3D Secure - Authentification

Content

Introduction

3D Secure is an authentication protocol provided by credit card systems.
The merchant may request a password from the consumer to confirm the payment. This procedure makes it possible to authenticate the consumer as being the holder of the card used for the payment. It enhances security and transfers the responsibility to the consumer of the card in case of unpaid.

Authentication is done in two steps:

- verification of the enrollment of the card to the 3D Secure system;
- consumer authentication request.

The implementation of 3D Secure must allow e-merchants to reduce the amount of their outstanding due to fraud, but this procedure also reduces the rate of payments accepted.

3DS Dynamic / 3DS Selective

The merchant can configure anti-fraud module rules to toggle payment requests with a 3D Secure consumer authentication request.
Payline offers to identify your payment method with an alias Contrat_Number. It is therefore possible to configure two Aliases on the same contract with a conventional contract without 3DS and another with 3DS.
You can also make payment requests directly in 3D Secure.

Integration

In web page, you must call the contract (Alias) of the payment method with the doWebPayment service .
In direct mode, you must manage the verification of enrollment with the verifyEnrollment service and then complete the payment request with the doAuthorization service .

Anti-Fraud Module

You must consult the anti-fraud module in order to manage the rules and actions to be put in place.
It is important to check your acceptance rates by setting up the anti-fraud module and to adjust the rules, several actions are possible to help you implement this module.

ECI values (Electronic Commerce Indicator)

ECI (*Electronic Commerce Indicator*) is the value returned from the Directory Server (Visa, Mastercard and JCB) to show result of authentication credit card payment from your customer on the features of 3D Secure.

1. Visa & CB

- **ECI 05:** Card holder and issuing bank are 3D Secure. 3dSecure authentication successful (Payment Authentication). ✅
- **ECI 06:** One of card holder or issuing bank not registered as a 3D Secure. ❌
- **ECI 07:** Card holder and issuing bank not registered as a 3D Secure. ❌

2. Mastercard

- **ECI 02:** Card holder and issuing bank are 3D Secure. 3dSecure authentication successful (Payment Authentication). ✅
- **ECI 01:** One of card holder or issuing bank not registered as a 3D Secure (Payment Authentication). ❌
- **ECI 00:** Card holder and issuing bank not registered as a 3D Secure (Payment Authentication). ❌
- **ECI 06**: Acquirer strong consumer authentication exception (TRA)- frictionless success (Payment Authentication) ✅
- **ECI 07**: Recurring Payment (initial / first payment) - frictionless success (Payment Authentication) ✅
- **ECI N0**: Frictionless failure (Non Payment Authentication) ❌
- **ECI N2**: Frictionless success (Non Payment Authentication) ✅

3. JCB

- **ECI 05:** Card holder and issuing bank are 3D Secure. 3dSecure authentication successful. ✅
- **ECI 06:** One of card holder or issuing bank not registered as a 3D Secure. ❌
- **ECI 07:** Card holder and issuing bank not registered as a 3D Secure. ❌

✅ Success / ❌ Failure