



# PrestaShop Extension

Hosted Payment Pages V2

April 5<sup>th</sup> 2016

## Contents

|  |   |
|--|---|
| About this guide.....                            | 3 |
| Copyright.....                                   | 3 |
| Introduction .....                               | 3 |
| Installation .....                               | 4 |
| Configuring PrestaShop .....                     | 5 |
| Payment page customisation.....                  | 6 |
| Verified by Visa and MasterCard SecureCode ..... | 6 |
| Live Transactions.....                           | 6 |
| Test Cards.....                                  | 7 |
| Simulating decline/error responses.....          | 7 |

## About this guide

This guide describes the specifications of the PrestaShop extension for Telr. The intended audience is the merchant's technical staff or the merchant's system integrator.

## Copyright

© 2016 Telr. All rights reserved.

While every effort has been made to ensure the accuracy of the information contained in this publication, the information is supplied without representation or warranty of any kind, is subject to change without notice and does not represent a commitment on the part of Telr. We assume no responsibility and shall have no liability, consequential or otherwise, of any kind arising from this material or any part thereof, or any supplementary materials subsequently issued by Telr. Telr has made every effort to ensure the accuracy of this material.

## Introduction

The Telr PrestaShop Extension allows merchants who use the PrestaShop system to take payments via the Telr Hosted Payment Pages. No card details are captured by or stored within the PrestaShop system, so there are no PCI requirements for the store.

When the customer places their order and selects Telr as the payment method, they will be taken to the Telr secure server to enter their card details. The result of the purchase attempt (authorised or otherwise) is sent back to the PrestaShop system to update the order details. The customer is also returned to the store.

The extension has been tested with PrestaShop 1.6.1.4

## Installation

You will need to download the TelrPrestaShop.zip file, and transfer this to the server that is running your PrestaShop store.

This contains a directory 'modules' which contains the Telr extension.

**You should take a back-up of your system before installing the extension.**

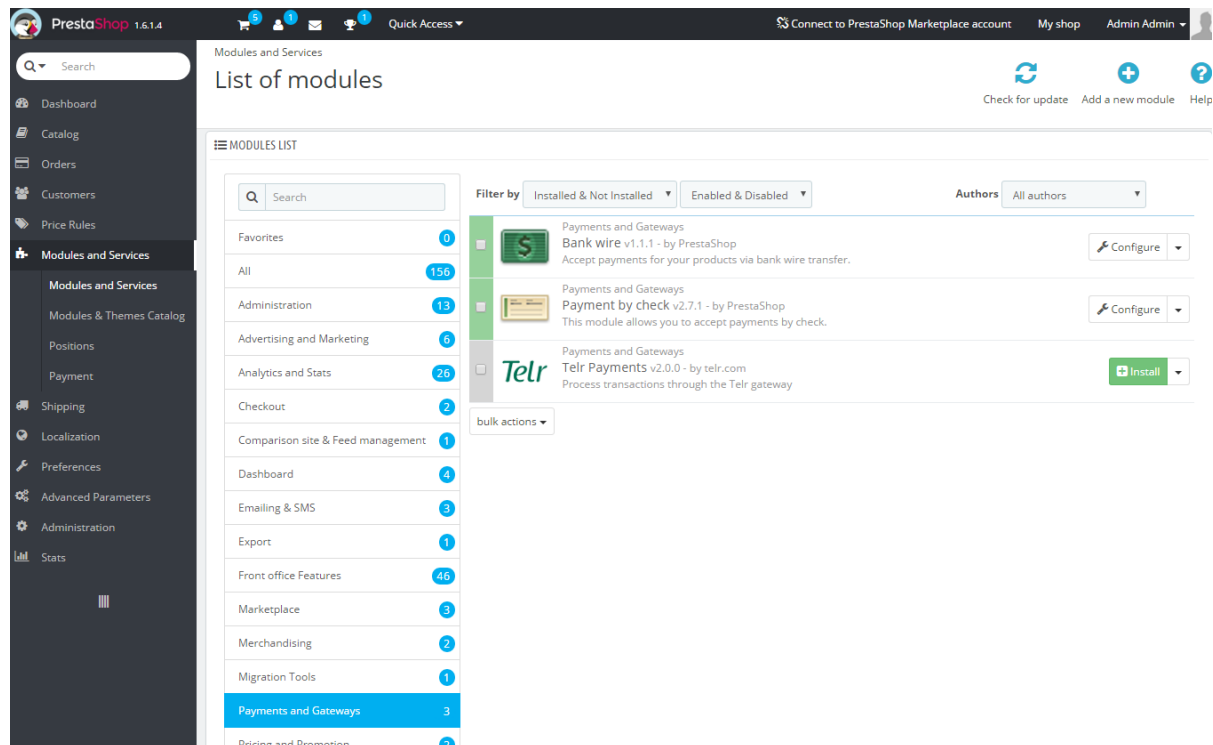
Copy the 'modules' directory from the zip file to your main PrestaShop installation - there will already be a modules directory within your installation, the content of the zip will be added to these.

You should end up with the Telr module installed as modules/telr and not as modules/modules/telr.

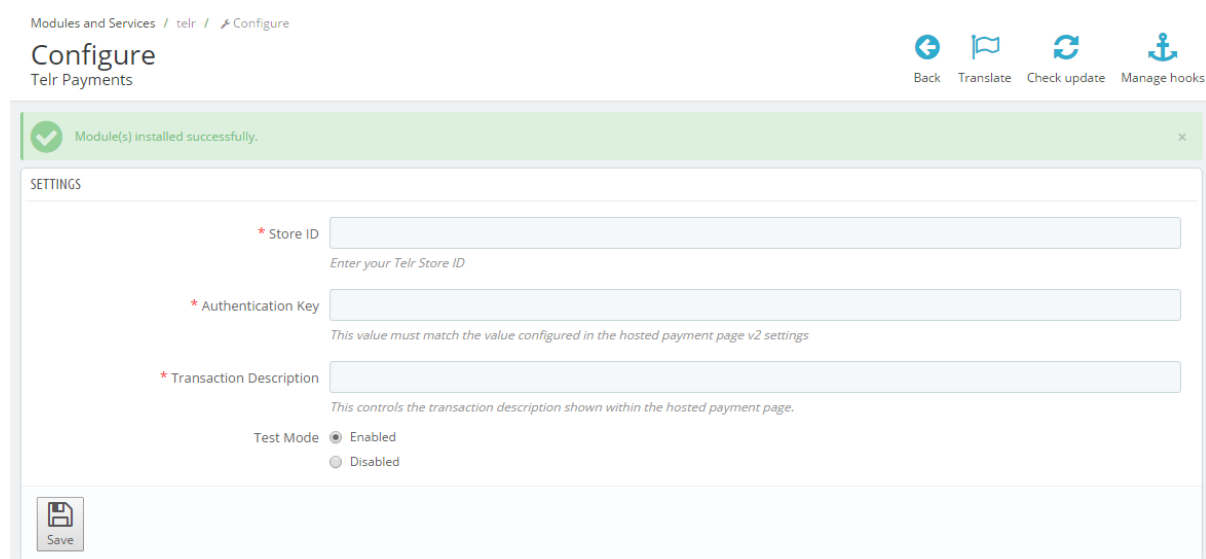
## Configuring PrestaShop

From the PrestaShop admin system, select Modules and Services from the side menu. Within this, select Payments and Gateways, and set the filter to Installed & Not Installed.

This will list the payment modules available, you will need to click on Install next to the Telr module. PrestaShop may ask you to confirm the installation, click on 'Proceed with the installation'.



You then need to edit the settings for the payment method. Your Telr Store ID is displayed in the top right of the Telr Merchant Administration System, and you must only enter the numeric part of the ID, not the full store name. The authentication key can be found in Telr Merchant Administration System in Hosted Payment Page V2 configuration page, under the Integrations menu.



## Payment page customisation

The payment page can be customised through the use of a CSS file. The core page display is based on the Bootstrap 3 responsive layout. You should ensure that you are familiar with the underlying styles used within Bootstrap before making any CSS changes. For more details please check the Hosted Payment Page integration guide.

## Verified by Visa and MasterCard SecureCode

After the consumer enters their card details, the payment gateway will check to see if that card is enrolled as part of the Verified by Visa or MasterCard SecureCode authentication systems (known as 3D-Secure).

If the card is part of one of these authentication systems, then an additional page is displayed which requires the relevant authentication details to be entered. This is usually in the form of a password that has been assigned by the consumer or via a one-time code sent to the customers mobile.

The actual data entry section is presented directly by the card issuer and cannot be customised. It is generally displayed on a white background.

Where possible the 3D-Secure authentication form is displayed over the payment page, allowing the customer to see that it is clearly part of the payment process.

## Live Transactions

When you are ready to start processing live transactions, you must ensure that the IP details of your PrestaShop server have been entered into the Payment Page V2 configuration with the Telr Merchant Administration System.

## Test Cards

These card numbers can be used when testing your integration to the payment gateway. These cards will not work for live transactions.

| Card number         | Type             | CVV  | MPI |
|---------------------|------------------|------|-----|
| 4000 0000 0000 0002 | Visa             | 123  | No  |
| 4111 1111 1111 1111 | Visa             | 123  | Yes |
| 4444 3333 2222 1111 | Visa             | 123  | Yes |
| 4444 4244 4444 4440 | Visa             | 123  | Yes |
| 4444 4444 4444 4448 | Visa             | 123  | Yes |
| 4012 8888 8888 1881 | Visa             | 123  | Yes |
| 5105 1051 0510 5100 | Mastercard       | 123  | No  |
| 5454 5454 5454 5454 | Mastercard       | 123  | Yes |
| 5555 5555 5555 4444 | Mastercard       | 123  | Yes |
| 5555 5555 5555 5557 | Mastercard       | 123  | Yes |
| 5581 5822 2222 2229 | Mastercard       | 123  | Yes |
| 3434 343434 34343   | American Express | 1234 | No  |
| 3566 0020 2014 0006 | JCB              | 123  | No  |

The card security code (CVV) to use with the test cards is 123 (except for American Express, which should be 1234) for an authorised response, other codes will be declined.

Cards which show 'Yes' in the MPI column will use a simulated 3D Secure authentication page, allowing you to test the transaction flow when Verified by Visa or MasterCard SecureCode is used.

## Simulating decline/error responses

When in test mode, and when using the above test cards, you can simulate any of the transaction response codes by using specific values for the card security code (CVV). By taking the response code you want to simulate, pad that code with a leading '0' in order to make it a 3 digit code and use that for the CVV.

For example, to simulate the Insufficient Funds response (status 'D', code '41') use 041 as the CVV.

You can also simulate an on-hold transaction in the same way. On hold is where the transaction has been authorised, but the anti-fraud system has flagged the transaction for inspection. Whilst the transaction is on-hold, no funds will be debited from the customers' card. You would need to use the Merchant Administration System to either accept or reject the transaction. To simulate the on-hold response within the test system, use a CVV value of '999' with one of the above test cards.