IMPLEMENTACIÓN DE AUTENTICACIÓN DEL TARJETAHABIENTE CON 3D SECURE 2.0 EN WEBSERVICE

DEPARTAMENTO DE SOLUCIONES DIGITALES PYME

12/13/22

SERVICIOS DIGITALES POPULAR

IMPLEMENTACIÓN DE AUTENTICACIÓN DEL TARJETAHABIENTE CON 3D SECURE 2.0

Tabla de Contenidos

IMPLEMENTACIÓN DE AUTENTICACIÓN DEL TARJETAHABIENTE CON 3D SECURE 2.0

Introducción

El entorno del comercio electrónico ha evolucionado significativamente durante la última década, lo que provocó un nuevo enfoque para reducir la fricción en la experiencia de transacciones con el servicio de Autenticación del Tarjetahabiente 3-D Secure.

EMVCo, en cooperación con las principales marcas de tarjetas, definió la nueva especificación EMV 3D Secure, conocida también como 3-D Secure 2.0, en beneficio de la industria para desarrollar en colaboración la próxima generación de protocolo 3-D Secure. La nueva versión promueve autenticación del consumidor sin fricciones y permite a los consumidores autenticarse con el emisor de su tarjeta cuando realizan compras de comercio electrónico.

El protocolo EMV 3-D Secure permite la autenticación e integración basadas en aplicaciones con billeteras digitales, así como las tradicionales transacciones de comercio electrónico basadas en navegador y ofrece funciones de seguridad líderes en la industria.

El propósito de este documento es brindarle una descripción general consolidada de la implementación de autenticación basada en navegador en nuestro servicio de WebServices AZUL.

En los ejemplos de mensajería el texto resaltado en amarillo muestra lo nuevo en comparación con el funcionamiento actual con la versión de 3D-Secure 1.

Vista general 3D-Secure 2.0

Si el comercio electrónico está habilitado con el Servicio de Autenticación del Tarjetahabiente, 3-D Secure (3DS), todas las transacciones de venta (Sale) o pre-autorización (Hold) realizadas con tarjetas Visa y Mastercard pasarán por defecto por el proceso de 3-D Secure, por lo que la autenticación se realiza en línea con el flujo de transacciones existente. El proceso comienza con la solicitud de una autorización de venta o Hold. Luego, la autorización se coloca en un estado de espera hasta que se completa el proceso de autenticación. Durante la autenticación, es posible que el comercio deba enviar información adicional una o más veces para hacer avanzar el flujo del proceso.

Al final del proceso de autenticación, la transacción original se actualiza con los resultados de la autenticación y se completa la autorización.

Es importante tener en cuenta que la funcionalidad de 3-D Secure (Autenticación del tarjetahabiente), aplica sólo para las transacciones que son de E-Commerce, donde el titular de la tarjeta es quien realiza la transacción en la plataforma del comercio y digita los datos de su tarjeta directamente.

IMPLEMENTACIÓN DE AUTENTICACIÓN DEL TARJETAHABIENTE CON 3D SECURE 2.0

La nueva versión del servicio de Autenticación del Tarjetahabiente con 3D-Secure 2.0 se implementa a partir de una transacción de venta o Hold enviando datos adicionales para la autenticación, y se definen 2 flujos posibles que puede tener el proceso de autenticación:

1. **Flujo sin fricción:** cuando el emisor no requiere que el tarjetahabiente complete un desafío para autenticarse.
2. **Flujo con desafío (o "challenge"):** cuando el emisor ha solicitado a su tarjetahabiente que proporcione detalles de autenticación adicionales.

ForceNo3DS

Para los casos de que se tenga el servicio para **activar el envío de las transacciones por los flujos de 3D-Secure** deberán enviar el campo con los siguientes valores:

ForceNo3ds = "0"; ForceNo3ds = Null; o ForceNo3ds = "".

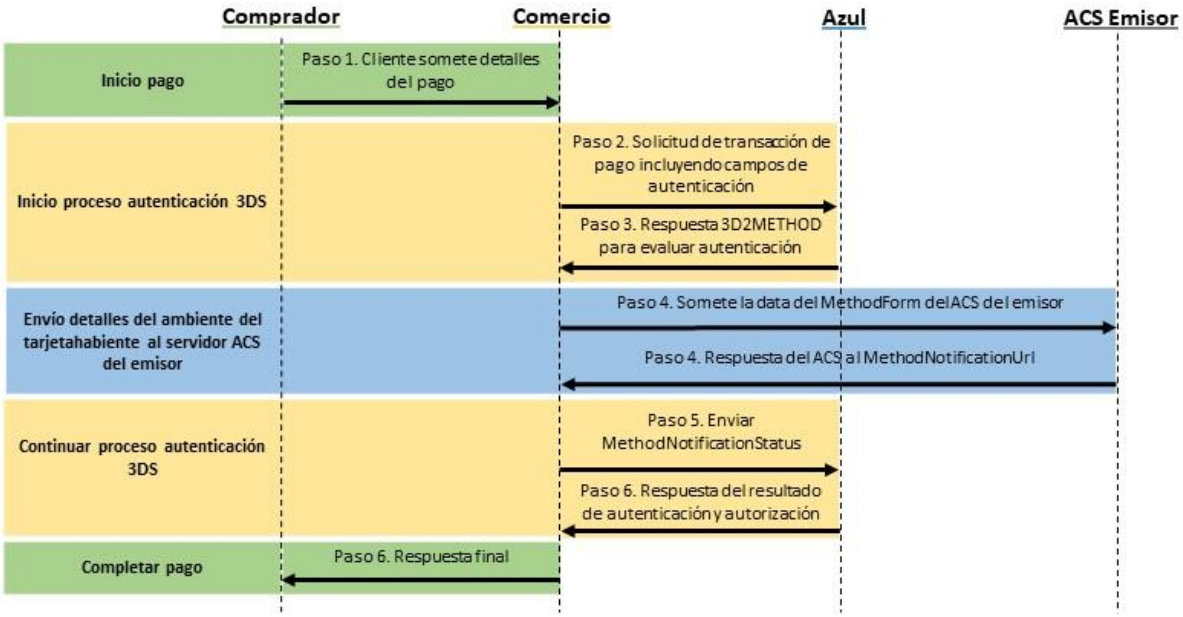
En caso de que se tenga el servicio de Autenticación del Tarjetahabiente habilitado y se desea enviar una transacción **que no pase por la autenticación con 3D-Secure**, se debe incluir en el mensaje inicial de Venta (Sale) o Hold el campo **ForceNo3DS = "1".**

Al enviar el campo **ForceNo3DS = "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 recibir un contra cargo en caso de que resulte ser fraudulenta.

Paso a paso: cómo implementar 3DSecure 2.0 Webservices AZUL

Flujo sin fricción (SF)

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



1. **Recopile los detalles de pago del tarjetahabiente:** primero, recopile la información de pago de la tarjeta (número de tarjeta de crédito o débito, fecha de vencimiento, código de seguridad) de su cliente.
2. **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 2.0 son:
    - **Sale:** Transacción de venta con captura inmediata
    - **Hold:** Transacción de venta con solo reserva de fondos

    Este mensaje debe ser enviado al Webservice de AZUL utilizando una de las siguientes URL según el tipo de mensajería elegida:
    - **SOAP** (método **ProcessPayment**): https://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 3-D Secure 2.0 se deben incluir en el mensaje de venta (Sale o Hold) dos campos o nodos adicionales, el "**ThreeDSAuth**", "**CardHolderInfo**" y "**BrowserInfo**", los cuales tienen sub-campos detallados a continuación:

    - **ThreeDSAuth**

Sub-campos	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=637195280075507073
RequestorChallengeIndicator	Este indicador sirve para comunicar al banco emisor la preferencia que tiene comercio de que se solicite el desafío

Valores RequestorChallengeIndicator:

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 que no se tenga la información de alguno de los campos, lo recomendable es omitir el campo en el mensaje, o sea que, no enviar el campo si está en blanco.**

Sub-campos:

Sub-campo	Descripción	Tamaño límite
BillingAddressCity	Ciudad de la dirección de facturación	96 caracteres incluyendo espacios
BillingAddressCountry	País de la dirección de facturación	Enviar código ISO 2 caracteres país*
BillingAddressLine1	Dirección de facturación – Línea 1	96 caracteres incluyendo espacios
BillingAddressLine2	Dirección de facturación – Línea 2	96 caracteres incluyendo espacios
BillingAddressLine3	Dirección de facturación – Línea 3	96 caracteres incluyendo espacios
BillingAddressState	Estado o provincia de la dirección de facturación	96 caracteres incluyendo espacios
BillingAddressZip	Código postal o "ZIP code" de la dirección de facturación	24 caracteres incluyendo espacios
Email	Dirección de correo electrónico	254 caracteres
Name	Nombre 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 postal 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 al Webservice 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.

Sub-campos:

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 pantalla
ScreenWidth	Dimensión de pantalla
ScreenHeight	Dimensión de pantalla
TimeZone	Zona Horaria
UserAgent	Detalles del Navegador del cliente
JavaScriptEnable	Habilitar JavaScript

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

Script de ejemplo para captura en navegador – JavaScript e impresión en 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>
```

* 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/XML (ver nodo BrowserInfo)

Utilizando el script de ejemplo anterior y TrxRequest fuera el objeto que representa la transacción que se va a enviar a AZUL, esta sería la forma de llenar los campos requeridos en un entorno de .NET Framework:

```
        // Get browser information (server side)

        TrxRequest.BrowserInfo.AcceptHeader = HttpContext.Request.ServerVariables["HTTP_ACCEPT"];
        TrxRequest.BrowserInfo.IPAddress = HttpContext.Request.ServerVariables["REMOTE_ADDR"];
        TrxRequest.BrowserInfo.UserAgent = HttpContext.Request.ServerVariables["HTTP_USER_AGENT"];

        // Get browser information (client side)

         TrxRequest.BrowserInfo.Language = HttpContext.Request.Form["BrowserLanguage"];
         TrxRequest.BrowserInfo.ColorDepth = HttpContext.Request.Form["BrowserColorDepth"];
         TrxRequest.BrowserInfo.ScreenWidth = HttpContext.Request.Form["BrowserScreenWidth"];
         TrxRequest.BrowserInfo.ScreenHeight = HttpContext.Request.Form["BrowserScreenHeight"];
         TrxRequest.BrowserInfo.TimeZone = HttpContext.Request.Form["BrowserTimeZone"];
         TrxRequest.BrowserInfo.JavaScriptEnabled = HttpContext.Request.Form["BrowserJavaScriptEnabled"];

              ...
```

Ejemplo mensaje SOAP/XML (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 en 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,application/signed-
exchange;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%3d637836351878902003
&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%2
                Cimage%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%2F537.36%20%2
                8KHTML%2C%20like%20Gecko%29%20Chrome%2F99.0.4844.51%20Safari%2F537.36
                &BrowserInfo.JavaScriptEnabled=true
```

3. 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 consumidor 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 3DSecure 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 contendrá los siguientes valores:

Atributo	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 utilizan para recopilar los datos del navegador web para el Emisor.

El siguiente documento JSON representa un ejemplo de respuesta:


```
{
   "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=\"eyAidGhyZWVEU1NlcnZlclRyYW5zSUQiIDogIjY3NThiYmY1LThjOWYtNWNiNS04MDAwLTAwMDAwMDBiNDRjZiIsICJ0aHJlZURTTWV0aG9kT
m90aWZpY2F0aW9uVVJMIiA6ICJodHRwOi8vd3d3LmZlZmVyZS5jb20vM2RzY2FwdHVyZS5hc3B4P3NpZD02MzcxOTUyODAwNzU1MDcwNzMmcmVmZ
```

```
XJlbm NlZFRyYW5zYWN0aW9uSWQ9ODQ1Mjc2MjYwMTEiIH0\" name=\"3DSMethodData\" type=\"hidden\"\/>\u000a<input
value=\"eyAidGhyZWVEU1NlcnZlclRyYW5zSUQiIDogIjY3NThiYmY1LThjOWYtNWNiNS04MDAwLTAwMDAwMDBiNDRjZiIsICJ0aHJlZURTTWV0
aG9kT
m90aWZpY2F0aW9uVVJMIiA6ICJodHRwOi8vd3d3LmZlZmVyZS5jb20vM2RzY2FwdHVyZS5hc3B4P3NpZD02MzcxOTUyODAwNzU1MDcwNzMmcmVmZ
XJlbm NlZFRyYW5zYWN0aW9uSWQ9ODQ1Mjc2MjYwMTEiIH0\" name=\"threeDSMethodData\"
type=\"hidden\"\/>\u000a<\/form><script xmlns=\"http:\/\/www.w3.org\/1999\/xhtml\"
type=\"text\/javascript\">\u000adocument.getElementById(\"tdsMmethodForm\").submit();\u000a<\/script>"
   },
   "Ticket":"" }
```


4. 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 para 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 contendrá 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 methodNotificationStatus de acuerdo a la siguiente tabla:

MethodNotificationStatus

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

5. Solicitud ProcessThreeDSMethod para continuar con la autenticación 3DS

Una vez que se ha completado la llamada al método 3DS, debe notificar al Webservice 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 al Webservice de AZUL utilizando una de las siguientes URL según el tipo de mensajería elegida:

- **SOAP** (método **ProcessThreeDSMethod**):

https://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.

Atributo	Descripción
Channel	Canal utilizado 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.

El siguiente documento JSON representa un ejemplo de una solicitud que se enviará después de la visualización del formulario:

```
{

        "Channel":"EC",
        "Store":"MerchantID",
        "AZULOrderId":"39306",
        "MethodNotificationStatus": "RECEIVED"

}
```

6. 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 de "**ErrorDescription**".

El siguiente documento JSON representa un ejemplo de una respuesta que recibe de la API que indica que la autorización se ha realizado correctamente:

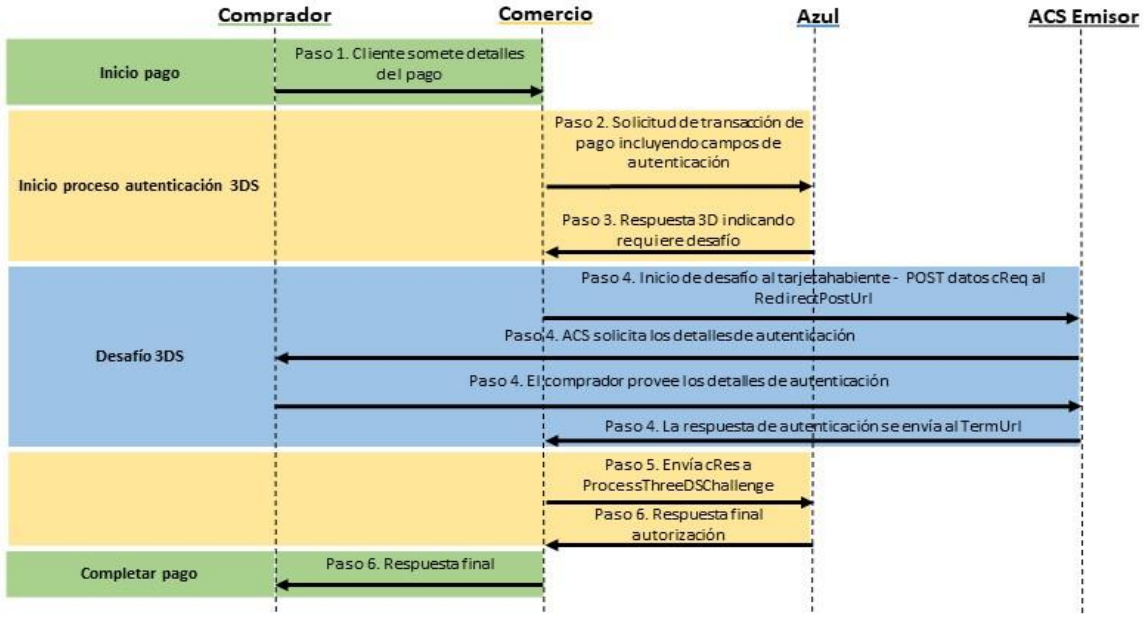
```
{
   "AuthorizationCode":"OK0937",
   "AZULOrderId":"39597",
   "CustomOrderId":"",
   "DataVaultBrand":"",
   "DataVaultExpiration":"",
   "DataVaultToken":"",
   "DateTime":"20200316102920",
```

```
   "ErrorDescription":"",
   "IsoCode":"00",
   "LotNumber":"1",
   "RRN":"20200316103117592602",
   "ResponseCode":"ISO8583",
   "ResponseMessage":"APROBADA",
   "Ticket":"2"
}
```

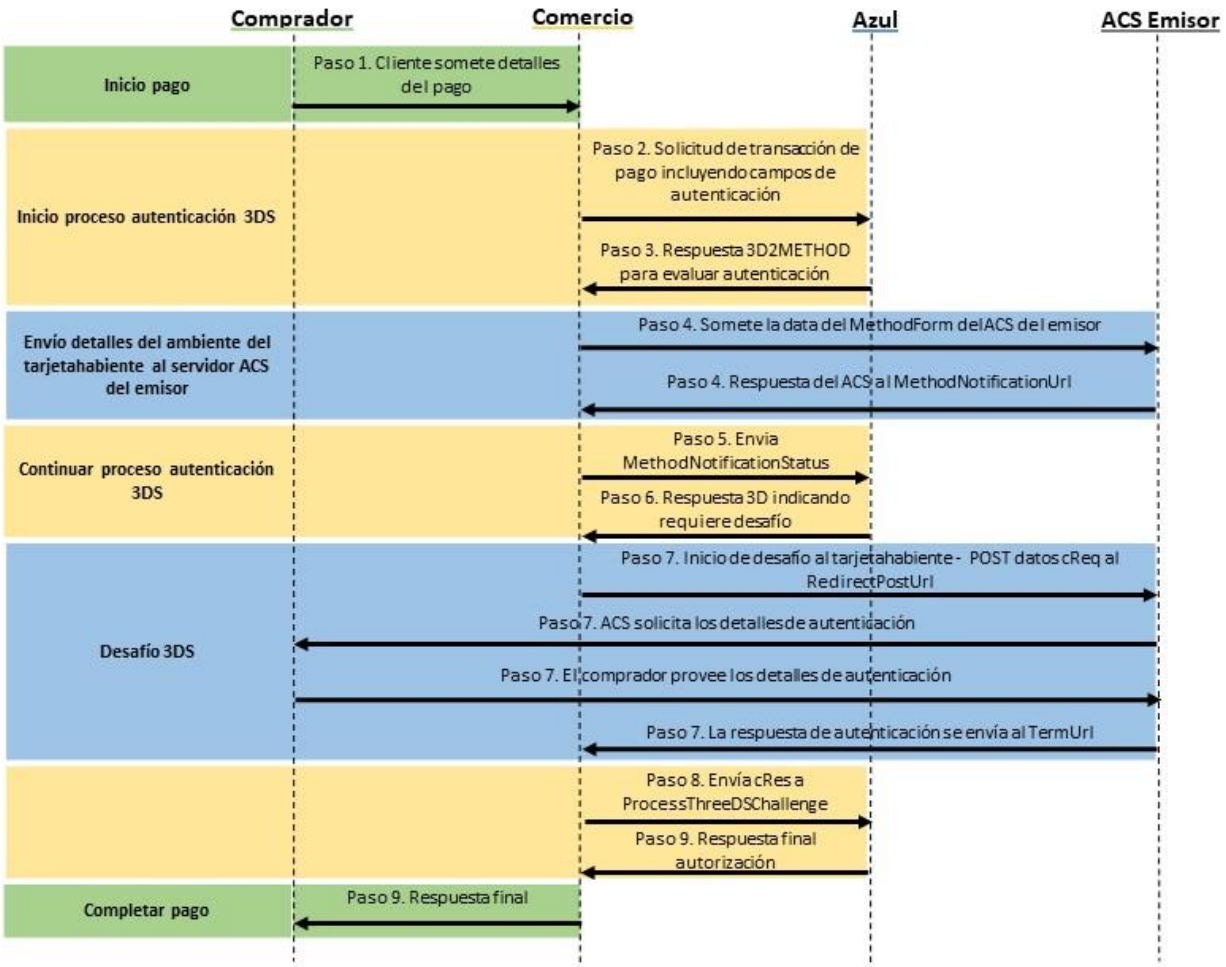

Flujo de desafío 3D-Secure 2.0

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

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



2. **Desafío con ThreeDSMethod (DM):** Inicia igual que el flujo sin fricción hasta el paso 5 (SF) donde se completa el **ProcessThreeDSMethod.** En el siguiente diagrama se muestra la secuencia del flujo de desafío con el **ThreeDSMethod**:



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

Paso 3 (D) | 6 (DM): Webservice AZUL responde para continuar con la autenticación 3DS

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

Atributo	Descripción o Valor
AZULOrderId	Identificador único para la transacción
DateTime	Fecha y hora transacción formato AAAAMMDDHHMMSS
IsoCode	"**3D**"
ResponseCode	"ISO8583"
ResponseMessage	"**3D_SECURE_CHALLENGE**"

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 el desafío del tarjetahabiente.

El siguiente documento JSON representa un ejemplo de respuesta:


```
{
   "AuthorizationCode":"",
   "AZULOrderId":"39306",
   "CustomOrderId":"",
   "DateTime":"20200312100359",
   "ErrorDescription":"",
   "IsoCode":"3D",
   "LotNumber":"",
   "RRN":"",
   "ResponseCode":"ISO8583",
   "ResponseMessage":"3D_SECURE_CHALLENGE",
   "ThreeDSChallenge":{
          "CReq":"ewogICAiYWNzVHJhbnNJRCIgOiAiNzlhZmU5MDUtN2E2Ni00OGZmLThkMmEtMDVjYjUyNWJlMWI2IiwKICAgImNoYWxsZW5nZVdp
bmRvd1NpemUiIDogIjAzIiwKICAgIm1lc3NhZ2VUeXBlIiA6ICJDUmVxIiwKICAgIm1lc3NhZ2VWZXJzaW9uIiA6ICIyLjEuMCIsCiAgICJ0aHJlZURTU
2VydmVyVHJhbnNJRCIgOiAiY2UyY2YxZTgtNWQ5YS01ZWZkLTgwMDAtMDAwMDAwNjMyZjRiIgp9",
          "MD":"",
          "PaReq":"",
          "RedirectPostUrl":"https:\/\/3ds-acs.test.modirum.com\/mdpayacs\/creq"
          },
   "Ticket":""
}
```


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

En el siguiente paso, se debe hacer un POST con los datos recibidos en el campo **cReq** al **RedirectPostUrl** indicado, normalmente implementado 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.

Asignación de nombres de campo

Esta información se publica utilizando los siguientes nombres de campo:

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.**

TermUrl= La URL del comercio donde serán posteados los valores de respuesta con el resultado de la autenticación del por el servidor ACS. Esta es la URL enviada en el paso 2.

Ejemplo:

```
<form name="frm" method="POST" action="https://3ds-acs.test.modirum.com/mdpayacs/creq ">
  <input type=”hidden” name=”creq” value=”ewogICAiYWNzVHJhbCIgOiA...wMDAtMDAwMDAwMDA0MWE5Igp9”>
  <input type=”hidden” name=”TermUrl” value=”http://www.mitienda.com/post3ThreeDs..”> </form>
```

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

Asignación de los nombres de campo

Esta información se publica con los siguientes nombres de campo:
cRes= El mensaje de respuesta de desafío codificado en base64 del servidor del emisor ACS.
threeDSSessionData= Los datos de sesión codificados en base64 del servidor Emisor ACS.

Ejemplo respuesta:

```
<form name="frm" method="POST" action="http://www.mitienda.com/post3ThreeDs..">
  <input type="hidden" name="cRes" value="ewogICAiYWNzUmVmZX…Fuc1N0YXR…IKfQ==">
  <input type=”hidden” name=”threeDSSessionData” value=”50F2156E03083CA665BCB4..”>
</form>
```

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

Después de recibir los datos de ACS, debe enviarnos 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 al Webservice de AZUL utilizando una de las siguientes URL según el tipo de mensajería elegida:

- **SOAP** (método **ProcessThreeDSChallenge**):
  https://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.

Atributo	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.

El siguiente documento JSON representa un ejemplo solicitud de **ProcessThreeDSChallenge** con el elemento **cRes**:


```
{
       "Channel":"EC",
       "Store":"MerchantID",
 "AZULOrderId":"39306",

"CRes":"ewogICAiYWNzUmVmZXJlbmNlTnVtYmVyIiA6ICJBQ1NFbXUyIiwKICAgImFjc1RyYW5zSUQiIDogIjAwMDAwMDAwLTAwMDUtNWE1
YS04MDAwLTAxNzBlM2M2MTg1YyIsCiAgICJtZXNzYWdlVHlwZSIgOiAiQ1JlcyIsCiAgICJtZXNzYWdlVmVyc2lvbiIgOiAiMi4xLjAiLAogICAidGhyZ
WEU1NlcnZlclRyYW5zSUQiIDogIjJkMWQzMTkyLWExMWUtNWI1MS04MDAwLTAwMDAwMDBiODJmNSIsCiAgICJ0cmFuc1N0YXR1cyIgOiAiWSIKfQ"      }
```


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.

El siguiente documento JSON representa un ejemplo de una respuesta que recibe que indica que la autorización fue 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:

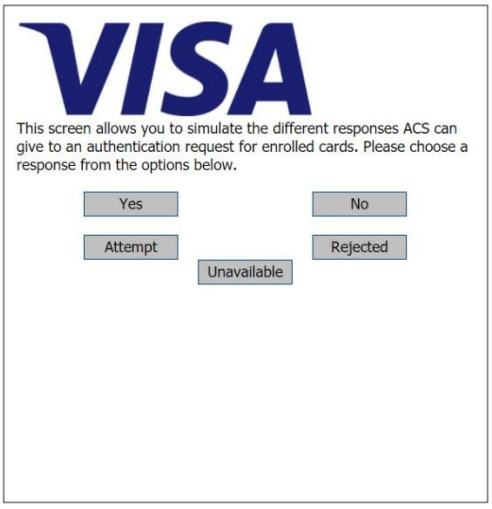
#	Escenario	Tarjeta
1	Sin fricción con 3DSMethod	4265*8800*0000*0007
2	Sin fricción sin 3DSMethod	4147*4630*1111*0117
3	Desafío con 3DSMethod	4005*5200*0000*0129
4	Desafío sin 3DSMethod	4147*4630*1111*0059

- Fecha de vencimiento para todas las tarjetas = 12/2024 o cualquier fecha futura.
- CVV cualquier número de 3 dígitos, valor recomendado = 999.

Tenga en cuenta que el propósito de las tarjetas de prueba 3DS es simular las respuestas de AUTENTICACIÓN, lo que significa que no garantizan automáticamente la aprobación AUTORIZACIÓN.

Las tarjetas de prueba solo deben usarse para el ESCENARIO DE AUTENTICACIÓN / CASO DE PRUEBA que admiten, haciendo un mal uso de la tarjeta para cualquier otra autenticación las respuestas no proporcionarán 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 que se pueden recibir 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.