Special remarks - 3-D Secure

- 1 Prepare for 3D Secure 2.0
  - 1.1 If you are connected with PAYONE via Server API
  - 1.2 If you are connected with PAYONE via Shop-Plugin
  - 1.3 Not sure if 3D Secure is active for you?
- 2 3D Secure - General Introduction
  - 2.1 Payment Service Directive 2
  - 2.2 3-D Secure 1
  - 2.3 3-D Secure 2
    - 2.3.1 3-D Secure basic workflow with detection 3-D Secure 1 vs. 3-D Secure 2
    - 2.3.2 3-D Secure 2 challenge workflow
  - 2.4 Test data
  - 2.5 External links

Prepare for 3D Secure 2.0

PAYONE built an EMV 3DS Service that does not require merchants to implement any changes to their existing integrations, while ensuring full compliance to minimum data requirements for authentication requests as stipulated by the card schemes.

However, relying on the current implementation will lead to an uptick in challenges during checkouts. This can affect your conversion rate negatively. Therefore, we've implemented additional and optional parameters you can send to our Server API in order to take advantage of 3D Secure's exemption management.

If you want to optimize your conversion rate, here's what you have to do:

If you are connected with PAYONE via Server API

Required parameters are already implemented in the PAYONE Server API.

The more information you can supply per transaction, the greater the chance to proceed frictionless since there is more information provided to the transaction risk assessment of the issuer.

Therefore, additional optional data can be provided to your payment requests. We recommend enlarging the parameters added to the authentication requests by the end of 2020.

If you are connected with PAYONE via Shop-Plugin

Please update regularly to ensure you use the latest version of our plugin and provide optional request parameters as we optimize our plugins for better conversion.

Not sure if 3D Secure is active for you?

Please contact your sales contact or our merchant service to ensure your merchant account is configured for 3DS.

dditional Parameter

atest Plugin Update

Contact

3D Secure - General Introduction

3-D Secure is a technology to increase safety for credit card payments on the Internet for both dealers as well as for customers. It is used in order to authenticate a buyer during the payment process and to reduce the risk of a chargeback.

Visa calls this procedure "Verified by Visa", MasterCard "MasterCard SecureCode", American Express "Safekey" and Diners/Discover "Protect Buy".

Payment Service Directive 2

The PSD2 states that all payment transactions must be processed with strong customer authentication as far as there are no excemptions.

- SCA due to the use of at least two factors:
    - Knowledge (e. g. password, code, PIN)
    - Ownership (e. g. token, smartphone)
    - Inherence (e. g. fingerprint, iris scan, blood vessel pattern)

That means that all credit card transactions will have to be handled with 3-D Secure - which can be 3-D Secure 1 or 3-D Secure 2 (EMV 3-DS) on the issuer side.

If you have already activated 3-D Secure in your merchant settings the PAYONE platform will be able to handle both varying processes for you: 3-D Secure 1 or 3-D Secure 2. This depends on the credit card and its issuer and if it is allowed to process with 3-D Secure 1 or 2.

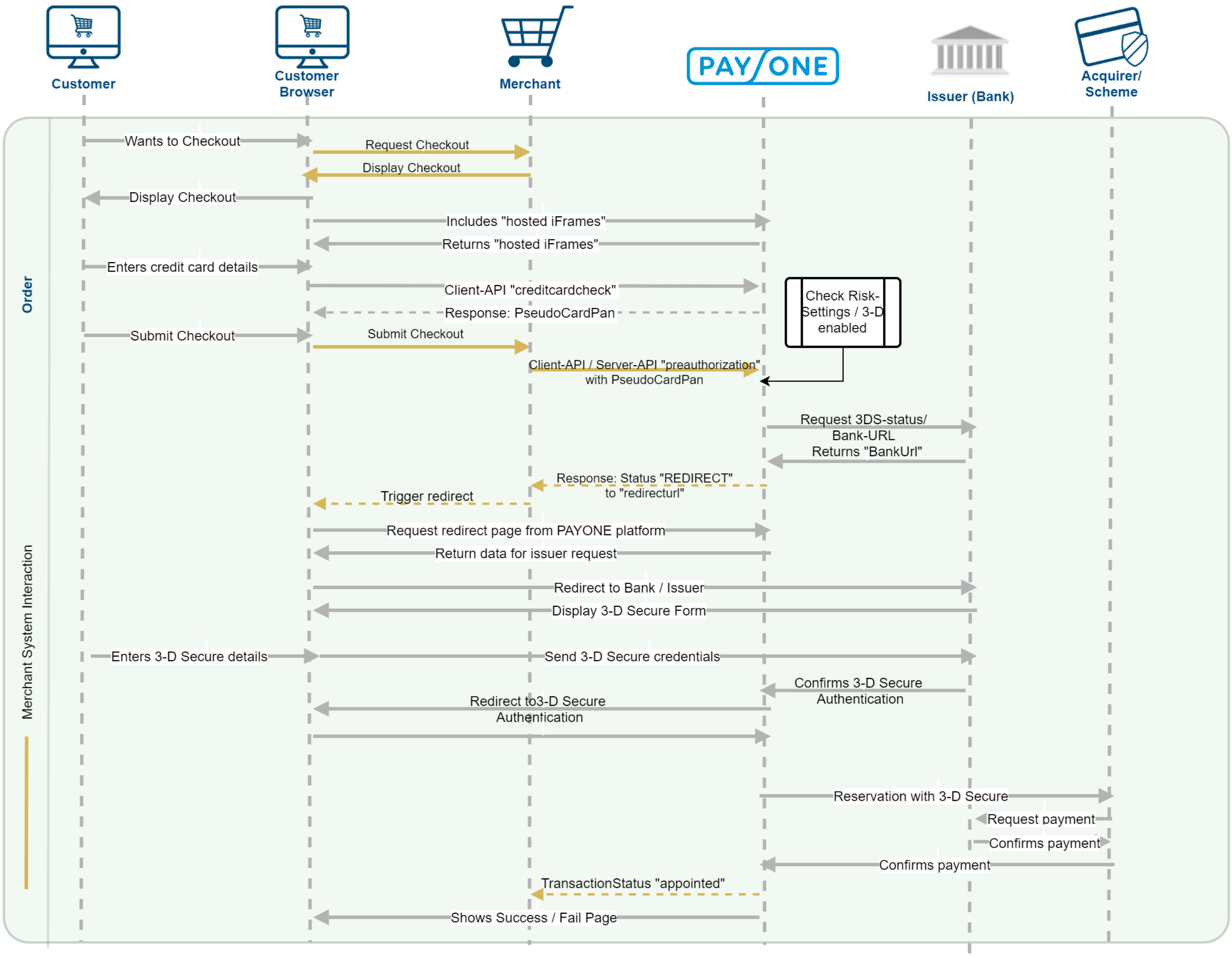
Please be aware that credit card transactions may be declined by your acquirer or the issuer if they are not processed with 3-D Secure at all.

3D Secure 1.0

3-D Secure 1

In the case of 3-D Secure, virtually every payment transaction must be authorized by the end customer if the end customer has registered for the 3-D Secure procedure and the card-issuing bank participates in the procedure. Therefore the customer is forwarded to a website of the card-issuing bank, where the 3-D Secure password must be entered.

The disadvantage of this method is that the customers often do not complete the authorization and thus have prematurely terminated the purchase process.


Customer
Customer Browser
Merchant
PAYONE
Issuer (Bank)
Acquirer/ Scheme
Order
Merchant System Interaction
Wants to Checkout
Request Checkout
Display Checkout
Display Checkout
Includes "hosted iFrames"
Returns "hosted iFrames"
Enters credit card details
Client-API "creditcardcheck"
Response: PseudoCardPan
Check Risk-Settings / 3-D enabled
Submit Checkout
Submit Checkout
Client-API / Server-API "preauthorization" with PseudoCardPan
Request 3DS-status/ Bank-URL
Returns "BankUrl"
Response: Status "REDIRECT" to "redirecturl"
Trigger redirect
Request redirect page from PAYONE platform
Return data for issuer request
Redirect to Bank / Issuer
Display 3-D Secure Form
Enters 3-D Secure details
Send 3-D Secure credentials
Confirms 3-D Secure Authentication
Redirect to3-D Secure Authentication
Reservation with 3-D Secure
Request payment
Confirms payment
Confirms payment
TransactionStatus "appointed"
Shows Success / Fail Page

3-D Secure 2

3-D Secure 2 was introduced by the EMVCo and leading credit card companies to facilitate the customer's payment process by offering up-to-date authentication methods such as biometric procedures.

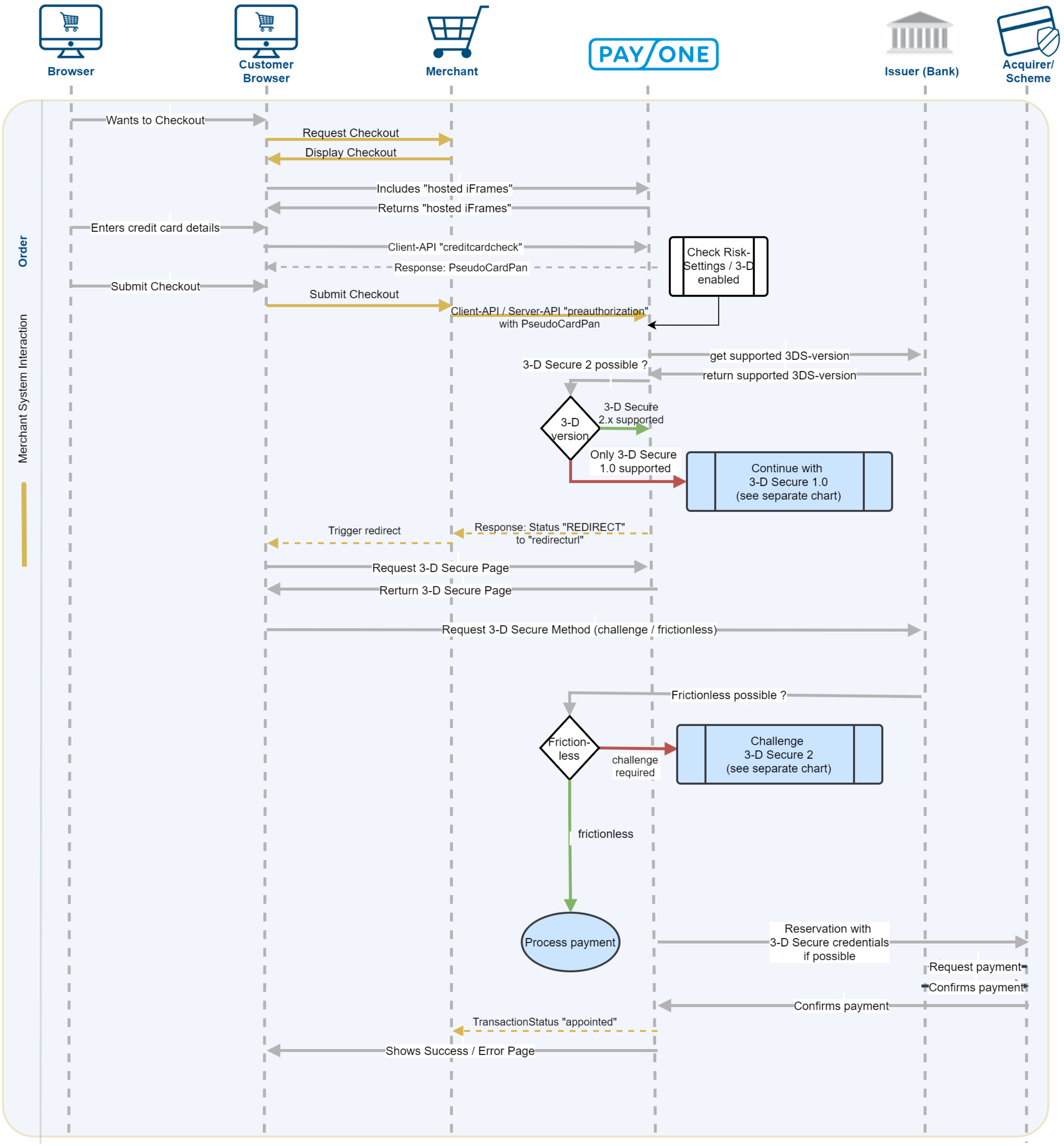
In addition, 3-D Secure 2 provides exemptions in order to bypassing this authentication if certain conditions are met an proceed "friction-less". In that case additional data, such as device data, can be transmitted and used to decide whether authentication by means of 3-D Secure is required. Transactions that are subject to higher risk or that have to comply with more stringent specifications (such as PSD2) can also be assigned to the authentication process.

PAYONE provides a landing page, which determines the necessary device data of the browser and makes them accessible to the ACS. As a result, no adjustments are required on by the merchant or the shop (other than stay updated on the latest shop-plug in version

3-D Secure basic workflow with detection 3-D Secure 1 vs. 3-D Secure 2

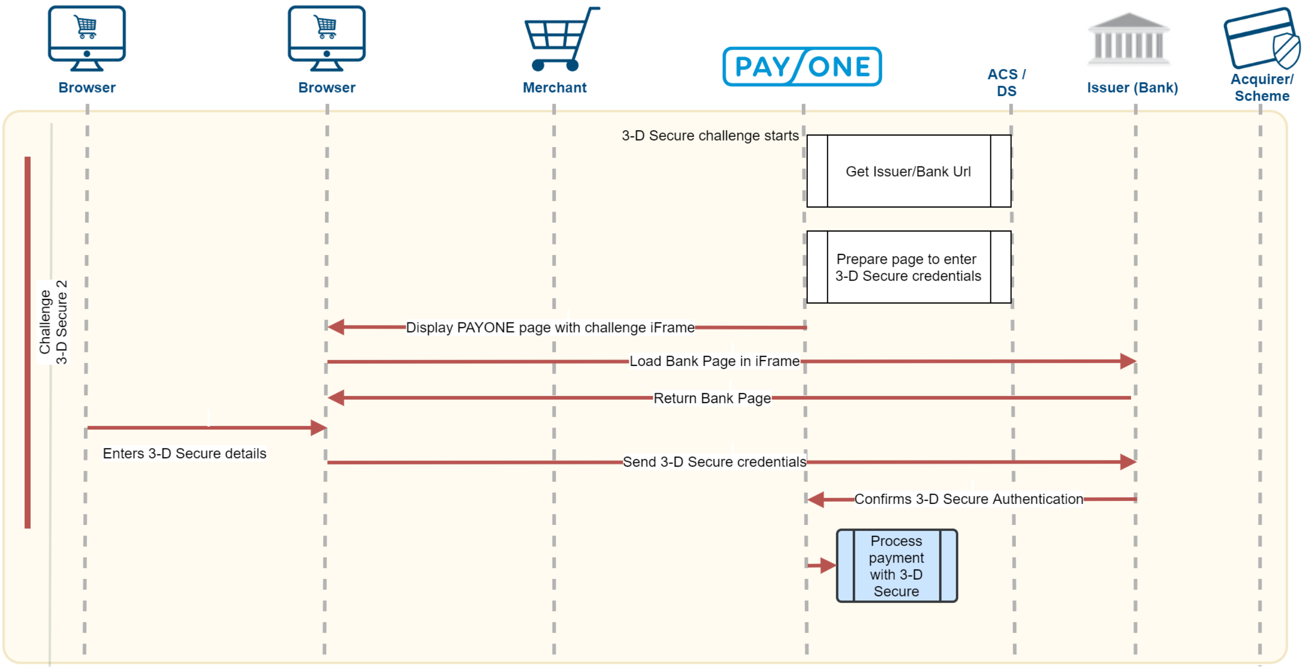
This sequence diagram shows the new workflow, which first asks whether 3-D Secure 2 is supported by the issuer. If not, then the 3-D Secure 1 workflow is triggered.

If 3-D Secure 2 is supported, device data from the browser will be determined and sent to the issuer along with the transaction data, which may agree to a friction-less process. In this case, the transaction is processed with 3-D Secure, without the customer having to enter his 3-D Secure credentials or to approve the transaction via his banking-app.


Browser
Customer Browser
Merchant
PAY/ONE
Issuer (Bank)
Acquirer/ Scheme
Order
Merchant System Interaction
Wants to Checkout
Request Checkout
Display Checkout
Includes "hosted iFrames"
Returns "hosted iFrames"
Enters credit card details
Client-API "creditcardcheck"
Response: PseudoCardPan
Check Risk-Settings / 3-D enabled
Submit Checkout
Submit Checkout
Client-API / Server-API "preauthorization" with PseudoCardPan
get supported 3DS-version
return supported 3DS-version
3-D Secure 2 possible ?
3-D version
3-D Secure 2.x supported
Only 3-D Secure 1.0 supported
Continue with 3-D Secure 1.0 (see separate chart)
Trigger redirect
Response: Status "REDIRECT" to "redirecturl"
Request 3-D Secure Page
Rerturn 3-D Secure Page
Request 3-D Secure Method (challenge / frictionless)
Frictionless possible ?
Friction-less
challenge required
Challenge 3-D Secure 2 (see separate chart)
frictionless
Process payment
Reservation with 3-D Secure credentials if possible
Request payment
Confirms payment
Confirms payment
TransactionStatus "appointed"
Shows Success / Error Page

3-D Secure 2 challenge workflow

If the issuer asks for a "challenge" - so the customer must be prompted to enter their 3-D Secure Credentials - a redirect to a browser page is created that includes the issuer page for entering the 3-D Secure credentials.


Browser
Browser
Merchant
PAYONE
ACS / DS
Issuer (Bank)
Acquirer/ Scheme
Challenge 3-D Secure 2
3-D Secure challenge starts
Get Issuer/Bank Url
Prepare page to enter 3-D Secure credentials
Display PAYONE page with challenge iFrame
Load Bank Page in iFrame
Return Bank Page
Enters 3-D Secure details
Send 3-D Secure credentials
Confirms 3-D Secure Authentication
Process payment with 3-D Secure

We have made all technical adjustments for the integration of 3-D Secure 2 for you. If you have already secured your credit card payments using the 3-DS procedure, you can now benefit from these advantages without restriction: They are thus ideally positioned for the PSD2 and the challenges of the future.

Please contact us immediately if you do not yet use the 3-DS procedure: In this case, there is a risk of payment defaults from 14 September 2019 onwards.

Further options will follow for seamless integration into shop systems via browser and app.

Test data

- Test data for 3-D Secure can be found here: TD - Credit card with 3-D secure 1.0 / 2.0

3-D Secure works with redirects - so the URLs for redirect / processing need to be set:

- SA - Initiating payment process (authorization)
- SA - Initiating payment reservation (preauthorization)
  - successurl
  - errorurl
  - backurl
- SA - 3-D Secure verification (3dscheck)
  - exiturl

External links

- (DE): Starke Kundenauthentifizierung: EMV 3-D Secure FAQ https://www.payone.com/de-de/kundenservice/3dsecure/
- (DE): Allgemeine Kunden-Information zum Thema PSD2 und 3-D Secure 2: https://www.bspayone.com/DE/de/about-us/kundeninformation