

**worldpay**  
from FIS

Corporate Gateway

# Dynamic 3D Secure Guide

v1.3 October 2021

# Contents

<b>1 Dynamic 3D Secure</b>	<b>3</b>
1.1 Benefits	3
1.2 Supported card schemes	4
1.3 Enabling the service	4
1.4 Rules	4
1.5 Override	4
1.6 Fail-safe	5
1.7 Testing	5
<b>2 Rules for Dynamic 3D Secure</b>	<b>6</b>
2.1 Criteria for Dynamic 3D Secure rules	6
2.1.1 Issuer country	6
2.1.2 Bank Identification Numbers (BINs)	6
2.1.3 Order currency	7
2.1.4 Order amount	7
2.1.5 Payment method	7
2.2 Rules processing	8
2.2.1 Example of rules processing	8
2.3 Setting up or changing rules	9
<b>3 Turn 3D Secure On</b>	<b>10</b>
3.1 Benefits of using rules to turn off 3D Secure	10
3.2 How it works	11
3.3 Rules	11
<b>4 Turn 3D Secure Off</b>	<b>12</b>
4.1 Benefits of using rules to turn on 3D Secure	12
4.2 How it works	13
4.3 Rules	13
<b>5 Override element</b>	<b>14</b>
5.1 Prerequisites and risk	14
<b>6 Viewing Dynamic 3D Secure information in the Merchant Interface</b>	<b>15</b>
<b>7 Sample XML code with the override element</b>	<b>16</b>
7.1 Direct integration sample order	16
7.2 Hosted integration sample order	18
<b>8 About this guide</b>	<b>19</b>
8.1 Changes	19
8.2 Legal	19
8.3 Feedback	20
<b>9 Contact Us</b>	<b>21</b>

# 1 Dynamic 3D Secure

Control the 'Mode of Operation' of 3D Secure (3DS) by choosing when your customers are authorised:

- By eliminating authentication on selected shopper journeys, Dynamic 3DS can help to streamline the payment process for your shoppers

- By turning on 3DS, you can ensure that the liability shifts from yourself to the cardholder's issuer

## 3D Secure Turned On

- In this 'Mode of Operation', the default setting of 3DS is *on* and the payment will need to be authenticated.

- The rules you create will turn *off* 3DS, essentially bypassing it. When a rule is triggered, the shopper *will not* need to provide authentication.

**Note:** This is explained further in [Turn 3D Secure On on page 10](#).

## 3D Secure Turned Off

- In this 'Mode of Operation', the default setting of 3DS is *off* and the payment will not be required to provide authentication.

- The rules you create will turn *on* 3D Secure. When a rule is triggered, a shopper *must* provide authentication.

**Note:** This is explained further in [Turn 3D Secure Off on page 12](#).

**Warning:** Payments in which the cardholder is not authenticated receive no liability shift.

**Note:** When using Dynamic 3D Secure, 3DS will be turned *on* by default.

## 1.1 Benefits

Controlling authentication through Dynamic 3DS can bring the following benefits:

- Improved customer experience

- Fewer barriers to authorisation

- If you use more than one account to control 3DS, you may be able to simplify your integration to a single account

- Increased conversion

## 1.2 Supported card schemes

Card scheme	3D Secure
Visa	Verified by Visa
MasterCard	MasterCard SecureCode
American Express	SafeKey
JCB	J/Secure

**Note:** To comply with a security mandate for Maestro, we recommend that you continue to use 3DS for Maestro payments. Some territories may mandate 3DS be used in every transaction.

## 1.3 Enabling the service

To enable Dynamic 3D Secure on your account, contact Corporate Support or your Relationship Manager.

**Warning:** You may need to sign a waiver to use Dynamic 3D Secure. For more information, please contact your Relationship Manager.

## 1.4 Rules

You can create rules based on a number of criteria, such as issuer country and order amount. For each payment submitted, your rule base is evaluated to see whether a rule is triggered. Depending on the criteria that was set up (and which 'Mode of Operation' you're using) authentication will either be required or bypassed.

To learn more about the criteria, see [Criteria for Dynamic 3D Secure rules on page 6](#).

## 1.5 Override

Another feature of Dynamic 3D Secure is the override element, which allows you to manually override 3DS on a transaction-by-transaction basis.

With the override option, you explicitly state in the XML order whether 3DS should be used or not. The XML element `<dynamic3DS>` is available for this purpose, and is explained in [Sample XML code with the override element on page 16](#).

When you submit an XML order with the override element, any defined rules are ignored. The value of the override element indicates whether the cardholder must provide authentication or not for that payment.

You can also use the override element when no rules are specified.

## 1.6 Fail-safe

A fail-safe exists when using Dynamic 3D Secure, where if the Dynamic 3D Secure component fails, the system will default to attempting 3DS.

## 1.7 Testing

We recommend that you test rules in Sandbox, our secure-test system. You can also test the override XML element in Sandbox. Once you are satisfied with your testing, you can make the rules available in the live production environment. You can find out more about testing in the [WPG Integration guide](#).

## 2 Rules for Dynamic 3D Secure

To set up rules you specify characteristics called criteria. These rules, when applied, decide whether or not a shopper must authenticate their payment, depending on your chosen 'Mode of Operation'.

For more information, see:

[Criteria for Dynamic 3D Secure rules below](#)

[Rules processing on page 8](#)

[Setting up or changing rules on page 9](#)

### 2.1 Criteria for Dynamic 3D Secure rules

You can set up rules based on the following criteria:

- Issuer country
- Bank Identification Numbers (BINs)
- Order currency
- Order amount
- Payment method

#### 2.1.1 Issuer country

The issuer country is the country in which the cardholder's card was issued.

##### Conventions for specifying issuer country

You can specify multiple issuer countries per rule.

#### 2.1.2 Bank Identification Numbers (BINs)

On a credit or debit card, the Bank Identification Number (BIN) appears as the first six digits of the card number. It identifies the institution that issued the card.

**Note:** In 2022 card issuers begin to use the first eight digits of the PAN to form the BIN. You must have a separate rule for six and eight digit BIN payments. A six digit BIN will not be accepted on an eight digit BIN rule, and vice versa.

##### Conventions for specifying BINs

You can specify multiple BINs per rule

**Warning:** Each BIN must be a minimum of six digits long. Card schemes are set to change the BIN length to 8 digits in 2022. We recommend you prepare for this change in advance

You must specify individual BINs. BIN ranges are not allowed

To provide BINs to us, use a comma-separated values (CSV) file type

## 2.1.3 Order currency

In XML orders, the order currency is specified in the *currencyCode* attribute.

### Conventions for specifying order currency

You can only specify one currency per rule.

To specify a currency, use three uppercase letters as specified in the ISO-4217 standard.

Specifying an amount for the currency is optional.

For the full list of currencies we accept, see the [XML Direct Integration Guide](#) or the [XML Redirect Integration Guide](#).

## 2.1.4 Order amount

In XML orders, the order amount is specified in the *amount value* attribute.

### Conventions for specifying order amount

If you specify an order amount in a rule, you *must* also specify an order currency.

The order amount must contain minor units. For example, for the amount €35.00, specify 3500.

The order amount cannot be a negative value.

To specify an order amount for a rule, use one of the following equations:

The order amount is less (<) than a specific amount.

The order amount is equal to or greater (≥) than a specific amount.

## 2.1.5 Payment method

You can specify most payment methods for which we support 3D Secure. For a list of supported payment methods, see [Supported card schemes](#).

### Conventions for specifying payment method

You can specify multiple payment methods per rule.

The Carte Bleue and Carte Bancaire payment methods are not available as criteria. To ensure 3D Secure is bypassed for these payment methods, set the following criteria instead:

*Payment method:* Visa

*Issuer country:* France

## 2.2 Rules processing

There are many criteria you can choose from to require shoppers to either authenticate their payments using 3D Secure, or bypass the tool entirely. An example is outlined below of how the rules or criteria can be used to bypass 3D Secure when the merchant has 3DS turned *on*.

### 2.2.1 Example of rules processing

A medium-sized company in the Netherlands sells consumer goods in the following countries:

 The Netherlands (NL)

 Belgium (BE)

 Luxembourg (LU)

 Germany (DE)

 France (FR)

 Denmark (DK)

### Sample order

The company receives an XML order containing the following payment details:

*Issuer country:* FI (Finland)

*Payment method:* OTHER\_CARD

*Order currency:* EUR

*Order amount:* €10.50

The company has set up four rules for Dynamic 3D Secure. They are shown in the order of increasing risk, as perceived by the company.

*Rule 1:*

*Issuer country:* NL

*Payment method:* PREFERRED\_CARD-SSL

*Order currency:* EUR

*Rule 2:*

*Issuer country:* NL

*Order currency:* EUR

*Order amount:* < €100

*Rule 3:*

*Issuer country:* BE, LU, DE, FR, DK

*Order currency:* EUR

*Amount:* < €50

Rule 4:

Order currency: EUR

Amount: < €15

## Outcome

In this example, *Rule 4* applies. 3D Secure is *bypassed*. As the company's perceived risk increases, the order amounts for which they are willing to bypass 3D Secure become lower.

The issuer country is not the Netherlands or one of the countries that the company normally trades with. In addition, the shopper is not using the company's preferred payment card. For Rule 4, the company bypasses 3D Secure only when amounts are relatively small.

## 2.3 Setting up or changing rules

To set up or update rules, contact Corporate Support or your Relationship Manager.

When rules are set up or updated, there are a few things to consider:

By default, any new rule is enabled in the Sandbox secure-test environment.

To make a rule available in the live production environment, you must request that it be made live by contacting your Relationship Manager.

**Note:** Changes to rules take effect immediately.

## 3 Turn 3D Secure On

When you choose to turn on 3D Secure, the default setting is "on". Every shopper that wishes to make a payment *is required* to provide authentication.

You can choose criteria which, when triggered, mean that the shopper will not be required to provide authentication. For example, if a merchant from Germany has set up a rule meaning that shoppers paying in EUR and are spending under €50, and is buying from within Germany, will not need to provide authentication, then a shopper which meets that criteria *will not* be required to authenticate their payment.

**Note:** "3D Secure Turned On" is the default configuration of Dynamic 3D Secure.

**Warning:** Because the default setting of 3D Secure will be set to on, the liability of the payment lies with the cardholder's issuer. When the rule triggers and no authentication is required, the liability will shift to you.

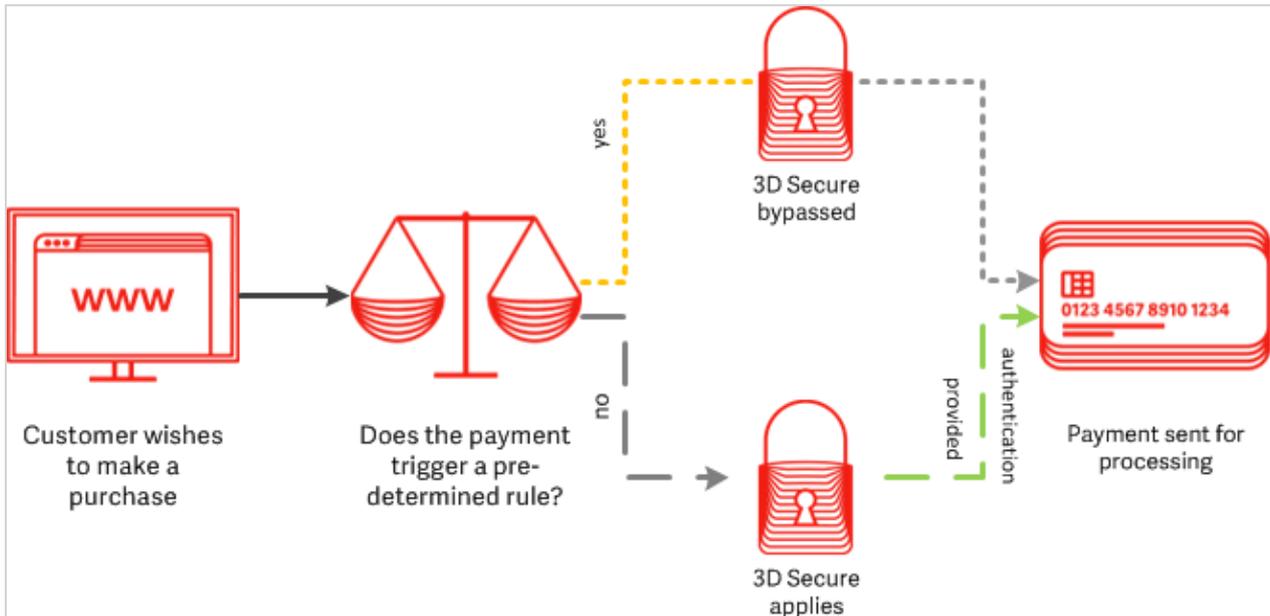
**Note:** If you are currently using 3D Secure Turned Off, and you wish to turn 3D Secure On, please talk to your Relationship Manager.

### 3.1 Benefits of using rules to turn off 3D Secure

Turning off 3D Secure for certain transactions can bring the following benefits:

- more streamlined customer experience
- More authorised transactions

## 3.2 How it works



### How it works

1. A shopper goes to your website and makes a payment.
2. When the payment is sent, your rule base is checked to see if the payment triggers one of your pre-determined rules.
  - a. If a rule is not triggered, then the shopper will need to authenticate their payment.
  - b. If the rule is triggered, then the shopper will not need to authenticate their payment.
3. The transaction is processed as usual.

## 3.3 Rules

Applying rules for 3D Secure Turned On works in the same way as applying rules for 3D Secure Turned Off. You can find out more about this in [Setting up or changing rules on page 9](#).

## 4 Turn 3D Secure Off

When you choose to turn off 3D Secure, the default setting is "off". Every shopper that wishes to make a payment to the merchant *will not* be required to provide authentication.

You can choose criteria which, when triggered, mean that the shopper will be required to provide authentication. For example, if a merchant from the United Kingdom has set up a rule meaning that shoppers paying in GBP and is spending over £50 will need to provide authentication, then a shopper which meets that criteria *will* be required to authenticate their payment.

**Note:** When 3D Secure is switched off, the liability of the payment becomes yours. It is only when the shopper is authenticated does the liability shift to the cardholder's issuer.

**Warning:** Turning 3D Secure off will remove any existing rules you have previously set up for turning on 3D Secure.

**Note:** If you are currently using 3D Secure Turned On, and you wish to turn 3D Secure Off, please talk to your Relationship Manager.

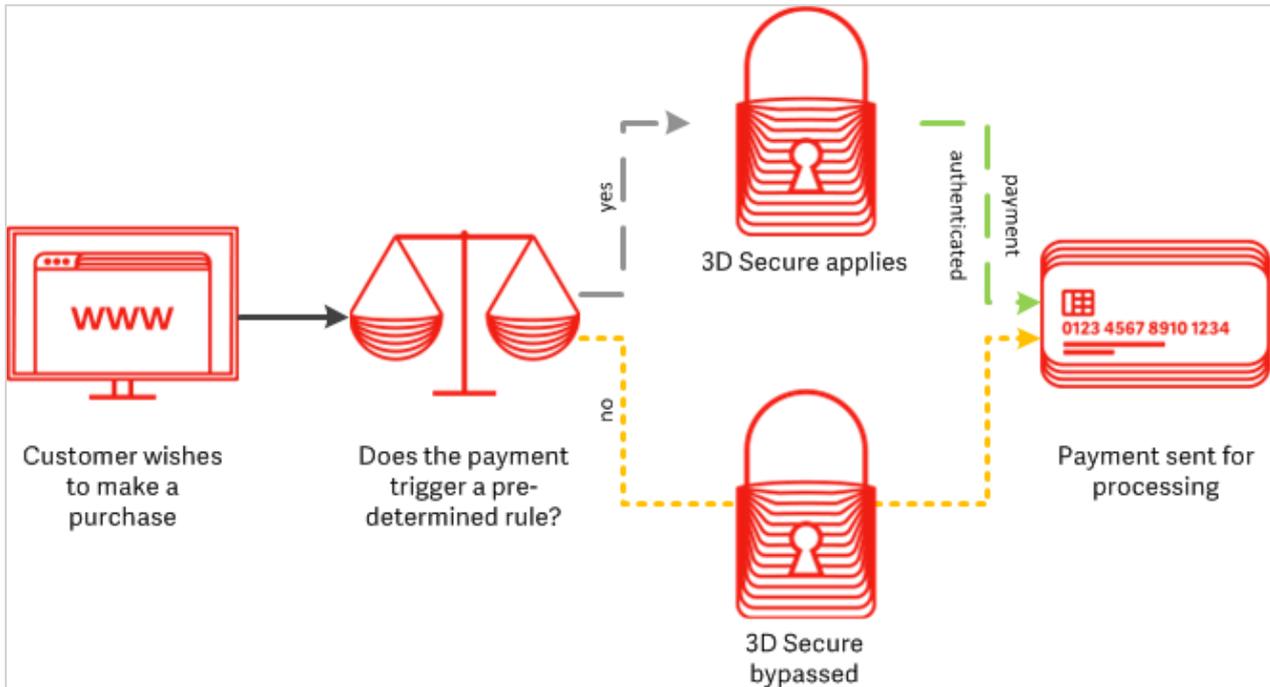
By eliminating authentication on shopper journeys, Dynamic 3D Secure helps to streamline the payment process for your customers, which may result in more authorised transactions.

### 4.1 Benefits of using rules to turn on 3D Secure

Turning 3D Secure on for certain transactions can bring the following benefits:

- ▣ Fewer chargebacks
- ▣ Liability shift from yourself to the cardholder's issuer
- ▣ Increased conversion rate

## 4.2 How it works



### How it works

1. A shopper goes to your website and makes a payment.
2. When the payment is sent, your rule base is checked to see if the payment triggers one of your pre-determined rules.
  - a. If the rule is triggered, then the shopper will be asked to authenticate their payment.
  - a. If no rule is triggered, the shopper will not need to authenticate the transaction and 3D Secure is bypassed.
3. If the payment is authenticated, the transaction will be processed as usual.

**Warning:** Payments in which the cardholder is not authenticated receive no liability shift.

## 4.3 Rules

Applying rules for 3D Secure Turned Off works in the same way as applying rules for 3D Secure Turned On. You can find out more about this in [Setting up or changing rules on page 9](#).

## 5 Override element

You can optionally include an override element in your XML order code on a transaction-by-transaction basis.

The override element specifies whether 3D Secure should take place. When you submit an order with the override element, any rules are ignored.

Use the `<dynamic3DS>` element to specify whether 3D Secure should take place. You can set the element's attribute, `overrideAdvice`, to one of the following values:

Attribute value	Meaning
do3DS	Perform 3D Secure for this order. Ignore any configured rules.
no3DS	Do not perform 3D Secure for this order. Ignore any configured rules.

You can also use the override element if you don't have rules set up.

Using the override element could simplify your integration and reporting. If you currently use two accounts to control 3D Secure, you may be able to simplify your integration to a single account.

For an example XML order code containing the `<dynamic3DS>` element, see [Sample XML code with the override element on page 16](#).

### 5.1 Prerequisites and risk

Payments in which the cardholder is not authenticated receive no liability shift.

To use the override element, you must have Dynamic 3D Secure enabled for your account. If Dynamic 3D Secure is not enabled and you submit an order with the override element, the following error is generated:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE paymentService PUBLIC "-//WorldPay//DTD WorldPay PaymentService v1//EN"
"http://dtd.worldpay.com/paymentService_v1.dtd">
<paymentService version="1.4" merchantCode="DEMO">
  <reply>
    <error code="5">
      <![CDATA[3DS overrideAdvice attempted but 3DS override not enabled.]]>
    </error>
  </reply>
</paymentService>
```

Code example 1: An example payment response showing that 3DS cannot be overridden as it is not enabled

## 6 Viewing Dynamic 3D Secure information in the Merchant Interface

When a rule is triggered for a payment, you can view its criteria in the Merchant Interface (MI).

To view *Dynamic 3D Secure* information for a payment:

1. In the MI, click *Payments* and then click the *Transaction ID* to display detail about a specific payment.

Payments			
<b>Payment and Order Details</b>			
<b>Order Details</b>			
transaction ID	jspxml3704140699	merchant	test-merchant.com
amount	EUR 100.00	shopper email	testshopper@worldpay.com
date - time	01/Sep/2015 - 14:41	description	test order
card ID		created by	Unknown
<b>Payment Details</b>			
creation date	01/Sep/2015 - 15:41	transaction ID	jspxml3704140699
amount	EUR 100.00	status	AUTHORISED
amount in settlement currency	not yet available	brand-protocol	VISA_CREDIT-SSL
last update	01/Sep/2015 - 14:41	Dynamic 3DS	<a href="#">Show rule</a>
cardholder name	AUTHORISED	customer phone number	
customer interaction	Cardholder Authenticated		
customer address	Worldpay 270-289 The Science Park Milton Road Cambridge CB4 0WE UNITED KINGDOM		
<b>Risk Details</b>			
Security Level	Acquirer returned		
AVS	E - Postcode and address not checked		
CVC	C - CVV/CVC not checked		

**Note:** If no rules are triggered for a payment, the *Dynamic 3DS* field is not displayed.

2. Under *Payment Details*, where it says *Dynamic 3DS*, click *Show rule*.

A new tab will open and the criteria for the rule are displayed. The rule's unique ID number is also displayed.

WorldPay - Payments		Dynamic 3DS	
<b>Dynamic 3DS Rule 1000349</b>			
<b>General</b>			
<b>Order currency</b>	<b>Order amount</b>		
EUR	≥ 10.00		

When you click *Show rule*, you will be able to see which rule was activated. For example, in the above figure, you can see that shoppers who are paying in Euros, and are spending over €10, must provide authentication.

**Note:** You can find out more about the rules you're able to select by heading over to .

## 7 Sample XML code with the override element

The `<dynamic3DS>` element specifies whether Dynamic 3D Secure should be carried out for the order. It can contain the `overrideAdvice` attribute. To specify whether 3D Secure should take place, you can set the attribute to one of the following values:

Attribute value	Meaning
do3DS	Perform 3D Secure for this order. Ignore any configured rules.
no3DS	Do not perform 3D Secure for this order. Ignore any configured rules.

### 7.1 Direct integration sample order

```

<?xml version="1.0"?><!DOCTYPE paymentService PUBLIC "-//WorldPay//DTD WorldPay
PaymentService v1//EN" "http://dtd.worldpay.com/paymentService_v1.dtd">
<paymentService version="1.4" merchantCode="MYMERCHANT">
  <submit>
    <order orderCode="T0211010">
      <description>Order description</description>
      <amount value="5000" currencyCode="EUR" exponent="2"/>
      <orderContent>
        <![CDATA[]]>
      </orderContent>
      <paymentDetails>
        <MAESTRO-SSL>
          <cardNumber>6759xxxxxxxxx8453</cardNumber>
          <expiryDate>
            <date month="06" year="2019"/>
          </expiryDate>
          <cardHolderName>J. Shopper</cardHolderName>
          <startDate>
            <date month="06" year="2010"/>
          </startDate>
          <issueNumber>0</issueNumber>
          <cvc>123</cvc>
          <cardAddress>
            <address>
              <firstName>John</firstName>
              <lastName>Shopper</lastName>
              <address1>Shopperstreet</address1>
              <address2>Shopperaddress2</address2>
              <address3>Shopperaddress3</address3>
              <postalCode>1234</postalCode>
              <city>Shoppercity</city>
              <countryCode>NL</countryCode>
            </address>
          </cardAddress>
        </MAESTRO-SSL>
        <session shopperIPAddress="127.0.0.1" id="ssn505847750"/>
      </paymentDetails>
      <shopper>
        <shopperEmailAddress>jshopper@example.com</shopperEmailAddress>
        <browser>
          <acceptHeader>text/html</acceptHeader>
          <userAgentHeader>Mozilla/5.0 ...</userAgentHeader>
        </browser>
      </shopper>
      <dynamic3DS overrideAdvice="do3DS"/>
    </order>
  </submit>
</paymentService>

```

Code example 2: An example Direct integration order with the `<dynamic3DS>` element

## 7.2 Hosted integration sample order

```
<?xml version="1.0"?><!DOCTYPE paymentService PUBLIC "-//WorldPay//DTD WorldPay
PaymentService v1//EN" "http://dtd.worldpay.com/paymentService_v1.dtd">
<paymentService version="1.4" merchantCode="MYMERCHANT ">
  <submit>
    <order orderCode="T0211010">
      <description>Order description</description>
      <amount value="5000" currencyCode="EUR" exponent="2"/>
      <orderContent>
        <![CDATA[]]>
      </orderContent>
      <paymentMethodMask>
        <include code="ALL"/>
      </paymentMethodMask>
      <shopper>
        <shopperEmailAddress>jshopper@example.com</shopperEmailAddress>
      </shopper>
      <billingAddress>
        <address>
          <firstName>John</firstName>
          <lastName>Shopper</lastName>
          <address1>Shopperstreet</address1>
          <address2>Shopperaddress2</address2>
          <address3>Shopperaddress3</address3>
          <postalCode>1234</postalCode>
          <city>Shoppercity</city>
          <countryCode>NL</countryCode>
        </address>
      </billingAddress>
      <dynamic3DS overrideAdvice="no3DS"/>
    </order>
  </submit>
</paymentService>
```

Code example 3: An example Hosted integration order with the `<dynamic3DS>` element

## 8 About this guide

### 8.1 Changes

Version history.

Version	Change Description	Date
1.3	Update BIN range advice in preparation for eight digit BIN in 2022	October 2021
1.2	Template update.	December 2019
1.1	Moved into new template. Homepage content changed. Introduction, Supported Card Schemes, and Enabling Dynamic 3D Secure content moved to <i>Dynamic 3D Secure on page 3</i> .	October 2016
1.0	New guide.	January 2016

### 8.2 Legal

© FIS 2021, and/or its subsidiaries. All rights reserved.

Worldpay (UK) Limited (Company No. 07316500 / FCA No. 530923), Worldpay Limited (Company No. 03424752 / FCA No. 504504), Worldpay AP Limited (Company No: 05593466 / FCA No: 502597). Registered Office: The Walbrook Building, 25 Walbrook, London EC4N 8AF and authorised by the Financial Conduct Authority under the Payment Service Regulations 2017 for the provision of payment services. Worldpay (UK) Limited is authorised and regulated by the Financial Conduct Authority for consumer credit activities. VAT number: 991 2802 07

Worldpay B.V. has its registered office in Amsterdam, the Netherlands (Handelsregister KvK no. 60494344). WPBV holds a licence from and is included in the register kept by De Nederlandsche Bank, which registration can be consulted through [www.dnb.nl](http://www.dnb.nl).

We use Google code-prettify to syntax highlight the code examples in this guide.

Copyright 2021 Worldpay

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at: <http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for specific language governing permissions and limitations under the License.

To find out more, get in touch with your corporate support manager or:

See our contact details at: [www.worldpay.com/global/about/contact-us](http://www.worldpay.com/global/about/contact-us)

## 8.3 Feedback

We'd really appreciate your feedback on this guide. If you have any comments or suggestions, please let us know.

You can email us at: [guides@worldpay.com](mailto:guides@worldpay.com)



## 9 Contact Us

To find out more, get in touch with your Relationship Manager  
or:

Email [corporatesupport@worldpay.com](mailto:corporatesupport@worldpay.com)

© FIS 2021, and/or its subsidiaries. All rights reserved.