Transition Guide for 3D Secure

Introduction

Under the Payment Services Directive 2 (PSD2) initiative, in order to prevent ever-evolving fraud methods, Payment Service Providers (PSPs), such as 2Checkout, must apply extra security steps to implement Strong Customer Authentication (SCA) and further protect the confidentiality of consumers’ data.

For more details about 3D Secure support in API, check the Payment Services Directive 2 (PSD2) article.

You can also read the resources below to have a better understanding of what is PSD2 and what it entails:

- What is the 2nd Payment Service Directive (PSD2)?
- What is PSD2 and What Does Strong Customer Authentication (SCA) Mean for You?
- The Impact of PSD2 and SCA: Ordering Flows and Exemptions

Impact

All merchants using the Growth, Standard, 2Sell, 2Subscribe, 2Monetize and Enterprise packages are not affected.

If your integration is using https://2checkout.com/checkout/api/1/ endpoint to trigger payments, then you need to follow the transition process below.

3D Secure (3DS) support added to our Payment API

For card-based payments, this resulted in the implementation of 3D Secure version 2 (3DS2 aka EMV 3DS). 3D Secure has been employed to secure online card transactions since 2001, but now a new version has been developed to meet the PSD2 SCA requirements. Basically, to be able to accept payments from the world’s largest card networks (Visa,
Mastercard, Amex, etc.), any merchant will need to have implemented 3D Secure version 2 for their online store. Initially, this will apply mainly to EU-based merchants and their clients. Outside the EU, the current implementation pace of EMV 3DS is considered slow and less dominant.

The new flow for 3DS transactions in the Payment API is asynchronous and requires that you redirect the buyer to an authentication URL that will be returned in the authorization response, and wait for the buyer and sale parameters to be returned to a callback URL on your server.

**WHAT HAPPENS IF I DO NOT UPDATE MY INTEGRATION**

If no change is done to your API integration, the Payment API will continue to work as normal, but you will start to notice a higher rate of declines as the processors will not be able to continue the transaction if the shopper’s card requires 3DS authentication.

**SET UP CALLBACK URL**

To enable 3DS support in your integration, you need to set up an endpoint on your server where the 2Checkout system will return the shopper and order parameters when the order is completed. The return will be a GET request and will include all standard 2Checkout Return Process parameters: `total`, `order_number`, `invoice_id`, `merchant_order_id`, and `key` parameter, which will contain the MD5 hash to validate the passback.

**MD5 Hash Validation**

The MD5 hash is calculated as: `UPPERCASE(MD5_ENCRYPTED(INS secret word + seller id + order_number + total))`. The INS secret word can be found in your Merchant Control Panel, under `Integrations → Webhooks and APIs → Secret word section`. The seller id is your numerical merchant code/seller ID. The order_number is the order number for the sale returned on the passback. The total is the numerical value for the total amount of the sale. Each of our community-supported libraries provides a binding to validate the hash.

**PASS CALLBACK URL IN THE AUTHORIZATION REQUEST**

To let the 2Checkout system know that you are ready to handle the new 3DS flow, a new parameter needs to be added `- returnUrl` - in the root of the JSON payload on your authorization (create sale) API call. The `returnUrl` value needs to be the absolute path of your callback URL.

**Authorization Request Sample**

```json
{
    "sellerId": "your-seller-id",
    "privateKey": "your-private-key",
    "merchantOrderId": "example-custom-id-123",
    "token": "client-side-token",
    "currency": "USD",
    "total": "1.11",
    "billingAddr": {
```
If the card needs 3D Secure authentication for the payment, then the API will return an HTTP status ‘400’. In the body of the response, under the exception object, the `errorCode` value will be ‘700’ and the `errorMsg` value will contain the URL where the customer needs to be redirected for the authentication of the payment.

**API Response Sample**

```json
{
  "validationErrors": null,
  "exception": {
    "errorMsg": "https://api.2checkout.com/5.0/scripts/credit_card/authorize?avng8apitoken=77fdf3f03b265840",
    "httpStatus": "400",
    "exception": false,
    "errorCode": "700"
  },
  "response": null
}
```

Once the shopper completes the 3DS authentication process, they will be redirected to your callback URL along with the order parameters. If the 3DS authentication fails, they will be returned to the 2Checkout cart so that they can verify their payment method and re-attempt the payment.

https://knowledgecenter.2checkout.com/API-Integration/Transition-Guide-for-3D-Secure

Updated: Sat, 14 Mar 2020 01:14:05 GMT