outpayce from amadeus

PAYMENTS SECURITY
AUTHENTICATION - 3DS 2 TRAVEL

1. Description

1.1 3DS v.2 is a security protocol designed by EMV to reduce the risk of fraud, identity theft and other illicit activities during e-commerce transactions.

1.2 3DS v.2 is based on a three-domain model, involving:

1.2.1 Acquirer domain: the acquirer or Customer to which money is paid.

1.2.2 Issuer domain: the cardholder's issuer.

1.2.3 Interoperability domain: the underlying systems that support 3DS v.2.

1.3 3DS v.2 authentication works by sending XML (Extensible Markup Language) messages over SSL (Secure Sockets Layer) connections with consumer authentication.

1.4 3DS v.2 authentication creates digital certificates that verify the identities of the different parties involved in the payment transaction.

1.5 3DS v.2 With 3DS v.2 the issuer conducts a risk-based authentication in the background using its ACS (Access Control Server) platforms, entirely out of sight for the consumer.

1.6 In some cases, the consumer does not have to complete any authentication steps at checkout.

1.7 This solution allows Customer to run 3DS 2.0 when accepting cards payments online.

2. How does the solution work?

2.1 The consumer visits Customer's website and enters the payment card information at checkout.

2.2 This solution sends transaction details and a 3DS v.2 verification request to the cardholder's issuer.

2.3 The issuer checks its internal records to determine whether the payment card is registered for 3DS v.2 services.

2.3.1 If the payment card is enrolled in 3DS 2.0, the issuer initiates a 3DS v.2 authentication flow.

2.3.2 If the payment card is not enrolled in 3DS 2.0, the flow automatically stops.

2.4 The issuer determines whether frictionless authentication is possible according to its risk rules:

2.4.1 Low-risk transaction: frictionless authentication is possible.

The issuer runs a fraud screening and risk assessment in the background, without input from the consumer.

2.4.2 High-risk transaction: frictionless authentication is not possible.

The issuer initiates a challenge authentication flow where the cardholder must verify their identity, for example by using a one-time authentication code (provided by the issuer).

2.5 Once the full verification process is successfully completed, we send the payment transaction for authorization on behalf of Customer, including the mandatory data needed to obtain liability shift (when applicable).

2.6 The consumer receives confirmation of the successful payment on Customer's website.

3. Key features

3.1 This solution was created specifically for the travel sector.

3.2 This solution provides real-time connections to the Card Schemes available for this solution (for example, Verified by VISA, Mastercard Identity Check, AMEX SafeKey, Diners/Discover ProtectBuy, JCB J/Secure, and Cartes Bancaires).

3.3 This solution is designed to comply with the current payment regulations globally, such as PSD2 strong Customer authentication in the European Union. New regulations may imply New Versions and New Releases of this solution, and that may trigger additional Charges.

3.4 For PNR integrated Customers, authentication data is added to the PNR and 3DS v.2 data appears in Customer's reports alongside payment and traveler data.

4. Disclaimers and limitations

4.1 We rely on Third-Party Providers to provide this solution.

4.2 This solution does not support two (2) payment cards authorization process and exemptions.

5. Integrations

5.1 This solution can be integrated with our Checkout SDK and Checkout UI solutions as well as with the PNR.

5.2 Other integrations with Customer's front and back ends may be available, subject to further scoping.