AZUL | SERVICIOS DIGITALES POPULAR

AUTENTICACIÓN DEL TARJETAHABIENTE

ID Check

SafeKey®

DISCOVER NETWORK

Diners Club INTERNATIONAL

ProtectBuy®

VISA SECURE

ÍNDICE

Autenticación del Tarjetahabiente....3
Flujos de implementación....3
ForceNo3DS....5
Flujo sin fricción....7
Recopile los detalles de pago del tarjetahabiente....7
Iniciar un pago....7
ThreeDSAuth....8
CardHolderInfo....8
BrowserInfo....10
Respuesta de autenticación de 3D-Secure....15
Solicitud y respuesta de notificación del método 3DS....16
ThreeDSServerTransID....17
Soporte del emisor 3DS....17
Solicitud "ProcessThreeDSMethod" para continuar con la autenticación 3DS....17
Flujo con desafío....19
Desafío sin "threeDSMethod" (D)....19
Desafío con "ThreeDSMethod" (DM)....19
Paso 3 (D) | 6 (DM): Integración vía API responde para continuar con la Autenticación del tarjetahabiente....20
Paso 4 (D) | 7 (DM): Redirección desafío al tarjetahabiente....21
Paso 5 (D) | 8 (DM): Envio solicitud "ProcessThreeDSChallenge" para completar autorización....22
Paso 6 (D) | 9 (DM): Respuesta final de 3DS....24
Datos para pruebas....24
Soporte....25

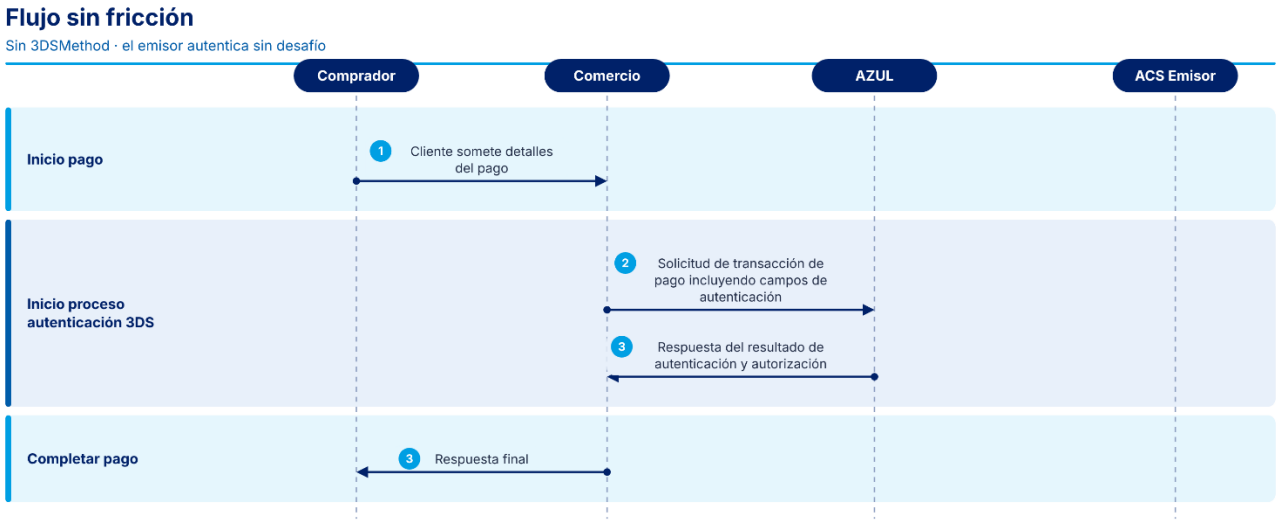
Autenticación del Tarjetahabiente

El servicio de Autenticación del Tarjetahabiente de AZUL permite autenticar a los clientes en las compras no presenciales mediante el protocolo EMV 3-D Secure, el estándar global que utilizan las marcas para confirmar que quien realiza la compra es el titular legítimo de la tarjeta. AZUL acepta la autenticación de los programas 3-D Secure de las siguientes marcas: Visa (**Visa Secure**), Mastercard (**Mastercard Identity Check**), American Express (**American Express SafeKey**) y Diners Club International y Discover (**ProtectBuy**). La autenticación se realiza con el banco emisor de la tarjeta de forma transparente para el comercio y, cuando es exitosa, reduce el riesgo de fraude y traslada al emisor la responsabilidad por contracargos de fraude (liability shift), de acuerdo con las reglas de cada marca.

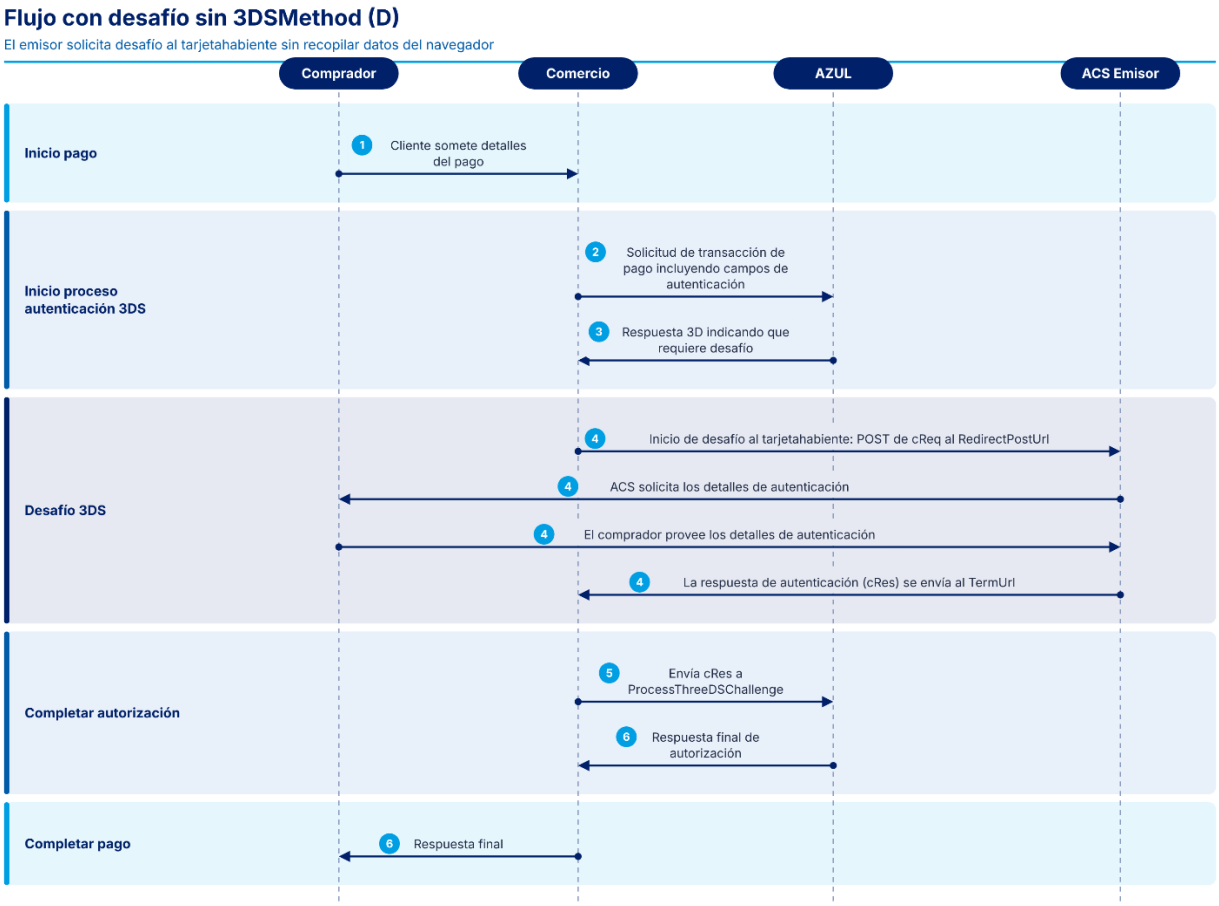
Flujos de implementación

La nueva versión del servicio de Autenticación del Tarjetahabiente se implementa a partir de una transacción de "**Venta**" o "**Hold**", enviando datos adicionales para la autenticación. Se definen dos flujos posibles que puede tener el proceso de autenticación:

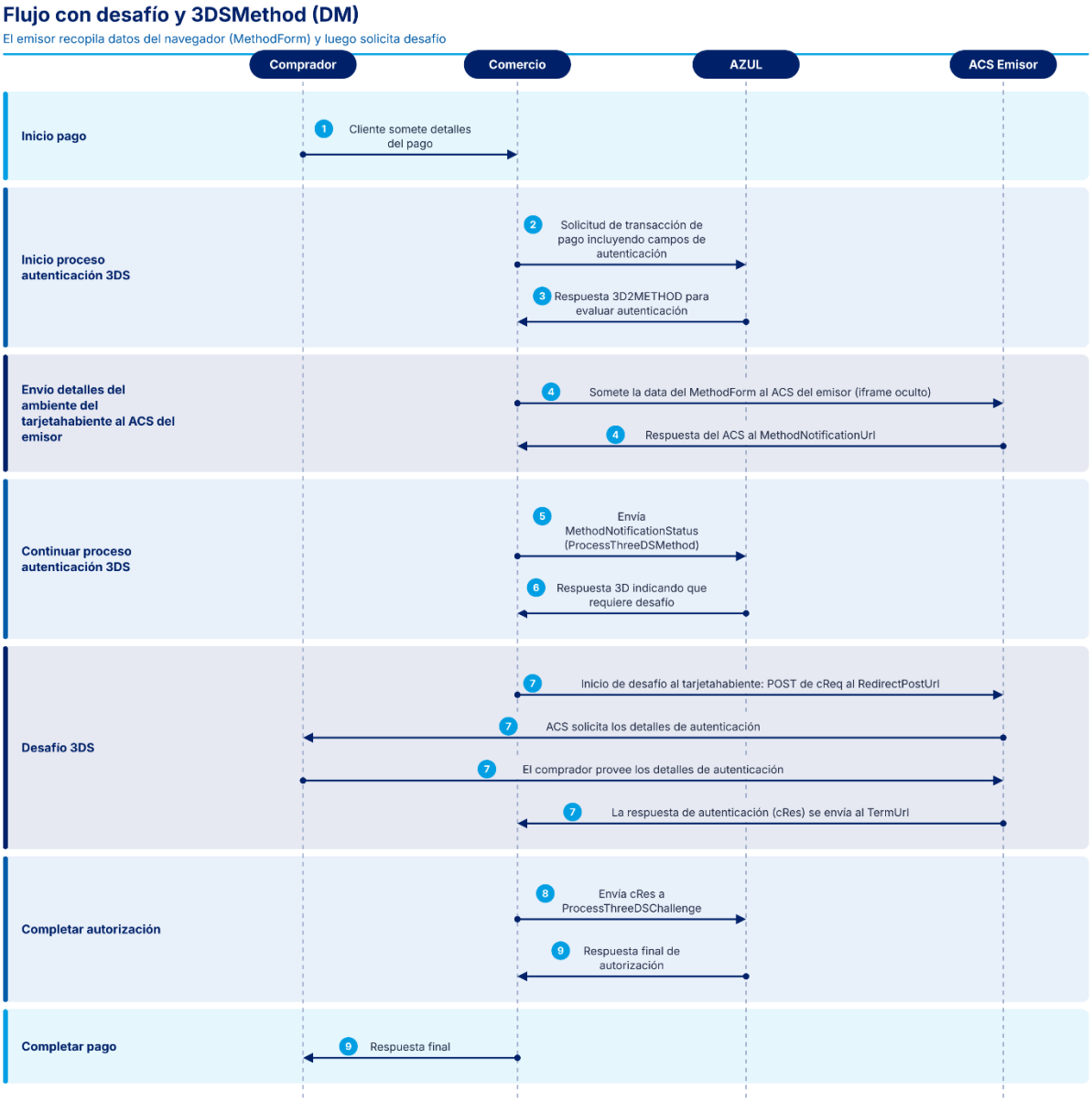
Flujo sin fricción: cuando el emisor no requiere que el tarjetahabiente complete un desafío para autenticarse.



Flujo con desafío (“**challenge**”): cuando el emisor ha solicitado a su tarjetahabiente que proporcione detalles de autenticación adicionales.



Flujo con desafío (“**challenge**”) **y método**: cuando el emisor ha solicitado a su tarjetahabiente que proporcione detalles de autenticación adicionales aparte del aplicado por el mismo Banco Emisor.



ForceNo3DS

Para los casos de que se tenga el servicio para activar el envío de las transacciones por los flujos de Autenticación del tarjetahabiente, deberán enviar el campo con los siguientes valores:

Activar Autenticación del tarjetahabiente	
Campo	Valor
	“0”

ForceNo3ds	Null
	""

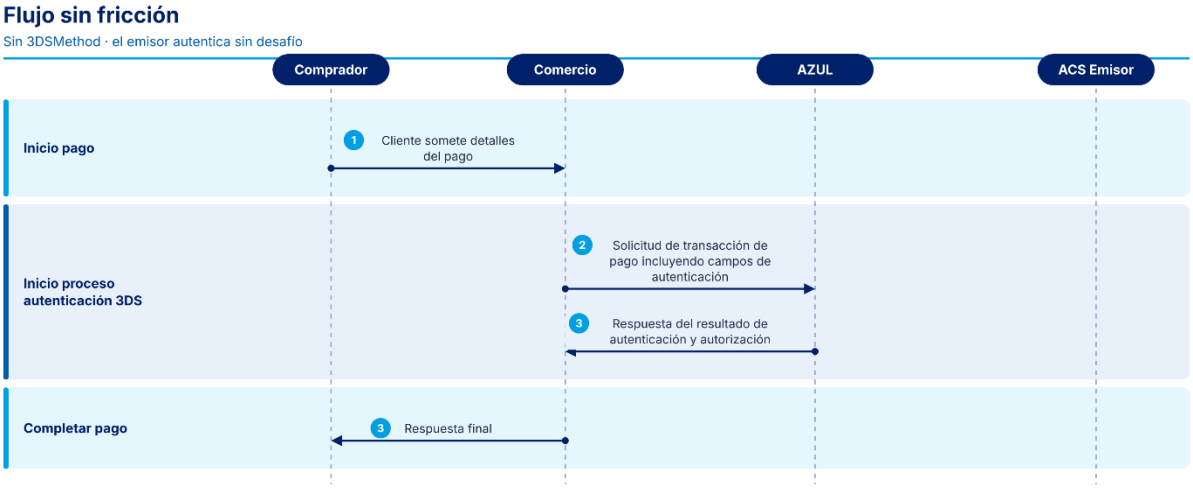
En caso de que se tenga el servicio de Autenticación del tarjetahabiente habilitado y se desea enviar una transacción que no pase por la autenticación con 3D-Secure, se debe incluir en el mensaje inicial de "**Venta**" o "**Hold**":

No activar Autenticación del tarjetahabiente	
Campo	Valor
ForceNo3ds	"1"

IMPORTANTE: al enviar el campo igual a "**1**", el comercio pierde la protección por fraude brindada por el servicio de Autenticación del tarjetahabiente para la transacción, **por lo que, asume el riesgo de recibir un contracargo en cado de que resulte ser fraudulenta.**

Flujo sin fricción

En el siguiente diagrama se muestra la secuencia del flujo sin fricción con cada paso detallado:



Recopile los detalles de pago del tarjetahabiente

Primero, recopila la información de pago de la tarjeta (número de tarjeta de crédito o débito, fecha de vencimiento, código de seguridad).

Iniciar un pago

Utilice la tarjeta de pago (o el token si utiliza el servicio de Bóveda de datos) para iniciar una transacción de pago principal. Los tipos de transacción relevantes para la autenticación con 3DSecure son:

- Sale: Transacción de venta con captura inmediata.
- Hold: Transacción de venta con solo reserva de fondos.

Este mensaje debe ser enviado a la Integración vía API de AZUL utilizando una de las siguientes URL según el tipo de mensajería elegido:

- SOAP (método "**ProcessPayment**"): pagos.azul.com.do/WebServices/SOAP/default.asmx
- JSON: https://pagos.azul.com.do/WebServices/JSON/default.aspx
- Para ambiente de prueba, utilizar el dominio pruebas.AZUL.com.do

Para el procesamiento con Autenticación del tarjetahabiente, se deben incluir en el mensaje de venta dos campos adicionales, el "**ThreeDSAuth**", "**CardHolderInfo**" y "**BrowserInfo**", los cuales tienen subcampos detallados a continuación:

ThreeDSAuth

Campos para autenticación	
ThreeDSAuth	
Sub-campo	Descripción
TermUrl	URL del comercio donde serán posteados los valores de respuesta con el resultado de la autenticación del por el servidor ACS (este es el servidor del banco emisor que procesa la autenticación del tarjetahabiente). Se deber construir con un identificador único que sirva para asociar.
MethodNotificationUrl	URL del comercio donde se recibirá la notificación de que se completó el iFrame (el cual se hará referencia más adelante) y capturó los datos del navegador para ser usados en el análisis de riesgo. Esta notificación debe llegar mediante un HTTP Post del servidor ACS del emisor y contiene un identificador único de transacción representado con el "**threeDSServerTransID**". Esta URL debe ser única e identificable, por lo que cuando se reciba la notificación, debería poder asociarse con la transacción correspondiente. Esto elimina cualquier dependencia del "**threeDSServerTransID**", que se recibe con la respuesta del nodo "**ThreeDSMethod**". Una forma sencilla de garantizar el mapeo correcto con las transacciones es pasar una referencia de transacción como un query string. Por ejemplo: "http://www.mitienda.com/3dscapture.aspx?sid=6371952800755 07073
RequestorChallengeIndicator	Este indicador sirve para comunicar al banco emisor la preferencia que tiene comercio de que se solicite el desafío.

RequestChallengeIndicator	
Indicador de desafío	Descripción
01	Sin preferencias (no tiene preferencia si se debe realizar un desafío. Este es el valor predeterminado).
02	No solicitar ningún desafío (comercio prefiere que no se realice ningún desafío).
03	Solicitar desafío: Preferencia del solicitante de 3DS (prefiere que se realice un desafío; esto debe establecerse para transacciones de alto riesgo o valor).
04	Cuando solicitar desafío es mandatorio (existen mandatos locales o regionales que indican que se debe realizar un desafío, actualmente en República Dominicana no es mandatorio por lo que en este momento este valor no aplica para nuestro país).

CardHolderInfo

Este grupo de campos sirven para ayudar al motor de 3-D Secure del banco emisor de la tarjeta a calcular el riesgo de la transacción e influir en la solicitud, o no, de un desafío. En caso de que no tenga la información de alguno de los campos, lo recomendable es omitir el campo en el mensaje, es decir, no enviar el campo si está en blanco.

Campos para autenticación		
CardHolderInfo		
Sub-campo	Descripción	Tamaño Limite
BillingAdressCity	Ciudad de la dirección de facturación.	96 caracteres incluyendo espacios.
BillingAdressCountry	País de la dirección de facturación.	Enviar código ISO 2 caracteres país.
BillingAdressLine1	Dirección de facturación – Línea 1.	96 caracteres incluyendo espacios.
BillingAdressLine2	Dirección de facturación – Línea 2.	96 caracteres incluyendo espacios.
BillingAdressLine3	Dirección de facturación – Línea 3.	96 caracteres incluyendo espacios.
BillingAdressState	Estado o provincia de la dirección de facturación.	96 caracteres incluyendo espacios.
BillingAdressZip	Código postal o "ZIP code" de la dirección de facturación.	24 caracteres incluyendo espacios.
Email	Dirección de correo electrónico.	254 caracteres.
Name	Nombre del tarjetahabiente.	96 caracteres incluyendo espacios.
PhoneHome	Teléfono de la casa.	32 caracteres.
PhoneMobile	Teléfono móvil.	32 caracteres.
PhoneWork	Teléfono del trabajo.	32 caracteres.
ShippingAddressCity	Ciudad de la dirección de envío.	96 caracteres incluyendo espacios.
ShippingAddressCountry	País de la dirección de envío.	Enviar código ISO 2 caracteres país.
ShippingAddressLine1	Dirección de envío – Línea 1.	96 caracteres incluyendo espacios.
ShippingAddressLine2	Dirección de envío – Línea 2.	96 caracteres incluyendo espacios.
ShippingAddressLine3	Dirección de envío – Línea 3.	96 caracteres incluyendo espacios.
ShippingAddressState	Estado o provincia de la dirección de envío.	96 caracteres incluyendo espacios.
ShippingAddressZip	Código portal o "ZIP code" de la dirección de envío.	24 caracteres incluyendo espacios.

BrowserInfo

Este grupo de campos deberán ser capturados del navegador del tarjetahabiente al momento de enviar la transacción a la Integración vía API de AZUL, para mejorar la autenticación de la transacción. Los campos a capturarse del navegador del cliente son referentes al soporte de JavaScript, resolución de pantalla, profundidad de color, idioma y zona horaria. **Todos los campos son obligatorios para autenticar la transacción**.

Campos para autenticación	
BrowserInfo	
Sub-campo	Descripción
AcceptHeader	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
IPAddress	Dirección IP.
Language	Idioma en-US.
ColorDepth	Dimensión/color de la pantalla.
ScreenWidth	Dimensión de la pantalla.
ScreenHeight	Dimensión de la pantalla.
TimeZone	Zona horaria.
UserAgent	Detalles del navegador del tarjetahabiente.
JavaScriptEnable	Habilitar JavaScript.

A continuación, utilizar el **Script** siguiente para la captura de estos campos:

Script de ejemplo para capturar en navegador. JavaScript e impresión de formulario HTML invisible.

```
<script type="text/javascript">
  document.write('<input type="hidden" id="BrowserJavaScriptEnabled" name="BrowserJavaScriptEnabled"
value="true">');
  document.write('<input type="hidden" id="BrowserTimeZone" name="BrowserTimeZone" value="' + new
Date().getTimezoneOffset() + '">');

  if (navigator.language)
    document.write('<input type="hidden" id="BrowserLanguage" name="BrowserLanguage" value="' +
navigator.language + '">');

  if (window.screen) {
    document.write('<input type="hidden" id="BrowserColorDepth" name="BrowserColorDepth" value="' +
window.screen.colorDepth + '">');

    if (window.devicePixelRatio) {
      document.write('<input type="hidden" id="BrowserScreenWidth" name="BrowserScreenWidth" value="' +
(window.screen.width * window.devicePixelRatio) + '">');
      document.write('<input type="hidden" id="BrowserScreenHeight" name="BrowserScreenHeight" value="'
+ (window.screen.height * window.devicePixelRatio) + '">');
    } else {
      document.write('<input type="hidden" id="BrowserScreenWidth" name="BrowserScreenWidth" value="' +
window.screen.width + '">');
```

```
      document.write('<input type="hidden" id="BrowserScreenHeight" name="BrowserScreenHeight" value="'
+ window.screen.height + '">');
    }
  }
</script>
```

NOTAS DEL FLUJO (PENDIENTE FORMATEAR):

---

* Estos podrían capturarse en otra pantalla y guardarlos en sesión, lo importante es que pertenezcan al navegador que está realizando la transacción.

** El uso de campos invisibles de HTML es una sugerencia. Es posible capturar estos y enviarlos vía una llamada asíncrona al servidor. En todo caso, el código sirve de ejemplo sobre cómo determinar la data requerida para luego poder enviarla al servidor.

Ejemplo mensaje SOAP (ver nodo BrowserInfo)

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header>
    <SOAPAuthHeader
        xmlns="http://Merit/AZULIS/TransactionServices/">
      <Auth1>xxxx</Auth1>
      <Auth2>xxxx</Auth2>
    </SOAPAuthHeader>
  </soap:Header>
  <soap:Body>
    <ProcessPayment
        xmlns="http://Merit/AZULIS/TransactionServices/">
      <ProcessPaymentRequest>
        <Channel>PP</Channel>
        <Store>99999991</Store>
        <CardNumber>xxxxx</CardNumber>
        <Expiration>202512</Expiration>
        <CVC>999</CVC>
        <PosInputMode>E-Commerce</PosInputMode>
        <TrxType>Sale</TrxType>
        <Amount>1075</Amount>
        <Itbis>121</Itbis>
        <OriginalDate></OriginalDate>
        <OriginalTrxTicketNr></OriginalTrxTicketNr>
        <AuthorizationCode></AuthorizationCode>
        <ResponseCode>string</ResponseCode>
        <AcquirerRefData>1</AcquirerRefData>
        <RRN></RRN>
        <AzulOrderId></AzulOrderId>
        <CustomerServicePhone></CustomerServicePhone>
        <OrderNumber></OrderNumber>
        <ECommerceUrl></ECommerceUrl>
        <CustomOrderId></CustomOrderId>
        <DataVaultToken></DataVaultToken>
        <SaveToDataVault>0</SaveToDataVault>
        <AltMerchantName></AltMerchantName>
        <ForceNo3DS></ForceNo3DS>
        <ThreeDSAuth>

<TermUrl>http://www.url.com/TestForms/webservicespost3ThreeDs.aspx?sid=637836351878902003</TermUrl>

<MethodNotificationUrl>http://www.url.com/3dscapture.aspx?sid=637836351878902003</MethodNotificationUrl
>
          <RequestorChallengeIndicator>04</RequestorChallengeIndicator>
        </ThreeDSAuth>
        <CardHolderInfo>
          <Name></Name>
          <Email></Email>
          <PhoneHome></PhoneHome>
          <PhoneMobile></PhoneMobile>
          <PhoneWork></PhoneWork>
          <BillingAddressLine1></BillingAddressLine1>
          <BillingAddressLine2></BillingAddressLine2>
          <BillingAddressLine3></BillingAddressLine3>
          <BillingAddressCity></BillingAddressCity>
          <BillingAddressState></BillingAddressState>
          <BillingAddressCountry></BillingAddressCountry>
          <BillingAddressZip></BillingAddressZip>
          <ShippingAddressLine1></ShippingAddressLine1>
          <ShippingAddressLine2></ShippingAddressLine2>
          <ShippingAddressLine3></ShippingAddressLine3>
          <ShippingAddressCity></ShippingAddressCity>
```

```
          <ShippingAddressState></ShippingAddressState>
          <ShippingAddressCountry></ShippingAddressCountry>
          <ShippingAddressZip></ShippingAddressZip>
        </CardHolderInfo>
        <BrowserInfo>

<AcceptHeader>text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9</AcceptHeader>
          <IPAddress>127.0.0.1</IPAddress>
          <Language>en-US</Language>
          <ColorDepth>24</ColorDepth>
          <ScreenWidth>2880</ScreenWidth>
          <ScreenHeight>1800</ScreenHeight>
          <TimeZone>240</TimeZone>
          <UserAgent>Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.51 Safari/537.36</UserAgent>
          <JavaScriptEnabled>true</JavaScriptEnabled>
        </BrowserInfo>
      </ProcessPaymentRequest>
    </ProcessPayment>
  </soap:Body>
</soap:Envelope>
```

Ejemplo de JSON de un mensaje de venta con los nuevos campos de 3-D Secure 2.0

```
{
  "Channel": "EC",
  "Store": "30082630281",
  "CardNumber": "1016000000051",
  "Expiration": "202112",
  "CVC": "999",
  "PosInputMode": "E-Commerce",
  "TrxType": "Sale",
  "Amount": "1075",
  "Itbis": "121",
  "OrderNumber": "",
  "CustomOrderId": "",
  "DataVaultToken": "",
  "SaveToDataVault": "0",
  "ForceNo3DS": "",
  "ThreeDSAuth": {
    "TermUrl": "http://www.mitienda.com/post3ThreeDs.aspx?sid=637195280075507073",
    "MethodNotificationUrl": "http://www.mitienda.com/3dscapture.aspx?sid=637195280075507073",
    "RequestorChallengeIndicator": "01"
  },
  "CardHolderInfo": {
    "BillingAddressCity": "Ciudad Facturación",
    "BillingAddressCountry": "País Facturación",
    "BillingAddressLine1": "Línea 1 Dirección Facturación",
    "BillingAddressLine2": "Línea 2 Dirección Facturación",
    "BillingAddressLine3": "Línea 3 Dirección Facturación",
    "BillingAddressState": "Estado o Provincia Facturación",
    "BillingAddressZip": "99999",
    "Email": "correo@dominio.com",
    "Name": "Nombre Tarjetahabiente",
    "PhoneHome": "8099999999",
    "PhoneMobile": "8299999999",
    "PhoneWork": "8499999999",
    "ShippingAddressCity": "Ciudad Envío",
    "ShippingAddressCountry": "País Envío",
    "ShippingAddressLine1": "Línea 1 Dirección Envío",
    "ShippingAddressLine2": "Línea 2 Dirección Envío",
    "ShippingAddressLine3": "Línea 3 Dirección Envío",
    "ShippingAddressState": "Estado o Provincia Facturación",
```

```
    "ShippingAddressZip": "99999"
  },
  "BrowserInfo": {
    "AcceptHeader":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
cation/signedexchange;v=b3;q=0.9",
    "IPAddress": "127.0.0.1",
    "Language": "en-US",
    "ColorDepth": "24",
    "ScreenWidth": "2880",
    "ScreenHeight": "1800",
    "TimeZone": "240",
    "UserAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.51 Safari/537.36",
    "JavaScriptEnabled": "true"
  }
}
```

Ejemplo mensaje HTTP PARAMS (ver variables comenzando con BrowserInfo)

```
Channel=PP
&Store=99999991
&CardNumber=xxxx
&Expiration=202512
&CVC=999
&PosInputMode=E-Commerce
&TrxType=Sale
&Amount=1075
&Itbis=121
&OriginalDate=
&OriginalTrxTicketNr=
&AuthorizationCode=
&ResponseCode=
&AcquirerRefData=1
&RRN=
&AzulOrderId=
&CustomerServicePhone=
&OrderNumber=
&ECommerceUrl=
&CustomOrderId=
&DataVaultToken=
&SaveToDataVault=0
&AltMerchantName=
&ForceNo3DS=
&ThreeDSAuth.TermUrl=http%3a%2f%2f1www.url.com%3a6010%2fTestForms%2fwebservicespost3ThreeDs.aspx%3fsid%
3d637836351878902003
&ThreeDSAuth.MethodNotificationUrl=http%3a%2f%2fwww.url.com%2f3dscapture.aspx%3fsid%3d63783635187890200
3
&ThreeDSAuth.RequestorChallengeIndicator=04
&CardHolderInfo.Name=
&CardHolderInfo.Email=
&CardHolderInfo.PhoneHome=
&CardHolderInfo.PhoneMobile=
&CardHolderInfo.PhoneWork=
&CardHolderInfo.BillingAddressLine1=
&CardHolderInfo.BillingAddressLine2=
&CardHolderInfo.BillingAddressLine3=
&CardHolderInfo.BillingAddressCity=
&CardHolderInfo.BillingAddressState=
&CardHolderInfo.BillingAddressCountry=
&CardHolderInfo.BillingAddressZip=
&CardHolderInfo.ShippingAddressLine1=
&CardHolderInfo.ShippingAddressLine2=
&CardHolderInfo.ShippingAddressLine3=
&CardHolderInfo.ShippingAddressCity=
&CardHolderInfo.ShippingAddressState=
```

```
&CardHolderInfo.ShippingAddressCountry=
&CardHolderInfo.ShippingAddressZip=
&BrowserInfo.AcceptHeader=text%2Fhtml%2Capplication%2Fxhtml%2Bxml%2Capplication%2Fxml%3Bq%3D0.9%2Cimage
%2Favif%2Cimage%2Fwebp%2Cimage%2Fapng%2C%2A%2F%2A%3Bq%3D0.8%2Capplication%2Fsigned-
exchange%3Bv%3Db3%3Bq%3D0.9
&BrowserInfo.IPAddress=127.0.0.1
&BrowserInfo.Language=en-US
&BrowserInfo.ColorDepth=24
&BrowserInfo.ScreenWidth=2880
&BrowserInfo.ScreenHeight=1800
&BrowserInfo.TimeZone=40
&BrowserInfo.UserAgent=Mozilla%2F5.0%20%28Windows%20NT%2010.0%3B%20Win64%3B%20x64%29%20AppleWebKit%2F53
7.36%20%28KHTML%2C%20like%20Gecko%29%20Chrome%2F99.0.4844.51%20Safari%2F537.36
&BrowserInfo.JavaScriptEnabled=true
```

Respuesta de autenticación de 3D-Secure

Nuestra respuesta incluirá el elemento "**ThreeDSMethod**", con el subcampo "**MethodForm**" que genera un iframe oculto que ayuda a recopilar los datos del navegador para los emisores. Esta información se suma al perfil general del tarjetahabiente y ayuda a identificar transacciones potencialmente fraudulentas. También aumenta la probabilidad de una transacción exitosa y sin fricciones.

Deberá incluir "**MethodForm**" en su sitio web como iframe oculto. No se presenta ninguna pantalla de interfaz de usuario al tarjetahabiente.

En este punto, se realiza una solicitud de verificación para determinar si el sistema 3DSecure es funcional y el tarjetahabiente está inscrito en 3DSecure. Si el sistema del banco emisor no está funcionando o el banco emisor declina el intento de autenticación, la transacción será rechazada.

Si se verifica que la tarjeta está inscrita en el programa 3DSecure, la respuesta presentará los siguientes valores:

Campos de respuesta	
Campo	Descripción
AzulOrderId	Identificador único para la transacción.
IsoCode	3D2METHOD.
ResponseMessage	3D_SECURE_2_METHOD.
ThreeDSMethod / MethodForm	Datos de formulario HTML con iFrame oculto que se utiliza para recopilar los datos del navegador web para el emisor.

Ejemplo de respuesta JSON:

```
{
  "AuthorizationCode": "",
  "AzulOrderId": "39306",
  "CustomOrderId": "",
  "DateTime": "20200312100359",
  "ErrorDescription": "",
```

```
  "IsoCode": "3D2METHOD",
  "LotNumber": "",
  "RRN": "",
  "ResponseCode": "ISO8583",
  "ResponseMessage": "3D_SECURE_2_METHOD",
  "ThreeDSMethod": {
    "MethodForm": "<iframe xmlns=\"http:\/\/www.w3.org\/1999\/xhtml\" src=\"javascript:false;\"
style=\"width: 1px; height: 1px; display: none;\" name=\"tdsMmethodTgtFrame\"
id=\"tdsMmethodTgtFrame\">\u000a<!--.-->\u000a<\/iframe><form
xmlns=\"http:\/\/www.w3.org\/1999\/xhtml\" target=\"tdsMmethodTgtFrame\" method=\"post\"
action=\"https:\/\/dsx.modirum.com\/dstests\/ACSEmu2?handshake=1\" name=\"tdsMmethodForm\"
id=\"tdsMmethodForm\">\u000a<input
value=\"eyAidGhyZWVEU1NlcnZlclRyYW5zSUQiIDogIjY3NThiYmY1LThjOWYtNWNiNS04MDAwLTAwMDAwMDBiNDRjZiIsICJ0aHJ
lZURTTWV0aG9kTm90aWZpY2F0aW9uVVJMIiA6ICJodHRwOi8vd3d3LmZlZmVyZS5jb20vM2RzY2FwdHVyZS5hc3B4P3NpZD02MzcxOT
UyODAwNzU1MDcwNzMmcmVmZXJlbmNlZFRyYW5zYWN0aW9uSWQ9ODQ1Mjc2MjYwMTEiIH0\" name=\"3DSMethodData\"
type=\"hidden\"\/>\u000a<input
value=\"eyAidGhyZWVEU1NlcnZlclRyYW5zSUQiIDogIjY3NThiYmY1LThjOWYtNWNiNS04MDAwLTAwMDAwMDBiNDRjZiIsICJ0aHJ
lZURTTWV0aG9kTm90aWZpY2F0aW9uVVJMIiA6ICJodHRwOi8vd3d3LmZlZmVyZS5jb20vM2RzY2FwdHVyZS5hc3B4P3NpZD02MzcxOT
UyODAwNzU1MDcwNzMmcmVmZXJlbmNlZFRyYW5zYWN0aW9uSWQ9ODQ1Mjc2MjYwMTEiIH0\" name=\"threeDSMethodData\"
type=\"hidden\"\/>\u000a<\/form><script xmlns=\"http:\/\/www.w3.org\/1999\/xhtml\"
type=\"text\/javascript\">\u000adocument.getElementById(\"tdsMmethodForm\").submit();\u000a<\/script>"
  },
  "Ticket": ""
}
```


Solicitud y respuesta de notificación del método 3DS

El 3DSecure "**MethodForm**" se utiliza para proporcionar detalles del entorno del tarjetahabiente al servidor de control de acceso del banco emisor (ACS). El "**MethodForm**" contiene el código HTML para un iframe oculto que debe ser incluido en una página web del comercio. Esto obligará a que la información se publique automáticamente en el servidor ACS. La información HTML es un bloque HTML autónomo que no necesita ser modificado o publicado, ya que será cargada automáticamente cuando se renderice la página en la que está insertada. Alternativamente, esto se puede crear en una página que nunca se vuelve visible parar el comprador.

Si se recibe correctamente, los datos de la respuesta se publicarán en la URL proporcionada en el campo "**methodNotificationURL**" original y el mensaje publicado contendrá un campo "**threeDSServerTransID**" que contiene el ID de transacción ACS único asociado con la solicitud original. Tenga en cuenta que la carga útil de esta respuesta contará con un solo elemento llamado "**threeDSMethodData**". Ese elemento contendrá una respuesta JSON codificada en base64 que contiene el campo "**threeDSServerTransID**". Ejemplo:

```
<form name="frm" method="POST" action="{value from methodNotificationURL}">
  <input type="hidden" name="threeDSMethodData"
         value="eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6IjNhYzdjYWE3LWFhNDItMjY2My03OTFiLTJhYzA1YTU0MmM0YSJ9">
</form>
```

"**ThreeDSMethodData**" decodificado:

```
{
  "threeDSServerTransID": "3ac7caa7-aa42-2663-791b-2ac05a542c4a"
}
```

ThreeDSServerTransID

El "**threeDSServerTransID**" no es necesario para ningún procesamiento posterior de 3DS. Sin embargo, se recomienda guardar este valor para referencia al servidor ACS en el futuro, si es necesario.

Soporte del emisor 3DS

No todos los emisores soportan la recopilación de datos del navegador mediante el formulario del método 3DS "**methodForm**". En esos casos, no se recibirán datos en el "**methodNotificationURL**", y el flujo debe continuar enviando un estado de "**EXPECTED_BUT_NOT_RECEIVED**" (ver más abajo).

Se debe esperar un mínimo de 10 segundos para que se complete la operación POST anterior y luego determinar el valor de "**methodNotificationStatus**" de acuerdo a la siguiente tabla:

Valores de método	
Estado	Descripción
RECEIVED	Ha enviado el elemento "**methodNotificationURL**" en la solicitud de transacción de venta inicial y ha recibido la notificación de ACS en 10 segundos. Recibirá un mensaje HTTP POST de ACS, que contendrá un identificador de transacción ´único representado por "**threeDSServerTransID**".
EXPECTED_BUT_NOT_RECEIVED	Ha enviado el elemento "**methodNotificationURL**" en la solicitud de transacción de venta inicial y no ha recibido la notificación de ACS en 10 segundos.
NOT_EXPECTED	No ha enviado el elemento "**methodNotificationURL**" en la solicitud de transacción de venta inicial.

Solicitud "ProcessThreeDSMethod" para continuar con la autenticación 3DS

Una vez que se ha completado la llamada al método 3DS, debe notificar a la Integración vía API de AZUL que el proceso de autenticación puede continuar enviando el campo "**methodNotificationStatus**" con el valor según la condición correspondiente de la tabla anterior.

Este mensaje debe ser enviado a la Integración vía API utilizando una de las siguientes URL según el tipo de mensajería elegida:

- SOAP (método "**ProcessThreeDSMethod**"): pagos.azul.com.do/WebServices/SOAP/default.asmx
- JSON: https://pagos.AZUL.com.do/WebServices/JSON/default.aspx?processthreedsmethod

- Para ambiente de prueba, utilizar el dominio pruebas.AZUL.com.do

Campos de respuesta	
Campo	Descripción
Channel	Canal utilizando para la integración (valor proporcionado por AZUL).
Store	Merchant ID (MID) AZUL.
AzulOrderId	Identificador único para la transacción.
methodNotificationStatus	Enviar el valor según el estado de la notificación. Ver tabla de arriba.

Ejemplo de una solicitud que se enviará después de la visualización del formulario:

```
{
  "Channel": "EC",
  "Store": "MerchantID",
  "AzulOrderId": "39306",
  "MethodNotificationStatus": "RECEIVED"
}
```

Respuesta final de 3DS

Luego que el banco ha autenticado completamente al cliente y determina que no se requiere un desafío, se completa el proceso de 3DSecure y se procesa la autorización de la transacción.

A continuación, se recibirá un mensaje de respuesta con el mismo formato utilizado para el método de venta. Se debe evaluar el campo "**IsoCode**" con la respuesta ("**00**" es aprobada) y el campo "**ResponseMessage**" en caso de obtener una respuesta distinta a "**00**". En caso de que haya ocurrido algún error para procesar la autorización, el mismo será descrito en el campo "**ErrorDescription**".

Ejemplo de respuesta que recibe de la Integración vía API que indica que la autorización se ha realizado correctamente:

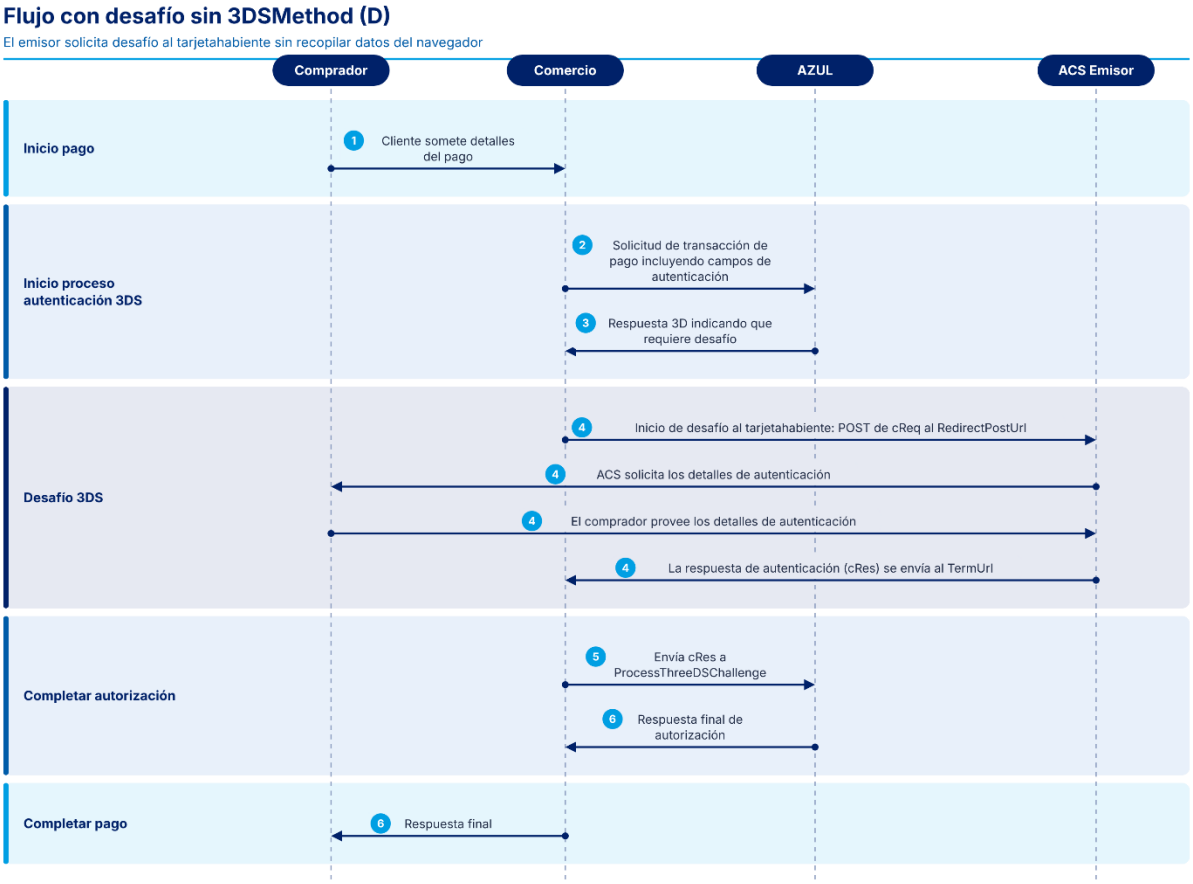
```
{
  "AuthorizationCode": "OK0937",
  "AzulOrderId": "39597",
  "CustomOrderId": "",
  "DataVaultBrand": "",
  "DataVaultExpiration": "",
  "DataVaultToken": "",
  "DateTime": "20200316102920",
  "ErrorDescription": "",
  "IsoCode": "00",
  "LotNumber": "1",
  "RRN": "202003161031175926O2",
  "ResponseCode": "ISO8583",
  "ResponseMessage": "APROBADA",
  "Ticket": "2"
}
```

Flujo con desafío

El flujo de desafío se activa cuando la transacción no se considera de bajo riesgo o cuando el emisor requiere autenticación por parte del titular. Este flujo inicia igual que el flujo sin fricción con una sola solicitud de transacción de Autorización o Venta inicial y dependiendo de la implementación del banco emisor podría iniciar en dos etapas:

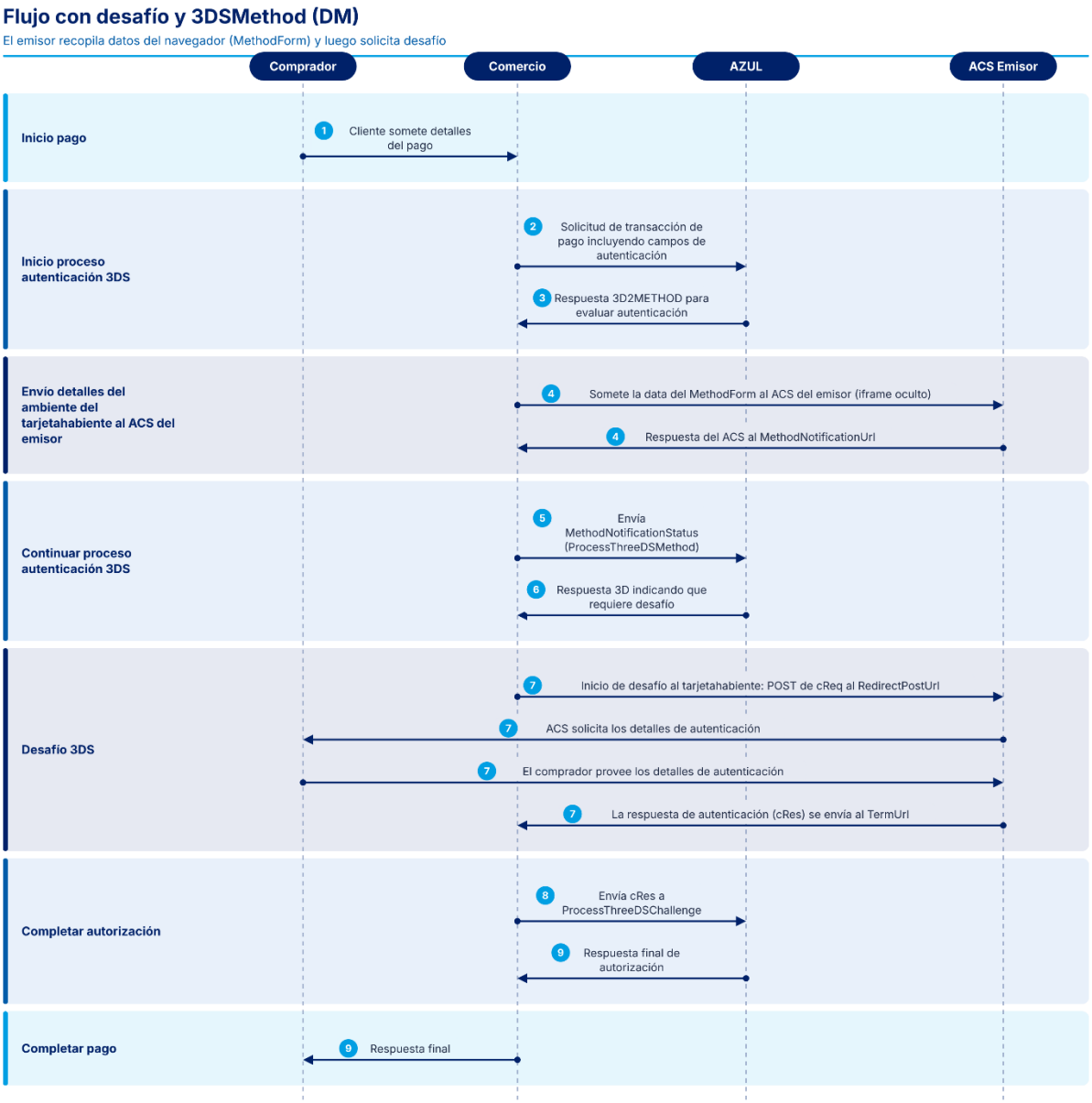
Desafío sin "threeDSMethod" (D)

Inicia igual que el flujo sin fricción, hasta el paso 2, pero en este caso el emisor no usa el campo "**MethodForm**" o decide desafiar al comprador de entrada. En el siguiente diagrama se muestra la secuencia del flujo de desafío sin el "**ThreeDSMethod**":



Desafío con "ThreeDSMethod" (DM)

Inicia igual que el flujo sin fricción hasta el paso 5. Se completa el "**ProcessThreeDSMethod**". En el siguiente diagrama se muestra la secuencia del flujo con desafío con el "**ThreeDSMethod**".



En ambos casos se recibe una respuesta con el "**IsoCode**" con valor "**3D**" con campos adicionales indicando que se requiere el desafío del tarjetahabiente.

Paso 3 (D) | 6 (DM): Integración vía API responde para continuar con la Autenticación del tarjetahabiente

Para el flujo de desafío, la respuesta contendrá los siguientes campos:

Campos de respuesta	
Campo	Descripción

AzulOrderId	Identificador único para la transacción.
DateTime	Fecha y hora transacción formato AAAAMMDDHHMMSS.
ThreeDSChallenge / creq	Un mensaje de solicitud codificado devuelto por el servidor ACS del banco emisor.
ThreeDSChallenge / RedirectPostURL	La URL del servidor ACS en la que se debe publicar el valor "**cReq**" para que se lleve a cabo un desafío del tarjetahabiente.
Campo	Valor
IsoCode	"**3D**"
ResponseCode	"**ISO8583**"
ResponseMessage	"**3D_SECURE_CHALLENGE**"

Ejemplo:


```
{
  "AuthorizationCode": "",
  "AzulOrderId": "39306",
  "CustomOrderId": "",
  "DateTime": "20200312100359",
  "ErrorDescription": "",
  "IsoCode": "3D",
  "LotNumber": "",
  "RRN": "",
  "ResponseCode": "ISO8583",
  "ResponseMessage": "3D_SECURE_CHALLENGE",
  "ThreeDSChallenge": {
    "CReq":
"ewogICAiYWNzVHJhbnNJRCIgOiAiNzlhZmU5MDUtN2E2Ni00OGZmLThkMmEtMDVjYjUyNWJlMWI2IiwKICAgImNoYWxsZW5nZVdpbm
Rvd1NpemUiIDogIjAzIiwKICAgIm1lc3NhZ2VUeXBlIiA6ICJDUmVxIiwKICAgIm1lc3NhZ2VWZXJzaW9uIiA6ICIyLjEuMCIsCiAgI
CJ0aHJlZURTU2VydmVyVHJhbnNJRCIgOiAiY2UyY2YxZTgtNWQ5YS01ZWZkLTgwMDAtMDAwMDAwNjMyZjRiIgp9",
    "MD": "",
    "PaReq": "",
    "RedirectPostUrl": "https:\/\/3ds-acs.test.modirum.com\/mdpayacs\/creq"
  }
}
```


Paso 4 (D) | 7 (DM): Redirección desafío al tarjetahabiente

Se debe hacer un POST con los datos recibidos en el campo "**cReq**" al "**RedirectPostUrl**" indicando, normalmente implementando como un formulario de envío automático (auto-submit). Esto debe implementarse dentro del sitio web del comercio. El tarjetahabiente será redirigido al ACS del emisor y se les presentará la interfaz de usuario para recopilar los detalles de autenticación. Por ejemplo, ingresar una contraseña única o realizar la autenticación usando su aplicación bancaria (autenticación fuera de banda). Una vez completada la autenticación, se redirige al consumidor a su página web.

Campos de entrada	
Asignación de nombres de campo	
Campo	Descripción

ThreeDSChallenge / creq	Mensaje de solicitud de desafío codificado en base64 completo como se obtuvo anteriormente. **Nota**: el nombre del campo "**creq**" es case-sensitive, por lo que debe ser enviado en minúscula.
ThreeDSChallenge / RedirectPostURL	La URL del comercio donde serán posteados los valores de respuesta con el resultado de la Autenticación del tarjetahabiente por el servidor ACS. Esta es la URL enviada en el paso 2.

Ejemplo:

Cuando se complete la autenticación, se publicará una respuesta en la URL especificada en el campo "**TermURL**".

Campos de respuesta	
Asignación de nombres de campo	
Campo	Descripción
ThreeDSChallenge / creq	El mensaje de repuesta de desafío codificado en base64 del servidor del emisor ACS.
ThreeDSChallenge / RedirectPostUrl	Los datos de sesión codificados en base64 del servidor Emisor ACS.

Ejemplo:

Paso 5 (D) | 8 (DM): Envio solicitud "ProcessThreeDSChallenge" para completar autorización

Después de recibir los datos de ACS, debe enviarlos los valores recibidos en el elemento "**cRes**" junto con la referencia a la transacción original. El comercio envía una solicitud utilizando el método "**ProcessThreeDSChallenge**" con los campos detallados abajo. Este mensaje debe ser enviado a la Integración vía API utilizando una de las siguientes URL según el tipo de mensajería elegida:

- SOAP (método "**ProcessThreeDSChallenge**"): pagos.azul.com.do/WebServices/SOAP/default.asmx
- JSON: https://pagos.AZUL.com.do/WebServices/JSON/default.aspx?processthreedschallenge
- Para ambiente de prueba, utilizar el dominio pruebas.AZUL.com.do

Campos de respuesta	
Campo	Descripción
Channel	Canal utilizado para la integración (valor proporcionado por AZUL).
Store	Merchant ID (MID) AZUL.

AzulOrderId	Identificador único para la transacción provisto por AZUL en el paso 3.
cRes	Valor devuelto por el ACS del emisor luego de la autenticación.

Ejemplo JSON de solicitud de "**ProcessThreeDSChallenge**" con el elemento "**cRes**":


```
{
  "Channel": "EC",
  "Store": "MerchantID",
  "AzulOrderId": "39306",
  "PaRes":
"eJzlWFmv47aS\/itB7qORaLet4PQBqF2yJFuLtb1pXy1Z+\/Lrr3xOd6fTyGBuBvMwwAgwTJbIYhWr+H0lvplZF8eMEYdjF7+\/KXH
f+2n8Sx59+fWmaycYPp9J5Nf3txvQ4\/5D\/DieYZI4krtwirs+b+p35Hf4d\/QN+tbdtXRh5tfD+5sftpSovhMfzxv0tfv2iDuReSd
JeH+wN+iz+wb9Oe82vlr9btGSR+\/OYMP+uZNtGb0nHnQW+jVSLknELcqXN+g14i3yh\/gdhVEEPqHwLwj5Bwz\/QeBv0If87flSBx7
NuOveR+yW\/Ch5233v4jpc31Fkn\/K99xYvz6aO9xG7c9\/bb9Cfxj39+h3+6dl179I303l\/G\/LHX43C0D9w8g36kL\/1gz+M\/bv
6Bn1tvUGvSdDHVr+\/GXla7+Iu\/mV5VHX\/5ddsGJ5\/QNA8z7\/P2O9Nl0LovhwEk9A+IOrz9F+\/fs6KI7FOmvc32q+bOg\/9Kt\
/8YQ+MEg9ZE\/0CqrTp8iF7\/J1KU39pRSCdpX\/b1f4WInj920sCYwix64f+XukP5v4nq\/xseNf7v\/WZ\/0o06CdF7296nMSvgMS
\/3HXxy6\/\/+iEBmTyN++F\/suK31X7U8E2f5Vdj\/B4f2\/p5LiVYuBIBTFh2flUo09kEK\/3ybd7nyDfou4lf7f8Wge++fA60bbS
8XEZ4o\/rAwybCzgefIoXhTmGiH9BKdSoRW+i89DYNIfRMepTiZJBB6PXGMxt2WZglSEQ+PeT2MCHAdtgoYy2vS+maOQneFT+ztBuMs
HyeVN6D8kbCHZK1oIT31eFmhFEShjDuDlpzl9zH1Q68XlsY4EikOqr7X1jNA6ISsO8ElOjLSDmvFHGkSBeSJPd25baT4tW+3CUnY2YW
uQhupQ\/x8MgKJ6\/mJ0js+vPpCdShbvHVSgcCurEBmw2OolIkK02h65LPGQxxrE3wOMCmcSEfyNkso7t5wI\/h0ioIWtAxbbD2Q4KD
2LJb7T4l7YoKdDfjY7kcQs6yolOahaTbPScqRcCXLz8kzdeIXOL1MwIOAZOMP\/ifLTruhjzZs3cHBUUU2dykaYDxKZhFCqSiFjt+gt
ekLKdGbWK5nYBkwgugUmnZZmXOkzNMAa3nAEPBitbPtOYylqbx7CxZ941VFdDzALmzdKawVlmZmslOCg1\/yhblYT2qzTUoKaj1KnwQ
WcRXU\/DgepFTq7D2ni56TzVH3QJUfbqO\/gxQfJFMUFCpalFAMQXOe4Yom3p3dQpsZNehViLHUSJbbSFmPYNHmGowOwtZqCoFWBRz\
/xXipjLKan\/IlFkxxfm7rKBQRYNnev7wQ2CAfrvDy03RtZlNP2QiAwbGtZen9yDX4FGNrsnKCig\/fKIyhTbL88Iy4PppY6NQMDJ5f
LVGNrwwJpA\/5b1CcbvPmLaIJki++qPwjFqGK5K5mDJGvLVFNDEEqP4Ma2uQH7uPr\/gY4sxornRpPDGbQhVoLEVpgElT9gaY\/b3W0
HubAle2RDDZgWSkb65QfuivVn9FTxTOWimnHy9KZsyEOthEhZFWZpNhkDSVoDkaXp1accuJZ3AAAWJABqZ78g3NnLPuEKJOJOlxVE2A
r8NjxBzjuCyEKN2exu0Yovb9KmZIZMnpbWYsToeR7pEeKkUlWXh+3IHkFnKskxAO5GOMk+1VCuxkiOwz7tRSIJpV2bFicL5C9uTQUCj
dqsLClXwTWre5yvrYpiOxyQ\/EKMmw6MYlh8qJsWxRYojENtrsQNQqRjIrzdcN0Oy+T\/LL+QYMn8qvHnz3F3mbt0OY3GyqqK8ySQ1u
Ap7Rict3D8swbZkdCIIum7LgoG1kB2BUChTCxWEsnK+wwtJgZgHwrzTQlfm15wqYX7GP2JmloFmjFQBm4ZU\/OlxQVDpzDbjHAO18jL
is8KalRRbVdv6MrbuAaOzspa54md09hndhjyW756D7OiM0vZ8d7c5RG6CznGsiQZ+v+Xly7SoLbXaMPs4OUQQoPH3Nf13b+54jztL8p
04F8DyPZnAkgKO8kpOLqfPP8\/fztYUMMF95KBh3lmHAhUrTjkpZjtL2NwVYP97pZ\/aygadCx6nkg+Kf2BU+5lnQPvblSlEuy10Geg
xmtdUfCiCYFdCBtMbLVs+bpwD8Y0+Zzz1ldzwSUuZvcAfscdhfl6XRcHLf8S09Umbq0cfWRiisuw6iFz1L7WGrKRVsKuZdDWD0hGlei
Tah0B1f7FI+zqt1kIpzdutHkNL96ezdEEDneH+4WcX91Azw45pbHbXhqu\/RaT6Xk2oca9oRIHnc9LU96vl91tpHYRnSJWvgc6tepDt
yeJhqKGFWOZxHMYGEaQ3XVLEwmSDKaYBRnX0Wrttpz56e8ErKUcHhj1YzxxvncM0UcdjobuDRa\/hTuLj35xwOyDSe+cmy6cnbUtw82
0e7FBbjxkWHZzlyCYEjUHbcDz5XxC0fAH\/OEos5cvEUw4\/zqkWtdJLP4fkwB\/jQD5GEC1wuSaIliaKaDbWrwVjhYW5VwNqLSH5mi
b+lDbHYYWduv9GGDi4nSr4aeHIx64s0XMY61vUE\/xm25B22Zv8n+LQs5QeYbEzqE+L3cwuGr9BpStUn7Bs2AXuONH5SA5EFNGXufdS
3dxpguS1EycK3Odi3yVHRm\/2cfkA4wy6c7TtqJvLWnqbIsM8pPIPSNRPE3AwvO7ghCpMuavGiBs7fZZuyveiDnXeawJVC8hVBW+gNS
J82uSaoLPMH6riws24blkopxnmWP2lRZlfvc122esH7Th+ftrn2nN5Ra92PzssOKsTUyUWrTzos2EqhlY\/92S0Iv1JmpaHkENjW+qL
I+33fi50mI7savZVitH9CExJWWGty004jHy1lBDSxKctBeJBXxcFltwBthTQtCSzfrzp35iP7WpVh2\/OIjltbfaaHCJV3kvGzJQuN2
r0W22kenKhi8OK5rvISGNJ6HkznNGa8Ozyn0r63Aur0RbW1vQQzV7zoz\/ChC469Tc4d2V825V4QjRMy5XIBw4CjJq+c\/DUx3OdIHx
8nVdyme1eF8q2xDMxNOt4qnaFAD0IoMkVRXbUNeIFcNFagIJHWCvrEcJts8EQd1aAgnFQ\/LVkEitN9NnuHt1fMd2FzhaK80N0w1821
Wu15ePZuRS7ptT521JScjtNj179T0yL5vjeAi08BhDUkG8XF6zGapt11je0bSeru32iCGk2aGgpw+4RPhQLJmaVMwABNgPYc+oA5Eei
Dwvezr7mch+\/Fw04LLvMqc75D8E43ruMLOhwyzSRjERatBPrKpY+ywCBnHy3nq\/YDlaTiLJvA5TLO8Byqd19ngtMb31FSi7fwiNlt
2OPP\/9fvP0oYQTt\/2gyUPWfcv0K4kKotOhyM\/YsBFkXc8fZMcSqLIu+UAnYKM1reEAOM2XOPnu8A4Ds+aIxc9\/PK0lPbHuraw4b
mGF5q2ZOKZbeESdr8eUS9q7XOeJDTfZ6cj2h7sLMK5H4RPY92HqG4U9Gt5enEHdFayzJEWzXxIb0J7pHyI39LtqmnDtUDIXYAEo3BL5
9bfjuEm3wHh8Ngb1OZNsxF0IExIlA9tFTCKDHAWu5St1ztU1l4S2WkW67MpDaHIBBPmxsWUHQODrFUkASb39a+uxhmmZ6F5eCyRYPkZ
nGsUSXcaBoaMaaykz5wT7TNSSnAcm0l9SbuIPR4Gvt2JQ\/U5vIEVAzGA87Y0fEOq1idVui2hJN2irLYxXzliN8u0CUIR+bWxCEpkjl
2yNqb7ZPYkKBFapWGvB2CEKP+Q6jmXlA9Hf+s8IcRMZTlWbMqqOvrhtwOt8H8mWnvrwr\/+d9W+C9o+l+o8PkCuN8q\/P1z7rPCt\/9
a4SsU7jAmuyk7mO+V\/Q7PIXy1ml2m\/Cz7P0Yx\/wCa1fKeVJfHsybQwRUxb6DUm31z8R6\/SDUkWHbIMQfDyv3rnbKzMx+v0RioUE
PPvDiUyWWZjJzR9YeR0HdRolrYrlgNG0MgBxB1EK+dPmtp3rdYoMKiJ4MQ3gTxudrO+PCbsj\/1\/g6cvY\/OXbBB7IC0pQIXUCNA07
VjIv8ikBJJtCXd4qZ36tlw3U\/bnDDlk0OTpvQG+H65cMNiCaHB3gwW2VQVWUp1MdTnaXo66zLJRk9DTtSd+ZNJp2iArItjc0V3g5Fx
T1O2lvYSwhNxGr3H2bwUownoxOhNCPDTwmSJfes6dgBHkw4Zsrs+SeY5O2puSPxtK8P73U4E\/r44KRm7aW6yDYni4f8PaKaWs7D6kQ
bsCqdGCrszC7ltnFqK28\/QvNv0FZrpGNk\/FW49AAe9URs4tGrkYMbh2XAjjQLcqaVrmeTizB\/xU4wdE4tX8+1arqJJAoFvuqOOyK
KfXZwDe3y0mun2Wy0ZROZIZ\/4cwjf4sew1chic1nLWiJlyW8dW0MC5PHPZjF3LThDQcXb7RFaSP+owuPq1XDxmVadAl67TsUI0Lzjd
FYxKSIOo4LHjFBneE+VMnciqigkHQ8WJLJIxHI+hL3aUXN6M5ei2h\/bM0j1+VnXjqh6gW\/sghWVGBAxaN7SVeXwzxdMiWQxreDzr+
JE805LDHK967KAcRA336NyiWFQ4XmC5uZiwZBx0eIohBEpVFi14KL\/eoiITRzkWUMQKTChaWUEAfwPN0J\/3MND3u5k\/b20+7n4\/
bp5fl6A\/3kj\/G2Hse1k=",
  "MD":
"MD_______359205020200312100359221 4XslDJDEA/Yarp9LHdBz5mqlYrzw=_____534537_____________30082630281_____
___________________170449200ww_____________________________________________________________________________
_____________returnurl?_____________________________________________________________________________________
_____________________________________VRQ17044920c7b8d5"
}
```

Paso 6 (D) | 9 (DM): Respuesta final de 3DS

Dado que esta transacción se inició como una venta (Sale) o pre-autorización (Hold), la autorización se realiza como parte de este paso final si la autenticación fue completada. Luego se recibirá la respuesta que debe ser evaluada con el campo "**IsoCode**" con el código de respuesta ("**00**" es aprobada) y el campo "**ResponseMessage**" con la descripción del código de respuesta.

Ejemplo JSON respuesta que indica autorización aprobada:


```
{
  "AuthorizationCode": "OK0937",
  "AzulOrderId": "39597",
  "CustomOrderId": "",
  "DataVaultBrand": "",
  "DataVaultExpiration": "",
  "DataVaultToken": "",
  "DateTime": "20200316102920",
  "ErrorDescription": "",
  "IsoCode": "00",
  "LotNumber": "1",
  "RRN": "202003161031175926O2",
  "ResponseCode": "ISO8583",
  "ResponseMessage": "APROBADA",
  "Ticket": "2"
}
```


Datos para pruebas

Estas son las tarjetas que se pueden utilizar en el ambiente de pruebas pruebas.AZUL.com.do:

#	Escenario	Tarjeta	Fecha de vencimiento	CVV
1	Sin fricción con 3DSMethod	4265*8800*0000*0007	12/2024	Cualquier número de 3 dígitos. (valor recomendado "**999**")
2	Sin fricción sin 3DSMethod	4147*4630*1111*0117		
3	Desafío con 3DSMethod	4005*5200*0000*0129		
4	Desafío sin 3DSMethod	4147*4630*1111*0059		

Tenga en cuenta que el propósito de las tarjetas de prueba 3DS es simular la respuesta de Autenticación del tarjetahabiente, lo que significa que no garantiza automáticamente la aprobación de autorización.

IMPORTNATE: Las tarjetas solo deben usarse para el escenario de autenticación / caso de prueba que admiten. **Hacer un mal uso de la tarjeta para cualquier otra autenticación, no proporcionará el resultado esperado**.

Para los casos de desafío, en el ambiente de prueba, se presentará la siguiente ventana en la que se podrán simular las diferentes respuestas posibles del ACS en este flujo:

#	Respuesta	Descripción

1	Yes	El emisor autenticó correctamente al tarjetahabiente, por lo que se procede a solicitar la autorización.
2	No	No se pudo autenticar al tarjetahabiente. En este escenario no se solicita la autorización y al completar el proceso se recibirá el mensaje con el ISO code "**99**" y el error "**Transaction declined. 3D Secure authentication failed.**"
3	Attempt	Se hace el intento de autenticar, pero el emisor o la tarjeta no participan en el programa por lo que la transacción es autenticada por la marca (Visa o Mastercard). El flujo continúa con la solicitud de la autorización.
4	Rejected	En este escenario el tarjetahabiente o el banco emisor decide no proceder con la autenticación. Se recibe el mensaje con el ISO code "**99**" y el error "**Transaction declined. 3D Secure authentication failed.**"
5	Unavailable	Este escenario simula cuando el servidor ACS del emisor no está disponible o no puede completar la autenticación por problemas técnicos. En este escenario no se solicita la autorización y al completar el proceso se recibirá el mensaje con el ISO code "**08**" y el error "**No autenticada**".

Soporte

Para solicitar soporte con cualquier duda o aclaración durante la implementación, puedes escribirnos a solucionesecommerce@azul.com.do o contactar directamente a tu oficial de negocios.