Ecommerce API Guide v2.1

Integración 3DS Hibrida

Enero 12, 2022

Contents

Bitácora de Actualizaciones

Versión del Documento	Descripción	Fecha
2.1	Versión inicial	Jan 15, 2022

1. Introducción

Este documento es una guía para desarrolladores con el fin de integrar el procesamiento de pagos de PowerTranz en el sitio web de un comercio. Esta guía de integración cubre el método de integración híbrido 3DS para transacciones de comercio electrónico 3DS con o sin utilizar una página de pago alojada.

1.1 Por qué y cuándo se necesita la integración híbrida para 3DS 2.x

La integración híbrida para 3DS 2.x es necesaria para los comercios que requieren el uso de características o funcionalidades que actualmente no están disponibles en la API de Powertranz.

Algunos de los comercios de Credomatic Bank requieren procesar Puntos o Impuestos como parte de sus integraciones. Para estos casos, se requerirá la integración híbrida ya que la funcionalidad de Puntos, Impuestos y Kount de Credomatic no se puede proporcionar a través de la api de Powertranz, estas solo se puede proporcionar a través de la api de FACPG2-Sentry.

2. Comercio electrónico con 3D-Secure Descripción general

El portal PowerTranz es compatible con las versiones 2.x de EMV 3D-Secure con fallback a la versión 1.0 de 3DS para la autenticación del titular de la tarjeta si fuera necesario; y envía solicitudes financieras (Autorización, Venta, Reembolso o Anulación) a las redes de pago a través de la plataforma FACPG2-Sentry (integración híbrida).

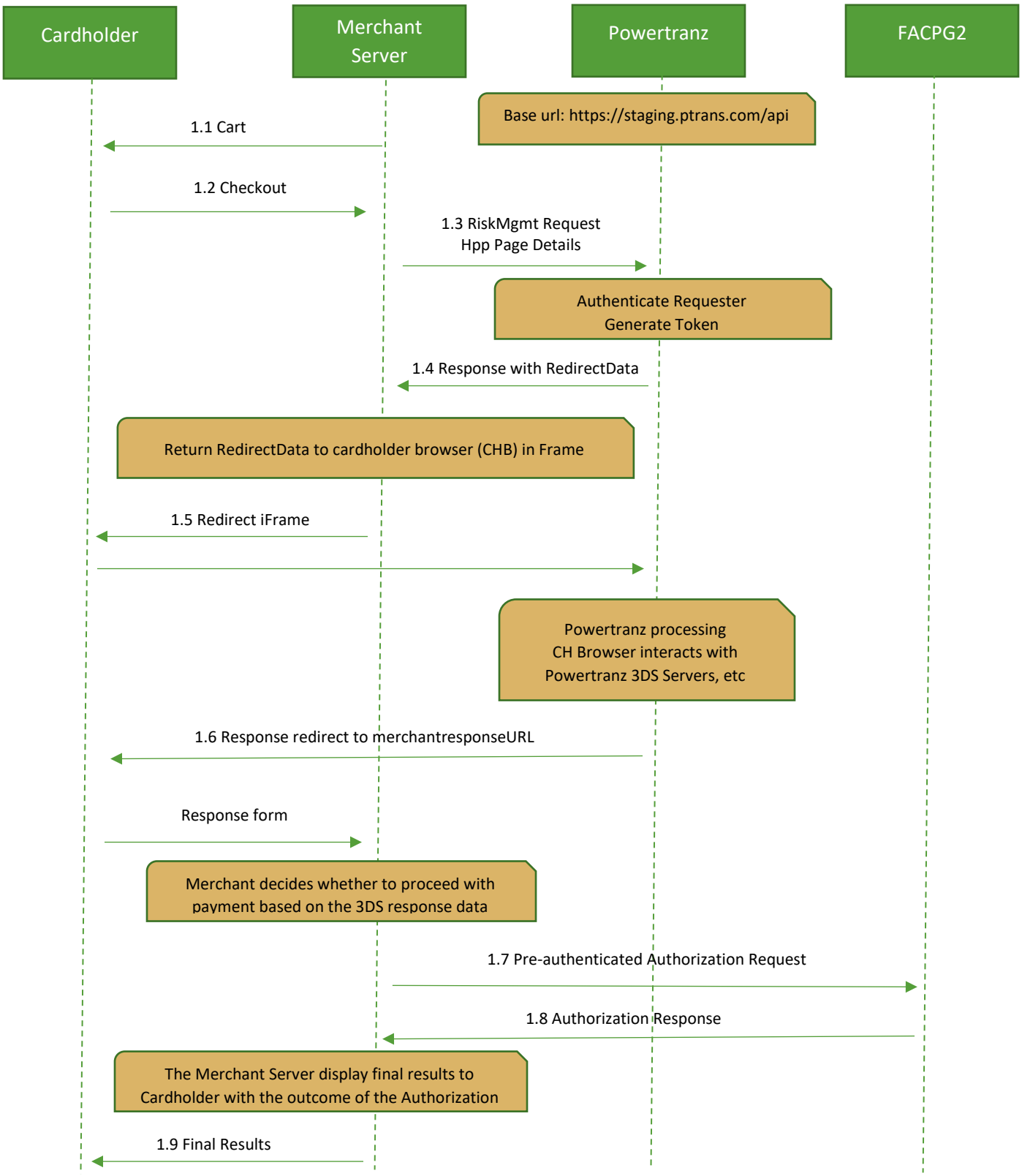
La plataforma FACPG2-Sentry es una plataforma de procesamiento de transacciones con todas las funciones que FAC ha estado utilizando durante más de 15 años.

Powertranz y FACPG2-SENTRY pueden interactuar entre sí a través de esta integración híbrida que se ha desarrollado específicamente para transacciones 3DS 2.x. Como mencionamos en la sección anterior, esta integración híbrida se ofrece como una solución de corto a mediano plazo hasta que se certifique una integración directa entre Powertranz y Credomatic con todas las características requeridas.

Una solicitud de 3D-Secure se inicia mediante el método de la API **RiskMgmt** con el indicador 3D-Secure activado. PowerTranz consultará la versión compatible de 3D-Secure según el número de tarjeta proporcionado y las capacidades del banco emisor. El método de integración 3DS híbrido simplificado manejará las interacciones requeridas para una autenticación 3DS 2.0 que puede ser sin fricciones, incluir huellas dactilares del dispositivo, un flujo de desafío o si 3DS 2.0 no es compatible, entonces un intento de fallback a la versión 1.0 de 3DS

Con este método de integración, habrá una autenticación previa seguida de una finalización del pago según el resultado de la autenticación previa. La información de pago se envía directamente desde la página de pago del comercio o la página de pago alojada (HPP) de PowerTranz. La parte de autenticación de la transacción es procesada de forma transparente por el servidor PowerTranz que notificará al comercio con el resultado de la autenticación 3D-Secure. Luego, el comercio decidirá (según el resultado de la autenticación) si procede con la solicitud financiera a través de la plataforma FACPG2-SENTRY.

2.1 Diagrama simplificado de integración híbrida de 3DS 2.x



2.2 Flujo de proceso de alto nivel de integración híbrida 3DS 2.x simplificado

Fase de autenticación 3DS

El servidor web del comercio muestra el carrito de compras final al titular de la tarjeta.

1.2 El titular de la tarjeta realiza el check-out.

1.3 Según el método de integración utilizado:

a. El comercio captura la información de pago del titular de la tarjeta y envía una solicitud de RiskMgmt (que incluye el titular de la tarjeta relevante y los detalles de pago) con la bandera 3DS habilitada al servidor PowerTranz;

b. O bien, el comercio envía una solicitud de RiskMgmt al servidor PowerTranz que incluye una página alojada y un nombre donde se recopilarán los datos del titular de la tarjeta y del pago correspondientes en la página alojada.

1.4 PowerTranz autentica la solicitud proveniente del comercio, genera un token y responde al servidor del comercio con datos de redirección.

1.5 Los datos de redirección están contenidos en la respuesta del extremo de RiskMgmt. contiene un formulario HTML con JavaScript que, cuando el comercio la inyecta en un iFrame, mostrará la página alojada (HPP) si se usa, o bien mostrara un flujo de Challenge (captura y validación de credenciales del tarjetahabiente) si lo requiere el banco emisor. Durante esta etapa, el iFrame en el navegador del titular de la tarjeta interactúa con PowerTranz y los servidores 3DS requeridos según el tipo de autenticación 3DS requerida. Esto podría ser un flujo totalmente sin fricciones o el titular de la tarjeta podría enfrentar un desafío (Challenge) durante este tiempo. Cuando se completa, el iFrame se redirige a MerchantResponseUrl y la aplicación Merchant reanuda el control del flujo. Ver ejemplo de código en el Apéndice.

1.6 PowerTranz responde con el resultado de la autenticación 3DS al servidor del comercio a través del navegador del titular de la tarjeta. Tenga en cuenta que esto no es una transacción financiera y es el resultado de la autenticación 3DS solamente.

Fase de Autorización (Transacción Financiera)

1.7 Según el resultado de la autenticación 3DS, el comercio determina si desea proceder con una Autorización de pago. Si el comercio opta por continuar con la transacción, deberá enviar la autorización de pago a la plataforma FACPG2-SENTRY utilizando la información de autenticación obtenida en la fase anterior. Luego, la solicitud de autorización se envía desde el servidor FACPG2-Sentry al procesador y luego al banco emisor.

1.8 FACPG2-SENTRY devuelve la respuesta de pago de Autorización al servidor del comercio.

1.9 El servidor del comercio luego muestra los resultados en el navegador del titular de la tarjeta. Si el comercio originalmente llamó a una Venta, la transacción financiera ahora está completa y luego, luego de la liquidación (controlada por FACPG2-Sentry), se facturará al titular de la tarjeta y se acreditará la cuenta del comercio. Si el comercio solicitó una Autorización, habrá una retención de fondos, pero se debe enviar una Captura cuando el comercio esté listo para finalizar la transacción y facturar al titular de la tarjeta.

2.3 Llamadas a la API del comercio: detalles adicionales

Dentro de la implementación 3DS 2.x híbrida simplificada, el comercio realizará varias llamadas a los puntos finales en las API de PowerTranz y FACPG2-Sentry. La primera solicitud (RiskMgmt) iniciará el proceso de autenticación y devolverá la información de autenticación de 3DS, que se utilizará en solicitudes posteriores a la API de FACPG2-SENTRY, tales como Autorización. Otras solicitudes posteriores a la API de FACPG2-Sentry se pueden realizar mediante "Captura", "Reversión" y "Reembolso" a través de puntos finales de Modificación de transacción para completar o cancelar la transacción según sea necesario.

Llamadas en Powertranz:

- Durante la llamada de RiskMgmt, el comercio debe pasar "MerchantResponseURL", que es el punto final del servidor del comercio al que PowerTranz enviará el resultado de autenticación final.
- Las llamadas a la API de PowerTranz se realizan mediante REST con JSON sobre HTTPS como protocolo de transporte.
- Las direcciones URL BASE accesibles externamente para los terminales PowerTranz SPI/HPP son:

Staging: https://staging.ptranz.com/api/spi/RiskMgmt
Prod: https://TBD.ptranz.com/api/spi/RiskMgmt

Llamadas en FACPG2-Sentry:

- Los comercios pueden posteriormente "Autorizar", "Capturar", "Revertir" o "Reembolsar" una transacción Autenticada con éxito a través de la operación TransactionModification. Las URL base externas para estos puntos finales son:

Interface	Environment	Url
SOAP	Test	https://ecm.firstatlanticcommerce.com/PGService/<Service Name>
SOAP	Prod	https://marlin.firstatlanticcommerce.com/PGService/<Service Name>
XML	Test	https://ecm.firstatlanticcommerce.com/PGServiceXML
XML	Prod	https://marlin.firstatlanticcommerce.com/PGServiceXML

Nombres de los Servicios

```
// Services.svc:
AuthorizeResponse Authorize(AuthorizeRequest Request)
TransactionModificationResponse TransactionModification(TransactionModificationRequest Request)
```

(para obtener una lista completa de las operaciones admitidas, consulte la guía de integración rápida FACPG2-SENTRY)

3. Endpoints y Operaciones de PowerTranz

PowerTranz expone para esta integración un conjunto de endpoints no financieros para el procesamiento de transacciones comerciales. La siguiente tabla muestra los puntos finales con una breve descripción de su uso y su URL.

Endpoint	Descripción	Tipo	Método	URL
Alive	Status de la pasarela	No financiero	GET	<API Root>/api/alive
RiskMgmt (Manejo de Riesgos)	Transacción de carácter no financiero. Empléese para pre-autenticar transacción tipo solo 3DS.	No Financiero	POST	<API Root>/api/spi/riskmgmt

4. Requisitos del encabezado de solicitud de PowerTranz

Todas las solicitudes a los puntos finales son solicitudes HTTP POST sobre TLS con cargas JSON en el cuerpo. Es obligatorio que el encabezado http incluya parámetros de autenticación del comercio (por ejemplo, PowerTranzId y contraseña).

La Powertranz-GatewayKey debe ser proporcionada por FAC y es un valor específico para cada banco adquirente (host) que se utiliza.

Los comercios deben llamar a los puntos finales de la API de PowerTranz mediante 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 de solicitud: RiskMgmt (autenticación 3DS)

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

Parámetro	M/O/C	Formato	Longitud Máx/Valor	Descripción
TransactionIdentifier (Identificador de transacción)	M	GUID (trama)	36	Identificador único asignado por el aplicativo del comercio Ejemplo : f62c3e58-1983-4165-8535-fe5bb6ba6127
TotalAmount (Monto total)	M	DEC	18,3	Monto total según autenticación
CurrencyCode (Código de moneda)	M	N	4	Deberá utilizarse el código numérico (ISO 4217)
ThreeDSecure	M	BOOL		
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
OrderIdentifier (No. de Pedido)	M	AN	2**55**	No. de Pedido asignado por el comercio
BillingAddress (Domicilio del tarjeta-habiente)				Objeto interior requerido (consultar Subjuego de Datos abajo)
FirstName (Nombre)	O	AN	30	Nombre (Para autenticación con 3DS, el campo CardholderName deberá estar relleno en el objeto fuente)
LastName (Apellido)	O	AN	30	Apellido (Para autenticación con 3DS, el campo CardholderName deberá estar relleno en el objeto fuente)
Line1 (Línea 1)	O	AN	30	Domicilio – Línea 1 (mandatorio para AVS)
Line2 (Línea 2)	O	AN	50	Domicilio – Línea 2
City (Ciudad)	O	AN	25	Ciudad
County (País)	O	AN	25	País
State (Estado o Provincia)	O	AN	25	Según el standard ISO 3166-2.
PostalCode (Código Postal)	O	AN	10	Código Postal (mandatorio para AVS)
CountryCode (Código del País)	C	AN	3	Código numérico de país según ISO 3166. Debe estar relleno si se indica Estado.
EmailAddress (Dirección email)	O	AN	50	Dirección email

PhoneNumber (Teléfono)	O	AN	20	Teléfono. Si no se sumninistra será del campo BilltoCountry. Ejemplos: +35301176543210 35301176543210 01176543210 (deberá incluir Cádigo del País)
PhoneNumber2 (Teléfono 2)	O	AN	20	No. del móvil (ver reglas de validación arriba)
PhoneNumber3 (Teléfono 3)	O	AN	20	Teléfono (trabajo) (ver reglas de validación arriba)
ShippingAddress (Dirección de entrega)				Objeto interior opcional (consultar Subjuego de Datos abajo). Se utiliza la misma validación del campo BillingAddress.
FirstName (Nombre)	O	AN	30	Nombre (para autentica-ción 3DS). El campo CardholderName deberá deberá ir relleno en objeto fuente.
LastName (Apellido)	O	AN	30	Apellido para autentica-ción 3DS). El campo CardholderName deberá ir relleno en objeto fuente.
Line1 (Línea 1)	O	AN	30	Domicilio Línea 1 (mandatorio para AVS)
Line2 (Línea 2)	O	AN	50	Domicilio Línea 12
City (Ciudad)	O	AN	25	Ciudad
County (País)	O	AN	25	País
State (Estado/Provincia)	O	AN	25	Estado o Provincia
PostalCode (Código Postal)	O	AN	10	Código Postal mandatorio para AVS)
CountryCode (Código del País)	O	AN	3	Deberá consistir de código numer. válido (ISO 4217)
EmailAddress (Dirección email)	O	AN	50	Dirección email
PhoneNumber (Teléfono)	O	AN	20	Teléfono (domicilio)
PhoneNumber2 (Teléfono 2)	O	AN	20	Teléfono (móvil)
PhoneNumber3 (Teléfono 3)	O	AN	20	Teléfono (trabajo)
AddressMatch (Concordancia de domicilios)	O	BOOL		'true' si domicilio de envío concuerda con domicilio a donde se envía el estado de cuenta
ExtendedData (Datos adicionales)				Objeto interior requerido
ThreeDSecure				Objeto interior requerido (consultar Subjuego de Datos abajo)
ChallengeWindowSize (Dimensiones del panel de solicitud 3DS **que se le presenta al tarjetahabiente**)	M	AN	1	Dimensiones preferidas por el comercio del panel de solicitud 3DS 1 – 250 x 400 2 – 390x400 3 – 500x600 4 – 600x400

				5 – 100%
MerchantResponseURL	M	AN	255	URL de Respuesta definido por el comercio
ChallengeIndicator (Indicador de solicitud al t/h)	O	N	2	Valor condicional (si lo maneja el comercio) 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).
HostedPage (Página Alojada)				Objeto interno dentro de ExtendedData (consultar Subjuego de Datos abajo) si se emplea una Página Alojada
PageSet	O	AN	50	PageSet de la Página Alojada
PageName	O	AN	50	PageName de la Página Alojada

6. Parámetros de Respuesta

(P)resente, (C)ondicional

Parámetro	P/C	Formato	Longitud Máx/Valor	Descripción
TransacciónType (Tipo de transacción)	P	numérico	2	Tipo de Transacción (1-Autorización, 2-Venta, 3-Captura, 4-Anulación, 5-Reembolso)
Approved (Aprobado)	P	BOOLEANA		Status de la transacción
AutorizaciónCode (Código de Autorización)	C	AN	6	Código de Autorización
TransacciónIdentifier (Identificador de la Transacción)	P	GUID (trama)	36	Identificador único asignado por el aplicativo del comercio Ejemplo: f62c3e58-1983-4165-8535-fe5bb6ba6127
TotalAmount (Monto Total)	P	DEC	18,3	Monto de la transacción procesada
CurrencyCode (Código de Moneda)	P	N	3	Moneda de transacción
CardBrand (Marca de Tarjeta)	P	AN	255	Marca de la tarjeta
IsoResponseCode (Código ISO de Respuesta)	P	AN	3	Código que indica aprobación, denegación o falla
ResponseMessage (Mensaje de Respuesta)	P	AN	255	Descripción de la respuesta según el Código Iso de Respuesta
RRN	P	string	12	No. de Rastreo

OriginalTrxnIdentifier (Identificador de Transacción Original)	C	GUID (trama)	36	Identificador de la transacción original comunicada en la respuesta a Captura, Reembolso o Anulación
RiskManagement				(Gestión de Riesgo)
CvvResponseCode	C			Resultado de verificación del CVV2
ThreeDSecure	P	BOOLEANA		
Eci	C	AN	2	Se indica si Status de la Autenticación = Y o A
Cavv	C	AN	100	Se indica si Status de la Autenticación = Y o A
Xid	P	AN	100	Identificador de la transacción 3DS
AuthenticationStatus	P	AN	1	Las posibles respuestas aparecen aquí: 3DS Autenticación Results
Token	P	AN	100	Se utiliza en procesos de autenticación 3DS1 and 3DS2
RedirectData (Datos de redirección)	C	Formulario HTML		Contiene el 12ormulation de redirección que se envía al navegador del t/h ante códigos de respuesta 3D4,3D5,3D6
AuthenticateUrl	C	AN	100	Mandatorio para Autenticaciones 3DS2 cuando se utilice “device fingerprinting” (identificación del dispositivo)
CardEnrolled	P	AN	1	Status del proceso de inscripción de la tarjeta
ProtocolVersion	P	AN	8	Versión del protocol 3DS manejado por el emisor
FingerprintIndicator	C	AN	1	Status de identificación del dispositivo. Valores posibles: U, Y o N
StatusReason	C	AN	2	Suministra la razón por la cual el campo AuthenticationStatus indica N, U o R. Las respuestas posibles aparecen aquí: StatusReason
DsTransID	P	AN	36	Identificador universal único asignado por el servidor del directorio que identifica transacciones individuales.
CardholderInfo	C	AN	255	Datos adicionales opcionalmente suministrados al t/h por el emisor
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. Ejemplos de solicitudes de RiskMgmt de PowerTranz 3DS2

7.1 Solicitud de RiskMgmt: página de pago del comercio

El siguiente ejemplo de Json corresponde al flujo RIskMgmt que un Comercio puede implementar utilizando su propia página de pago o la página de pago alojada (HPP).

7.2 Solicitud de RiskMgmt: página de pago alojada

El siguiente ejemplo de Json corresponde al flujo de RIskMgmt que un comercio puede implementar en la página de pago alojada (HPP).

Auth Request	**Auth Response**

POST #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": 1,
"CurrencyCode": "978",
"ThreeDSecure": true,
"OrderIdentifier": "INT-95e75078-7d58-40e8-8053-c3d488f05f59-Orc 3569",
"AddressMatch": false,
"ExtendedData": {
"ThreeDSecure": {
"ChallengeWindowSize": 4,
"ChallengeIndicator": "01"
},
"HostedPage": {
"PageSet": "PageSet",
"PageName": "PageName"
},
"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 es un script de publicación automática, se devuelve en la respuesta de **RiskMgmt.**
	
	• La secuencia de comandos resaltada deberá representarse en el Navegador de titulares de tarjetas.
	• Se recomienda incluir el script mencionado anteriormente en un iFrame.

Browser's iFrame redirections	**Final 3DS Authentication Response**

iFrame
 	
iFrame – Redireccion desde el Servidor a 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": "NY",
	"PostalCode": "200341",
	"CountryCode": "840",
	"EmailAddress": "john.smith@gmail.com",
	"PhoneNumber": "211-345-6790"
	}
	}

8. Parámetros de respuesta de PowerTranz RiskMgmt (autenticación)

Como se muestra en los ejemplos de códigos anteriores, hay dos conjuntos distintos de códigos de respuesta que el comercio debe analizar y determinar los próximos pasos.

El IsoResponseCode inicial correspondiente a la solicitud de RiskMgmt que devolverá el resultado de la autenticación 3DS (que se muestra arriba resaltado en azul).

Y luego el IsoResponseCode final que se muestra arriba resaltado en verde

8.1 Código de respuesta de autenticación de 3DS

El 3DS IsoResponseCode es generado por PowerTranz que muestra el estado de la autenticación 3DS.

La nota 3D0 significa que el proceso se completó con éxito, pero aún es necesario interpretar los resultados detallados y tomar una decisión antes de determinar si enviar o no una finalización de pago. También hay reglas que se pueden establecer por comercio que determinan si se permitirá la finalización de un pago según el resultado de la autenticación 3DS.

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

Ejemplo de Respuesta de autenticación :

```
"IsoResponseCode": "3D0",
  "ResponseMessage": "3D-Secure complete",
```

8.2 Resultado de la autenticación 3DS

El objeto anidado ThreeDSecure en la respuesta de autenticación muestra el resultado de la autenticación 3DS. Los comercios deben poder interpretar valores de campo importantes y decidir si continuar o no con la finalización del pago en función del resultado.

8.3 Estado de autenticación de 3DS

La siguiente tabla muestra posibles valores de estado de autenticación y sus significados. Si el estado de autenticación es N (no autenticado), no se permitirá la finalización del pago.

Valor	Descripción
Y	Autenticación o verificación de cuenta exitosa
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

**Tenga en cuenta que una respuesta de desafío solo devolverá un resultado de Y o N

8.4 Valor 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 exitosa.
- 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 exitosa.
- ECI 01: Se intentó realizar autenticación 3DS.
- ECI 00: La autenticación 3DS fracasó o no estaba disponible. La transacción se considera no 3DS.

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

8.5 Resultado del Código de razón para el Estado de la transacción (StatusReason)

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

9. Consideraciones Especiales

9.1 Tipos de tarjetas no compatibles: no 3DS

Las tarjetas que actualmente no son compatibles con 3DS (JCB, Discover, Diners) aún se pueden enviar de la misma manera que las tarjetas habilitadas para 3DS se envían a través del método de integración simplificado con o sin HPP. En lugar de recibir un resultado de 3DS, recibirá una respuesta 3D1, lo que significa que 3DS no es compatible y puede elegir si desea continuar con la finalización del pago o no.

9.2 Identificadores de transacciones y órdenes

PowerTranz requiere un ***TransactionIdentifier*** y un ***OrderIdentifier*** únicos para todas las transacciones que debe generar el comercio.

El TransactonIdentifier es un formato GUID y es la identificación única dentro de PowerTranz.

El OrderIdentifier es uno de los valores utilizados en Merchant Portal y en el sistema de reportes y debe ser único para cada transacción aprobada.

9.3 3DS 2 e información del titular de la tarjeta

Si bien solo el nombre del titular de la tarjeta es obligatorio para las transacciones 3DS2, se recomienda incluir tantos campos de Dirección de facturación como sea posible. El servidor ACS (servidor de autenticación del banco emisor) decidirá sobre el flujo sin fricciones versus el flujo de desafío en función de una serie de factores y cualquier información proporcionada por adelantado puede ayudar a un flujo de autenticación sin problemas.

Tenga en cuenta que para 3DS 2, el nombre del comercio que se usa en la autenticación debe coincidir exactamente con el nombre del comercio que se usa en la autorización. Si se realiza una transacción de solo autenticación 3DS y la autorización se realiza por separado, es responsabilidad del comercio asegurarse de que estos valores se envíen correctamente.

9.4 Validación de datos

El protocolo EMV 3DS utiliza el conjunto de caracteres comunes ISO 8859 para los valores permitidos. Si los parámetros de una solicitud de autenticación 3DS (como el nombre o la dirección del titular de la tarjeta) se envían en un juego de caracteres no compatible, la autenticación fallará.

10. FACPG2-SENTRY Autorización Financiera y Modificación de Transacción

Como se explicó anteriormente en la sección ***2.3 Merchant API Calls – Additional Details***, una vez que se haya completado el flujo de autenticación en el banco emisor y se haya devuelto la prueba de la información de autenticación a la URL del comercio proporcionada a través de una devolución de llamada, se usará la siguiente información para completar la parte financiera de la transacción, como Autorización/Captura.

Todas estas operaciones estarán disponibles en la plataforma FACPG2-SENTRY:

- Los comercios pueden posteriormente "Autorizar", una transacción autenticada con éxito
- pueden "Capturar", "Revertir" o "Reembolsar" una transacción Autorizada con éxito a través de la operación Modificación de Transacción.
- Las URL base externas para estos puntos finales son:

Interface	Entorno	Url
SOAP	Test	***https://ecm.firstatlanticcommerce.com/PGService/<Service Name>***
SOAP	Producción	***https://marlin.firstatlanticcommerce.com/PGService/<Service Name>***
XML	Test	*https://ecm.firstatlanticcommerce.com/PGServiceXML*
XML	Producción	*https://marlin.firstatlanticcommerce.com/PGServiceXML*

Service Names

```
// Services.svc:
AuthorizeResponse Authorize(AuthorizeRequest Request)
TransactionModificationResponse TransactionModification(TransactionModificationRequest Request)
```

(para obtener una lista completa de las operaciones admitidas, consulte la guía de integración rápida FACPG2-SENTRY)

10.1 Ejemplos usando la interface XML

Request	Response
POST /PGServiceXML/Authorize HTTP/1.1 Content-Type: text/xml User-Agent: PostmanRuntime/7.29.0 Accept: */* Postman-Token: f038c02d-aa6f-4e57-907c-e9725f3dcc32 Host: ecm.firstatlanticcommerce.com Accept-Encoding: gzip, deflate, br Connection: keep-alive Content-Length: 2776 <AuthorizeRequest xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.firstatlanticcommerce.com/gateway/data"> <TransactionDetails> <AcquirerId>464748</AcquirerId> <MerchantId>88800033</MerchantId> <OrderNumber>7507950196142093875</OrderNumber> <TransactionCode>4</TransactionCode> <Amount>000000000110</Amount> <Currency>840</Currency> <CurrencyExponent>2</CurrencyExponent> <SignatureMethod>SHA1</SignatureMethod> <Signature>P15uB/CNc34IRnL+kGCM1b8sAHI=</Signature> <IPAddress /> <CustomData /> <CustomerReference>This is a XML Authorization for merchant: 88800033</CustomerReference> <ExtensionData /> </TransactionDetails> <CardDetails> <CardNumber>4242424242424242</CardNumber> <CardExpiryDate>0622</CardExpiryDate> <CardCVV2>123</CardCVV2> <IssueNumber /> <StartDate /> <Installments>0</Installments> <DocumentNumber /> <ExtensionData /> </CardDetails> <ThreeDSecureDetails> <AuthenticationResult>U</AuthenticationResult> <ECIIndicator>00</ECIIndicator> <TransactionStain>50691073-2f4b-4a00-a6af-01abe595528e</TransactionStain> </ThreeDSecureDetails> <ThreeDSecureAdditionalInfo> <ProtocolVersion>2.0</ProtocolVersion> <DSTransId>d0ededd6-a28d-498e-8efa-078b2e089842</DSTransId> </ThreeDSecureAdditionalInfo> </AuthorizeRequest>	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/html; charset=utf-8 Server: X-AspNet-Version: 4.0.30319 Content-Security-Policy: default-src https: 'unsafe-eval' 'unsafe-inline' Strict-Transport-Security: max-age=31536000; includeSubdomains=true X-Frame-Options: sameorigin X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Referrer-Policy: no-referrer-when-downgrade Date: Wed, 26 Jan 2022 21:55:29 GMT Content-Length: 1831 <AuthorizeResponse xmlns="http://schemas.firstatlanticcommerce.com/gateway/data" xmlns:i="http://www.w3.org/2001/XMLSchema-instance"> <AcquirerId>464748</AcquirerId> <CreditCardTransactionResults> <AVSResult/> <AuthCode>1</AuthCode> <CVV2Result/> <OriginalResponseCode>00</OriginalResponseCode> <PaddedCardNumber>XXXXXXXXXXXX4242</PaddedCardNumber> <ReasonCode>1</ReasonCode> <ReasonCodeDescription>Transaction is approved.</ReasonCodeDescription> <ReferenceNumber>202621619840</ReferenceNumber> <ResponseCode>1</ResponseCode> <TokenizedPAN/> </CreditCardTransactionResults> <CustomData/> <MerchantId>88800033</MerchantId> <OrderNumber>7507950196142093875</OrderNumber> <Signature>4ofaquqUT5p6ynmWxFD8xE4tcjA=</Signature> <SignatureMethod>SHA1</SignatureMethod> </AuthorizeResponse>

Captura

REQUEST	RESPONSE
POST https://ecm.firstatlanticcommerce.com/PGServiceXML/TransactionModification HTTP/1.1 Content-Type: text/xml Host: ecm.firstatlanticcommerce.com Content-Length: 453 Expect: 100-continue Connection: Keep-Alive <TransactionModificationRequest xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.firstatlanticcommerce.com/gateway/data"> <AcquirerId>464748</AcquirerId> <Amount>000000000110</Amount> <CurrencyExponent>2</CurrencyExponent> <MerchantId>88800033</MerchantId> <ModificationType>1</ModificationType> <OrderNumber>7507950196142093875</OrderNumber> <Password>q7Y7Xqwy</Password> </TransactionModificationRequest>	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/html Server: X-AspNet-Version: 4.0.30319 Content-Security-Policy: default-src https: 'unsafe-eval' 'unsafe-inline' Strict-Transport-Security: max-age=31536000; includeSubdomains=true X-Frame-Options: sameorigin X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Referrer-Policy: no-referrer-when-downgrade Date: Wed, 26 Jan 2022 22:42:20 GMT Content-Length: 442 <TransactionModificationResponse xmlns="http://schemas.firstatlanticcommerce.com/gateway/data" xmlns:i="http://www.w3.org/2001/XMLSchema-instance"> <AcquirerId>464748</AcquirerId> <MerchantId>88800033</MerchantId> <OrderNumber>7507950196142093875</OrderNumber> <OriginalResponseCode/> <ReasonCode>1101</ReasonCode> <ReasonCodeDescription>Transaction successful</ReasonCodeDescription> <ResponseCode>1</ResponseCode> </TransactionModificationResponse>

Reembolso

REQUEST	RESPONSE
POST https://ecm.firstatlanticcommerce.com/PGServiceXML/TransactionModification HTTP/1.1 Content-Type: text/xml Host: ecm.firstatlanticcommerce.com Content-Length: 453 Expect: 100-continue <TransactionModificationRequest xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.firstatlanticcommerce.com/gateway/data"> <AcquirerId>464748</AcquirerId> <Amount>000000000110</Amount> <CurrencyExponent>2</CurrencyExponent> <MerchantId>88800033</MerchantId> <ModificationType>2</ModificationType> <OrderNumber>7507950196142093875</OrderNumber> <Password>q7Y7Xqwy</Password> </TransactionModificationRequest>	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/html Server: X-AspNet-Version: 4.0.30319 Content-Security-Policy: default-src https: 'unsafe-eval' 'unsafe-inline' Strict-Transport-Security: max-age=31536000; includeSubdomains=true X-Frame-Options: sameorigin X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Referrer-Policy: no-referrer-when-downgrade Date: Wed, 26 Jan 2022 22:42:30 GMT Content-Length: 442 <TransactionModificationResponse xmlns="http://schemas.firstatlanticcommerce.com/gateway/data" xmlns:i="http://www.w3.org/2001/XMLSchema-instance"> <AcquirerId>464748</AcquirerId> <MerchantId>88800033</MerchantId> <OrderNumber>7507950196142093875</OrderNumber> <OriginalResponseCode/> <ReasonCode>1101</ReasonCode> <ReasonCodeDescription>Transaction successful</ReasonCodeDescription> <ResponseCode>1</ResponseCode> </TransactionModificationResponse>

reversión (Anulación)

REQUEST	RESPONSE
POST https://ecm.firstatlanticcommerce.com/PGServiceXML/TransactionModification HTTP/1.1 Content-Type: text/xml Host: ecm.firstatlanticcommerce.com Content-Length: 453 Expect: 100-continue <TransactionModificationRequest xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.firstatlanticcommerce.com/gateway/data"> <AcquirerId>464748</AcquirerId> <Amount>000000000110</Amount> <CurrencyExponent>2</CurrencyExponent> <MerchantId>88800033</MerchantId> <ModificationType>3</ModificationType> <OrderNumber>7507950196142093875</OrderNumber> <Password>q7Y7Xqwy</Password> </TransactionModificationRequest>	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/html Server: X-AspNet-Version: 4.0.30319 Content-Security-Policy: default-src https: 'unsafe-eval' 'unsafe-inline' Strict-Transport-Security: max-age=31536000; includeSubdomains=true X-Frame-Options: sameorigin X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Referrer-Policy: no-referrer-when-downgrade Date: Wed, 26 Jan 2022 22:42:30 GMT Content-Length: 442 <TransactionModificationResponse xmlns="http://schemas.firstatlanticcommerce.com/gateway/data" xmlns:i="http://www.w3.org/2001/XMLSchema-instance"> <AcquirerId>464748</AcquirerId> <MerchantId>88800033</MerchantId> <OrderNumber>7507950196142093875</OrderNumber> <OriginalResponseCode/> <ReasonCode>1101</ReasonCode> <ReasonCodeDescription>Transaction successful</ReasonCodeDescription> <ResponseCode>1</ResponseCode> </TransactionModificationResponse>

Tokenización:

Request	Response
POST https://ecm.firstatlanticcommerce.com/PGServiceXML/Tokenize HTTP/1.1 Content-Type: text/xml Host: ecm.firstatlanticcommerce.com Content-Length: 329 Expect: 100-continue Connection: Keep-Alive <TokenizeRequest xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.firstatlanticcommerce.com/gateway/data"> <CardNumber>4242424242424242</CardNumber> <ExpiryDate>0723</ExpiryDate> <MerchantNumber>88800033</MerchantNumber> <Signature>m//jB6Dpgl3OyXeA/thFQNelXb0=</Signature> </TokenizeRequest>	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/html Server: X-AspNet-Version: 4.0.30319 Content-Security-Policy: default-src https: 'unsafe-eval' 'unsafe-inline' Strict-Transport-Security: max-age=31536000; includeSubdomains=true X-Frame-Options: sameorigin X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Referrer-Policy: no-referrer-when-downgrade Date: Wed, 26 Jan 2022 22:48:35 GMT Content-Length: 216 <TokenizeResponse xmlns="http://schemas.firstatlanticcommerce.com/gateway/data" xmlns:i="http://www.w3.org/2001/XMLSchema-instance"> <ErrorMsg/> <Success>true</Success> <Token>424242_04XOK4242</Token> </TokenizeResponse>

Annex B Common Character Set

Table 36 shows the character set common to all parts of 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	1	0	14			.	>	N	^	n	~
1	1	1	1	15			/	?	O	_	o	

Table 36: Common Character Set

10. Cuentas y Casos de Prueba

Existen dos flujos distintos de proceso para 3DS, fluido y con cuestionamiento (challenge). El flujo fluido ocurre cuando interacción con el tarjetahabiente no es necesario durante la autenticación. Por otra parte, el flujo con cuestionamiento involucra una redirección desde el navegador del tarjetahabiente al servidor del banco emisor, para efectuar uno o más cuestionamientos (verificación de credenciales) necesarios para completar la autenticación.

La necesidad de efectuar una verificación del dispositivo empleado por el tarjetahabiente (por ejemplo, su navegador de internet durante la sesión de compra ecommerce) la determina el servidor del emisor. Esta verificación puede ocurrir en ambos flujos, es decir, como parte del flujo fluido y del flujo con cuestionamiento.

Las cuentas de tarjetas de pruebas generan resultados pre-establecidos de autenticación y autorización.

Caso	Nro. de Tarjete	Versión 3DS	PW	Observaciones
Los siguientes casos producen transacciones aprobadas				
M1-01-YA	5115010000000018	1.0.2	3ds1	Retrocede a 3DS 1, Status=A
V2-01-YA	4012000000020071	2.1.0		Flujo fluído, Status=Y
V2-02-AA	4012000000020089	2.1.0		Flujo fluído, Status=A
M2-01-YA	5100270000000023	2.1.0		Flujo fluído, Status=Y
M2-02-RA	5100270000000072	2.1.0		Flujo fluído, Status=R
V2-03-YA	4012000000020006	2.1.0	3ds2	Cuestionamiento, Status=Y
M2-03-YA	5100270000000031	2.1.0	3ds2	Cuestionamiento, Status=Y
V2-04-YA	4012010000020070	2.1.0		Flujo fluído, Verificación de dispositivo, Status=Y
V2-05-AA	4012010000020088	2.1.0		Flujo fluído, Verificación de dispositivo, Status=A
M2-04-YA	5100271000000120	2.1.0		Flujo fluído, Verificación de dispositivo, Status=Y
V2-06-YA	4012010000020005	2.1.0	3ds2	Custionamiento, Verif. de dispositivo, Status=Y
V2-07-YA	4012000000020071	2.1.0	3ds2	Custionamiento, include ChallengeIndicator = 03
A2-01-YA *	341111000000009	2.1.0		Flujo fluído, Status=Y
DS-01-0A	6011111111111111	n/a		Discover
JC-01-0A	3528111111111108	n/a		JCB
Los siguientes casos producen transacciones denegadas				
V2-01-ND	4012000000020121	2.1.0		Flujo fluído, Status=N, Finalización del Pago no permitida (código de respuesta 12)
M2-01-ND	5100270000000098	2.1.0		Flujo fluído, Status=N, Finalización del Pago no permitida (código de respuesta 12)
M2-02-ND	5100270000000056	2.1.0		Cuestionamiento, Status=N, Finalización del Pago no permitida (código de respuesta 12)
V2-02-AD	4666666666662222	2.1.0		Flujo fluído, Status = A, Código de Respuesta ISO = 05, Respuesta al CVV = N
M2-03-UD	5555666666662222	2.1.0		Flujo fluído, Status=U, Código de Resp ISO = 05
V2-03-AD	4111111111119999	2.1.0		Flujo fluído, Status=U, Código de Resp ISO = 98
M2-04-AD	5111111111113333	2.1.0		Flujo fluído, Status=A, Código de Resp ISO = 05
V2-04-YD	4111111111110000	2.1.0	3ds2	Cuestionamiento, Status =Y, Código de Resp ISO = 91
M2-05-YD	5111111111110000	2.10	3ds2	Cuestionamiento, Status =Y, Código de Resp ISO = 91
DS-01-0D	6011111111111152	n/a		Discover
JC-01-0D	3528111111111157	n/a		JCB

* Por favor confirme con el equipo de Soporte de Powertranz si AMEX 3DS se soporta para su cuenta en la actualidad.

Apéndice 1 – Códigos de Respuesta

Códigos de Respuesta PowerTranz e Información de Errores

Código de Respuesta Code	Código de Respuesta	Mensaje de Respuesta	Detalles del Error
00		Transacción aprobada	
03	310	Comercio inválido	
05	22	Transacción declinada	Declinación por defecto
12	315	Tarjeta o moneda inválida	Tarjeta o moneda inválida
12	321	Errores de procesamiento	Errores de procesamiento
12	326	Transacción inválida	Campo inválido en el Host plugin: {nombre del campo}
12	330	Transacción Inválida	No se permite {nombre del campo}
12	343	Transacción Inválida	Comercio inválido
12	386	Transacción Inválida	Transacción clausurada
12	384	Transacción Inválida	Reembolso inválido
12	387	Transacción duplicada	ID de la Transacción Duplicado
12	354	Transacción Inválida	Error criptográfico
12	380	Transacción Inválida	autorización original inválida
12	381	Transacción Inválida	No se encontró autorización original
12	382	Transacción Inválida	Monto de autorización original inválido
12	383	Transacción Inválida	Monto inválido
12	344	Transacción Inválida	Comercio cerrado/cancelado
12	345	Transacción Inválida	Parámetros de pago deshabilitados
12	370	Transacción no concuerda	Transacción no concuerda en el simulador de pruebas
12	320	Transacción Inválida	Transacción de Prueba Inválida
12	426	Transacción Inválida	Campo inválido en el Host plugin: {nombre del campo}
12	76	Transacción Inválida	Transacción SPI Inválida
12	757	Transacción Inválida	No se encontró Página Alojada
12	546	Error 3DS1	Retroceso (fallback) a 3D1 no permitido
12	362	Transacción Inválida	Transacción Inválida
12	361	Transacción Inválida	Transacción Inválida
12	75	Error SPI	Error SPI
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 cuestionamiento
3D3	641	Error sistema 3DS2	Error en el cuestionamiento
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	3DS2 notify error
3D3	544	Error sistema 3DS2	3DS2 fingerprint error
3D3	550	Error 3DS2	DS error
3D3	548	Error 3DS	Error de comunicación DS
3D3	551	Error 3DS2	Servidor 3DS inalcanzable
3D3	549	3DS error	Error de Cache
3D3	649	Error sistema 3DS2	Error de Cache
3D3	510	3DS error	3DS parámetro invalido: {Nombre del Campo
57	316	Invalid card type	Tipo de tarjeta invalida
89	312	Failed autenticación	Credenciales invalidas
91	391	Host timeout	Timeout del host
91	392	Host comms error	Error de comunicación con el Host
91	329	Host comms error	Host no disponible
96	424	Error de sistema	Error de comunicación interna
96	44	Error de sistema	Error General en GateApi
96	432	Error de sistema	Missing action: {Nombre del Campo
96	459	Error de sistema	Error de Persistencia
96	460	Error de sistema	Error de mapeo de tarjeta
96	85	Error de sistema	SPI Error de sistema
96	850	Error de sistema	HPP Error de sistema
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	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 detectados
96	422	Error de procesamiento del Host	Error del plugin 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 plugin 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 de comunicación del host	Error PL
HP0		Preprocesamiento finalizado en la Página Alojadas	
SP4		Preprocesamiento SPI finalizado	
TK0		Tokenización completa	

Códigos de Respuesta ISO

Código de Respuesta Code y Descripción		Código de Respuesta Code y Descripción	
00	Aprobada	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 registro de la tarjeta
04	Retenga tarjeta	57	Transacción no permitida a la tarjeta
05	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 identidad	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 tarjeta no existe	67	Retenga tarjeta en cajero automático
15	Emisor no existe	68	Respuesta se recibió demasiado tarde
16	Aprobada, actualice pista # 3	75	Intentos con PIN incorrecto excedió límite
17	Cancelación por parte del cliente	76	No se ubicó anterior mensaje
18	Disputa del cliente	77	Datos no concuerdan con mensaje original
19	Reingrese 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 archive	89	Fracaso de Autenticación
28	Archivo temporalmente indisponible	90	Proceso de cierre en marcha
29	Actualización de archive no fue exitoso	91	Emisor o servidor indisponible
30	Error de formato	92	Ruta no disponible
31	Emisor no disponible	93	Violación de la 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	Transacción con error
38	Excedió límite de intentos de ingresar PIN	N0	STIP Forzoso
39	No se ubicó cuenta de crédito	N3	Servicio de efectivo no disponible

40	Función no soportada	N4	Solicitud de efectivo excede límite del emisor
41	Retenga tarjeta (tarjeta perdida)	N7	Denegada por CVV incorrecto
42	No se ubicó cuenta universal	P2	Información del facturador incorrecta
43	Retenga tarjeta (tarjeta robada)	P5	Solicitud de cambio de PIN Unblock Denegada
44	No se ubicó cuenta de inversiones	P6	PIN inseguro
51	Fondos insuficientes	XA	Enviar al emisor
52	No se ubicó cuenta de cheques	XD	Enviar al emisor

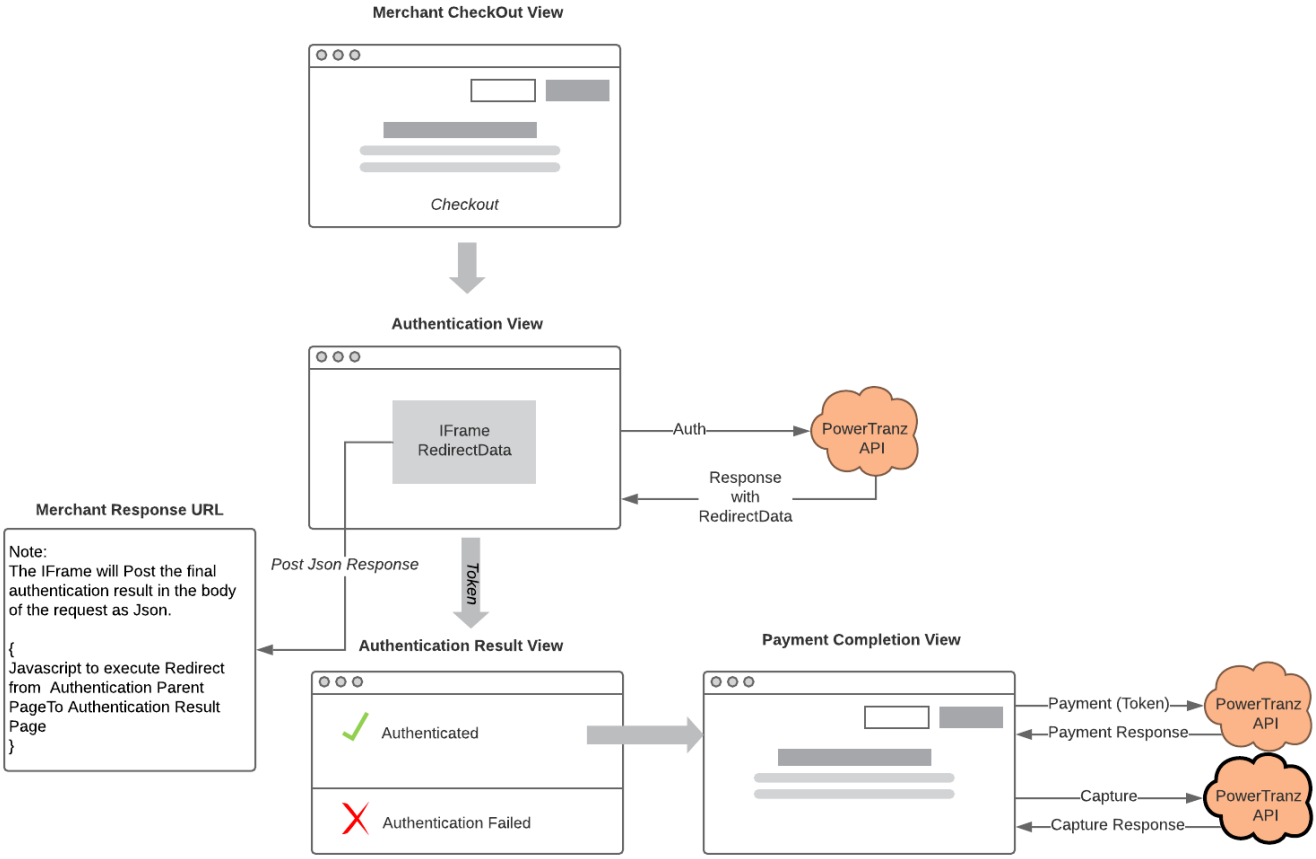
Códigos de Respuesta CVV2

Código	Definición
M	Concuerda
N	No concuerda
P	No se procesó
S	Debería aparecer en la tarjeta, pero no se suministró (Visa únicamente)
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 ilustrar todas las posibilidades en este documento. A continuación, se muestra un 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) Vista de pago del comercio

   La aplicación del comercio recopila datos del titular de la tarjeta y los publica en la vista de autenticación.

2) Vista de autenticación con iFrame

   La aplicación Comercio envía una solicitud de RiskMgmt al extremo de RiskMgmt y devuelve una respuesta de RiskMgmt a la vista de autenticación. Esta vista contendrá un Iframe al que se vinculará RedirectData.

   - Punto final de PowerTranz: {URL raíz de PowerTranz}/api/spi/RiskMgmt
   - Cuerpo de la solicitud: Solicitud de RiskMgmt
   - El atributo MerchantResponseUrl debe contener un URI en el dominio de la aplicación Merchant en el que el Iframe publicará la respuesta de autenticación final.
   - Respuesta: Respuesta de RiskMgmt que contiene IsoResponseCode y RedirectData: un formulario HTML que se ejecutará dentro del contexto del Iframe.

- RiskMgmtResponse.RedirectData se inyecta o vincula al Iframe.

  Por ejemplo:

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

3) iFrame
   Una vez que los datos de redirección (*RedirectData*) han sido acoplados al *iFrame*, el proceso continuará dentro del context 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 fluído), el contexto del *iFrame* será posteado del resultado de la autenticación directamente al URL de respuesta del comercio.
   - En ambos casos (Flujo Fluído y Cuestionamiento), los resultados de la autenticación serán posteados al URL de respuesta del comercio.
4) 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 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 redirecciona el contenedor matriz del *iFrame* al resultado Autenticación, lo cual elimina el *iFrame*y y devuelve el control al Comercio. Por Ejemplo:

```
<script>

    window.onload = redirectParent;

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

</script>
```

5) Vista de resultados de autenticación. Esta vista procesará el resultado final de la autenticación. Si tiene éxito, la aplicación Merchant continuará hasta la finalización del pago.
6) Vista de finalización de pago. La aplicación Merchant ahora puede llamar a puntos finales posteriores, como Autorización, Captura y/o Reversión utilizando la API FACPG2-SENTRY.