
29 Actualización de archivo fracasó	91 Emisor o servidor indisponible
30 Error de formato	92 Ruta no disponible
31 Emisor no disponible	93 Violación de ley
32 Completada parcialmente	94 Transmisión duplicada
33 Tarjeta caducada	95 Error de conciliación
34 Sospecha de fraude	96 Mal funcionamiento del sistema
35 Comercio debe contactar adquirente	97 Error de formato
36 Tarjeta restringida	98 Host inalcanzable
37 Comercio debe contactar adquirente	99 Error de la transacción
38 Excedió límite de intentos de ingresar PIN	N0 STIP Forzoso
39 No se ubicó cuenta de crédito	N3 Servicio de efectivo indisponible
40 Función no soportada	N4 Solicitud de efectivo excede límite del emisor
41 Retenga tarjeta (tarjeta perdida)	N7 Denegada por CVV2 incorrecto
42 No existe cuenta universal	P2 Datos del facturador inválidos
43 Retenga tarjeta (tarjeta robada)	P5 Solicitud de actualización de PIN denegada
44 No existe cuenta de inversionismo	P6 PIN de insuficiente seguridad
51 Insuficiencia de fondos	XA Enviar al emisor
52 No existe cuenta corriente (de cheques)	XD Enviar al emisor

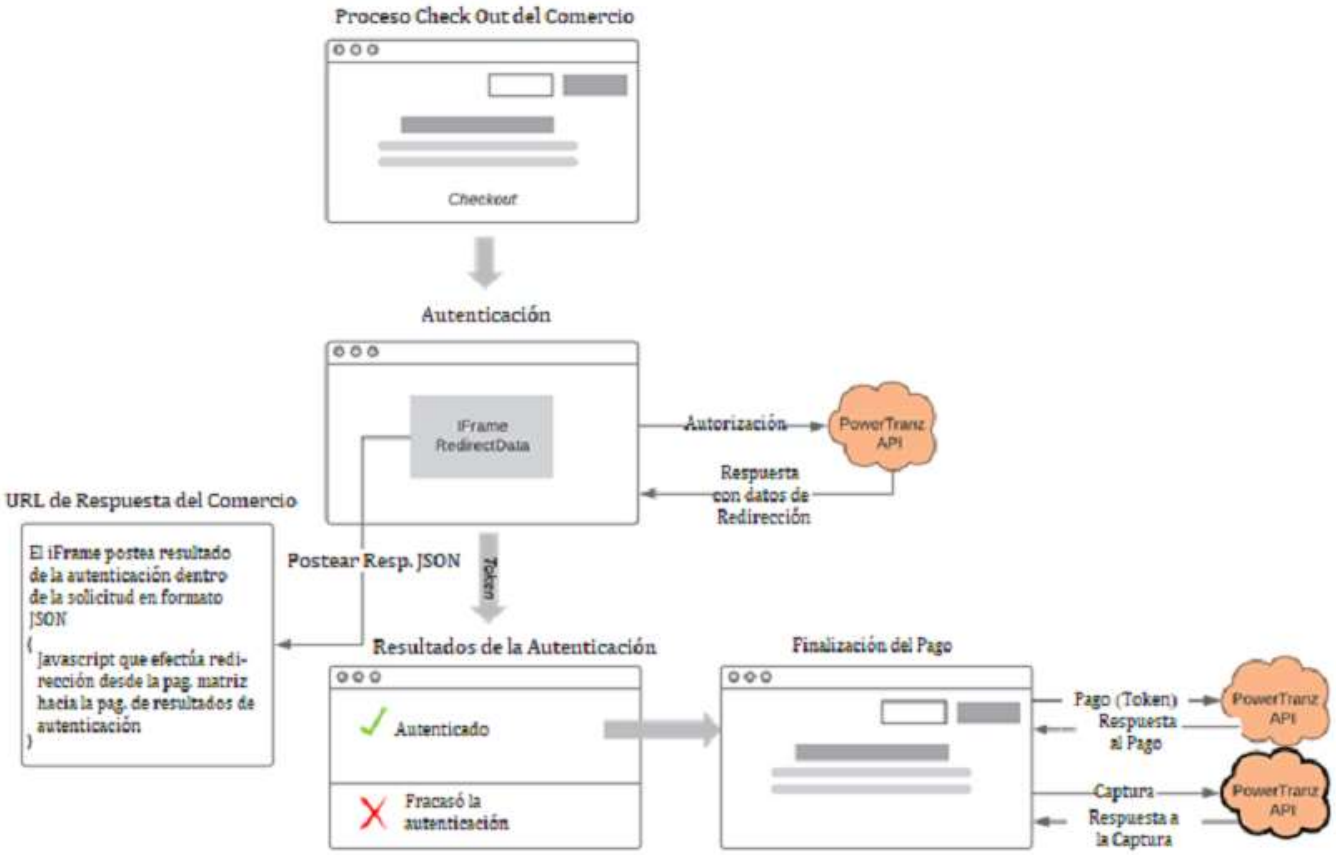
Códigos de Respuesta CVV2

Código	Definición
M	Concuerda
N	No concuerda
P	No se procesó
S	Debería aparerecer en la tarjeta pero no se suministró (Visa unicamente)
U	Emisor no participa o no está certificado

Apéndice 2 – Ejemplos de Codificación

Ejemplo de Integración de un Comercio

Dada la variedad de integraciones posibles (ejemplos: SPA Web App, MVC Application, etc.) no es posible brindar ejmplos de todas en este documento. A continuación se muestra ejemplo de una integración del API de PowerTranz a una aplicación web de un comercio, que emplea una arquitectura MVC (*Model* [Modelo], *View* [Visión], *Controller* [Controlador]) bajo OpenAPI para generar un Cliente HTTP Client y un Modelo.



1. Proceso Check Out
   El aplicativo del comercio recolecta los datos del tarjetahabiente y los postea al proceso de Autenticación.
2. Proceso de Autenticación utilizando un iFrame
   El aplicativo del comercio envía una solicitud de autorización al Endpoint de autorizaciones, devolviendo la respuesta al proceso de Autenticación. Este proceso incluye un iFrame al cual los datos de redirección (RedirectData) estarán acoplados.
   - PowerTranz End Point: {PowerTranz URL raíz}/api/spi/auth
   - Contenido de la Solicitud: Solicitud de Autorización
   - El atributo AuthSolicitud.ExtendedData.ComercioRespuestaUrl deberá incluir URI en el dominio del aplicativo del comercio, al cual el iFrame posteará la respuesta del proceso de Autenticación.
   - Respuesta: Respuesta del proceso de Autorización, que incluye código ISO de respuesta (IsoResponseCode) and los datos de redirección (RedirectData) –se trata de un formulario HTML el cual será ejecutado dentro del contexto del Iframe.

- AuthResponse.RedirectData se inyecta en o acopla al iFrame. Ejemplo:

```
<div class="text-center">
       <h4 class="display-4">IFrame</h4>
       <iframe id="threedsIframe" ref="threedsIframe" srcdoc="@Model.RedirectData">
       </iframe>
</div>
```

1) Iframe
   Una vez que los datos de redirección (RedirectData) han sido acoplados al iFrame, el proceso continuará dentro del contexto del iFrame.
   - A continuación, el tarjetahabiente podrá ser cuestionado con el propósito de agregar mayores detalles de autenticación. Entonces un formulario será desplegado en el iFrame para que el tarjetahabiente ingrese detalles adicionales. Cuando el tarjetahabiente suministra datos adicionales, el iFrame posteará los resultados de la Autenticación directamente al URL de respuesta.
   - Alternativamente, si datos adicionales del tarjetahabiente no son necesarios (flujo fluido), el contexto del iFrame será posteado del resultado de la autenticación directamente al URL de respuesta del comercio.
   - En ambos casos (Flujo Fluido y Cuestionamiento), los resultados de la autenticación serán posteados al URL de respuesta del comercio.

2) URL de respuesta del comercio y eliminación del iFrame
   - El URL de respuesta del comercio es una página que se ubica dentro del dominio del aplicativo del comercio.
   - El contexto del iFrame se encarga de postear el resultado de la the autenticación a esta página. Su ciclo de vida será bien corto y no visible desde el navegador del tarjetahabiente.
   - Esta página contiene el JavaScript que re direcciona el contenedor matriz del iFrame al resultado Autenticación, lo cual elimina el iFrame y devuelve control al aplicativo del comercio. Ejemplo:

```
<script>

    window.onload = redirectParent;

    function redirectParent() {
        window.parent.location = './AutenticaciónResult';
    }

</script>
```

3) Resultado de Proceso de Autenticación
   Este paso maneja los resultados de la autenticación. Si la autenticación es fructífera, el aplicativo del comercio continua procesando hacia la finalización del pago.
4) Proceso de Finalización del Pago

El aplicativo del comercio puede entonces hacer llamados a los *endpoints* siguientes, como por ejemplo Pago, Captura y/o Anulación.

Apéndice 3 – Detalles del control de fraude

Parámetro	P/C	Formato	Longitud Max/Valor	Description
FcDetails	C			Datos suministrados por Kount
Version	C	AN	4	No. de la versión de Kount
Mode	C	AN	1	U (valor constante)
TransactionId	C	AN	12	No. de identidad de la transacción de Kount
MerchantID	C	N		No. de Identidad asignado al comercio por Kount
SessionId	C	AN	32	No. único de sesión
OrderNumber	C	AN	32	No. del pedido que genera el comercio
Auto	C	AN	1	Código de respuesta que refleja la decisión: - A – Aprobada - D – Denegada - R – Revisar - E – Referir a supervisor
Score	C	N		Puntaje de Kount
Geox	C	AN	2	País relacionado con el puntaje "Persona" de Kount con la mayor probabilidad de fraude
Brand	C	AN	4	Marca de la tarjeta
Velo	C	N		Cantidad de pedidos registrados por "Persona durante los últimos 14 días
Vmax	C	N		Cantidad de pedidos según "Persona" " en el más activo intervalo de 6 horas durante los últimos 14 días
Network	C	AN	1	Tipo de red de mayor riesgo según "Persona" durante los últimos 14 días - A – Anónimo - H – *High School* (bachillerato) - L – Biblioteca - N – Normal - O – Proxy abierta - P – Prisión - S - Satélite
Kapcha	C	Bool		Indica si los datos del dispositivo fueron recopilados por el proceso de Colección de Datos
Proxy	C	Bool		Indica si un servidor proxy fue detectado en este pedido
Emails	C	N		Cantidad de direcciones email distintos vinculados con "Persona" según Kount
HttpCountry	C	AN	2	País de domicilio que el dueño ha definido en el panel de control del dispositivo
TimeZone	C	AN	6	El huso horario el dueño ha definido en el panel de control del dispositivo. Indica la cantidad de minutos a partir de GMT. Divídase entre 60 para obtener horas,
Cards	C	N		Cantidad de tarjetas de crédito relacionadas con "Persona" según Kount
PcRemote	C	BOOL		Indica si el dispositivo está habilitado para emplear software PC Remote
Devices	C	N		Cantidad de dispositivos relacionados con "Persona" según Kount

DeviceLayers	C	AN	55	5 capas del dispositivo que representan el sistema operativo, navegador, parámetros de Javascript, parámetros de cookies, y parámetros de flash. Las capas del dispositivo se utilizan para crear las huellas digitales (*fingerprinting*) del dispositivo
MobileForwarder	C	BOOL		Si se trate de un dispositivo móvil, este indicador muestra si se emplea substituto (*forwarder*) para procesar los servicios del proveedor de señal telefónica
VoiceDevice	C	BOOL		Indica si el dispositivo se activa por voz
LocalTime	C	AN	20	Hora local definida por el dueño en el panel de control del dispositivo
FingerPrint	C	AN	32	La huella digital del dispositivo que hace el pedido
Flash	C	BOOL		Este indicador muestra si el dispositivo que hace el pedido tiene 'Flash' habilitado
Language	C	AN	2	Idioma definido por el dueño en el panel de control del dispositivo
Country	C	AN	2	Código ISO del país del dispositivo físico
Cookies	C	BOOL		Indica si el dispositivo que hace el pedido tiene *cookies* habilitadas
MobileDevice	C	BOOL		Indica si el dispositivo que hace el pedido es de carácter móvil: iPhone, Android, Blackberry, iPad, etc.
Site	C	AN	8	Identifica el sitio web o el no. del comercio donde el pedido se originó
IPAddress	C	N		Dirección IP proxy
IPAddressLatitude	C	N		Latitud de la dirección IP proxy
IPAddressLongitude	C	N		Longitud de la dirección IP proxy
IPAddressCountry	C	AN	2	País de la dirección IP proxy
IPAddressRegion	C	AN	2	Estado/Provincia de la dirección IP proxy
IPAddressCity	C	AN	255	Ciudad de la dirección IP proxy
IPAddressOrganization	C	AN	64	Propietario de la dirección IP
DateDeviceFirstSeen	C	AN	10	Fecha de la primera vez que el dispositivo fue detectado
UserAgentString	C	AN	1024	Trama del agente del usuario
DeviceScreenResolution	C	AN	10	Resolución de la pantalla del dispositivo
OS	C	AN	64	Sistema operativo
ErrorCode	C	AN		Código de error indicado por Kount
Browser	C	AN	64	Navegador
JavaScript	C	BOOL		Indica si el dispositivo que hace el pedido tiene Javascript habilitado
MobileType	C	AN	32	iPhone, Android, iPad, etc.
PiercedIPAddress	C	N		Dirección IP *pierced*
PiercedIPAddressLatitude	C	N		Latitud de la dirección IP *pierced*
PiercedIPAddressLongitude	C	N		Longitud de la dirección IP *pierced*
PiercedIPAddressCountry	C	AN	2	País de la dirección IP *pierced*
PiercedIPAddressRegion	C	AN	2	Estado/provincia de la dirección IP *pierced*
PiercedIPAddressCity	C	AN	255	Ciudad de la dirección IP *pierced*
PiercedIPAddressOrganization	C	AN	64	Propietario de la dirección IP *pierced*
ReasonCode	C	AN	16	Cód. de razón de a la acción definida en la(s) regla(s)
Region	C	AN	2	Región donde se ubica el dispositivo