3D Secure 2.0 - Comply with DSP2

Content 3DSV2

What is DSP2 ?

The new Payment Services Directive (DSP2) initiated by the European Commission has been applied since 01/13/2018.

Objective: Strengthen the security of online payments

The European Banking Authority (EBA) has developed implementing measures called Regulatory Technical Standards (RTS) which will come on 09 /14/2019.
DSP2 will make SCA (Strong Customer Authentication) or two-factor authentication mandatory for online transactions.

What is SCA strong authentication ?

To strengthen the protection of buyers during remote payments, the PSD2 makes mandatory SCA (Strong Customer Authentication) authentication, also known as “two-factor authentication”.

Strong buyer authentication requires verification of at least two of the following 3 factors:

- Knowledge: what the buyer knows (PIN, password);
- Possession: what the buyer has (card, mobile, token);
- Inherence: what the buyer is (fingerprint, facial recognition, iris).

which are independent of each other in the sense that the compromise of one does not lead to the compromise of the other.

Although not recognized as a strong authentication method by the European banking authority, the SMS-OTP will still be used until new methods (biometrics for example) take over.

This method, adopted massively by buyers, has helped to significantly lower the fraud rates for e-commerce card payments. It is currently the most common among banks (86%).

What are the impacts for your activity ?

PSD2 applies to banks and not to merchants, which means that issuing banks that accept non-compliant transactions run the risk of being outlawed.

All transactions are not subject to RTS (see out-of-scope cases and exemptions).

- In the case of an out of scope transaction, strong authentication is not required.
- If a transaction falls within the scope of an exemption, strong authentication is optional and the choice to strongly authenticate is in the hands of the buyer's bank.
- If a transaction does not fall within the scope of an exemption, strong authentication is mandatory.

Strong authentication impacts the user journey and the acceptance rate, in particular on mobile, so it should only be triggered for risky transactions.

The objectives for the merchant are therefore:

- compliance in order to avoid refused transactions;

- maintaining an optimal user experience;
- reducing fraud.

We provide you with the tools to achieve these goals.

3DS V2

The rules describing SCA are technically neutral and do not impose any particular method.

The 3DS V2 protocol provides a mechanism which enables strong authentication to be carried out in accordance with the DSP2.

The main advantage of 3DS is to shift the responsibility for possible fraud from the merchant to the card issuer, which reduces chargebacks.

However, many merchants do not use the 3DS solution due to loss of conversion rates and service costs.

As a reminder, the main disadvantage of the 3D-Secure 1.0 version :

- payment process can be complicated or confusing for a cardholder, resulting in lower conversion (abandoned carts issue);
- 3-D Secure 1.0 does not adapt well to mobile devices;
- lack of seamless integration with modern payment tools such as wallets;
- limited set of possible authentication methods, some of which are obsolete and dangerous (date of birth);
- very limited ability of frictionless clearance based on score.

Major developments in the new 3-D Secure 2.0 specification.

Functionality	Profit
Risk-Based Authentication (RBA)	Allows frictionless authentication, without challenge, for the cardholder.
Data-driven risk management	Use the following data to assess the payment risk: • device ; • order ; • buyer ; • merchant authentication process ; • delivery .
Native mobile devices support	Designed to support native mobile interfaces, thus providing the buyer a fluid experience to the m-commerce buyers.
Flexible integration in the merchant's customer journey	Allows the merchant to embed seamlessly the authentcation in the checkout process, thus maintaining a consistent user experience.
Support for biometrics and other methods	Reduces friction in the user experience.
Flags in messages to support derogations related to DSP2	Allows meAllowserchantts andnd acquiirers to tto tellll isssuwheetheyrs wwhen they wato nt to applyy aan exemption aand ttakeke responsiibilityy for theforthe transaction.

The biggest difference with 3DS 1.0 is the “frictionless” flow which allows the issuer to approve a transaction without cardholder interaction based on risk-based authentication performed in the ACS.
Thanks to these developments, buyers' banks will have access to more information allowing them to refine decision support scoring for triggering strong authentication (or not / frictionless).

3DS 2.0 solves several technical issues of 3DS v1.0. Such as optimizing buyer journeys, making the payment process smoother for browser and inapp purchases, the introduction of a frictionless authentication flow and enhanced security.
3DS V1 authentication will remain possible until the end of 2020. From 2021, all 3DS authentications must use version 2.

How to comply with DSP2 ?

The 3DSecure authentication method will meet the requirements of RTS - SCA from 09/14/2019.

We must however distinguish the following cases:

- Case 1: systematic 3DS

  A merchant currently performing a 3DS V1 authentication systematically will be in compliance with the DSP2.

- Case 2: selective 3DS

A merchant currently performing 3DS V1 authentication selectively is subject to refusal by the buyer's bank for non-3DS transactions.

- Case 3: no authentication performed

  A merchant who does not currently perform any authentication is liable to a refusal by the buyer's bank for all his transactions.

In any case, we recommend that you consider migrating to the 3DS V2 protocol now in order to be ready to benefit from its advantages and in particular frictionless.

In order to integrate the 3DS V2 protocol, please consult the following article 3DSv2 :

- 3DSv2 - Webpage Interface
- 3DSV2 - Direct Interface

Linked pages

- 3D Secure 2.0 - Se mettre en conformité avec la DSP2
- 3DSv2 - Augmenter le frictionless
- 3DSV2 - Cloture d'un dossier PLBS
- 3DSV2 - Comment intégrer
- 3DSV2 - Comment ça marche
- 3DSV2 - Direct Interface - JSON container format
- 3DSv2 - Exemption acquéreur
- 3DSv2 - Exigences Visa
- 3DSv2 - Glossaire
- 3DSV2 - Indicateur de transfert de responsabilité
- 3DSV2 - Interface Directe - Ajout Modification de données carte (card on file)
- 3DSV2 - Interface Directe - Commande avec expédition pendant la garantie de l'autorisation
- 3DSV2 - Interface Directe - Paiements pour la Location de Biens et Services
- 3DSV2 - Interface Directe - Paiements récurrents
- 3DSV2 - Interface Directe - Pré-commande ou expedition tardive