

PSD2: reconciling compliance and a smooth customer experience



CHANGES AND RECOMMENDATIONS

- **Strong authentication vs. frictionless flow:** the new rules of the game
- **Risk analysis and requests for exemption:** the virtuous circle
- **Issuers, merchants and PSPs:** winning collaborations

Preamble



The Payment Services Directive (PSD2) has had a major impact in the European financial ecosystem, particularly in the e-commerce world. Its progressive roll-out is allowing digital commerce players to alleviate its negative impacts and to implement it in line with their customer loyalty challenges.

A large number of publications have raised awareness of the dates, obligations and technological impacts of this directive, but few have focused on the systemic paradigm shift that it brings about.

Indeed, in the framework of the fight against fraud, merchants have so far had the upper hand in the implementation of so-called “frictionless” experiments, that is to say without strong authentication; they directly control the fraud and conversion combination. The PSD2 now gives issuing banks (cardholders’ banks) the choice of whether or not to trigger this strong authentication, thus depriving e-merchants of a lever for optimising the user experience.

Regulators have taken this impact into account, and are paving the way for requests by merchants for exemption from strong authentication (decided by the issuing banks) if they are:

- justified by an analysis of fraud risks,
- based on the transaction data,
- shared with the holder’s bank.

The challenge of implementing this new regulation thus lies in cooperation between merchants, their payment service providers and banks.

The sharing of data and smart use of this data in the context of the GDPR (General Data Protection Regulation) will be key to the success of the post-PSD2 environment.

The aim of this white paper is to explain in detail the context, the stakes and the modes of cooperation that the e-commerce and payment ecosystem must implement from 2020 onwards to make PSD2 a success.



**Happy
reading!**



E-merchants: what changes with PSD2 and its new standards (RTS)

THE SYSTEM BEFORE RTS

1

You controlled the model

Depending on the rules you defined with your PSP*, you decided when to trigger strong authentication requests

BUSINESS
SAFETY



2

Depending on the situation, your customers could:



Complete their order without any further steps, **smoothly**

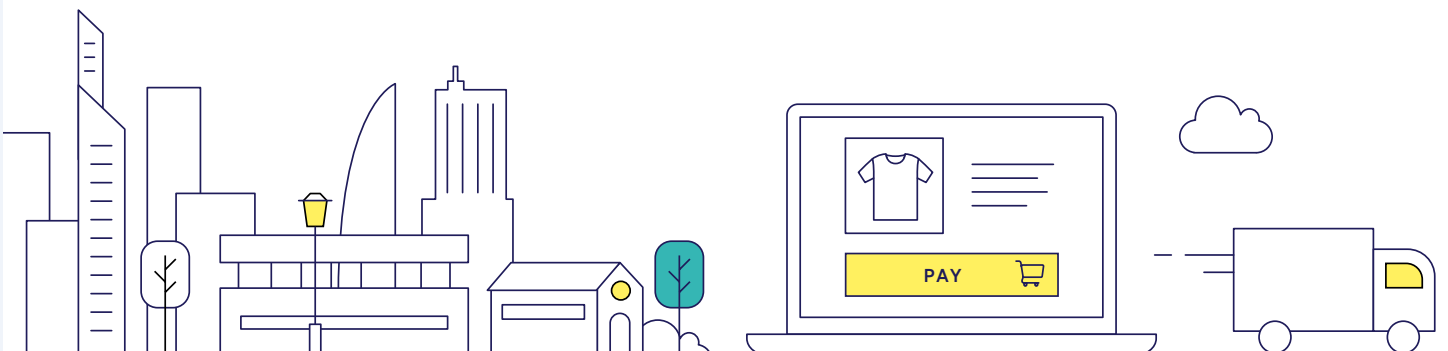
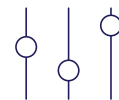


Receive a **single-use code** by SMS to authenticate themselves when making an on-line payment

3

You adjusted your anti-fraud policy

to improve your acceptance rate and reduce your chargebacks



* See Glossary p. 19

THE SYSTEM AFTER RTS



> The model is handed over to the banks

Requests for strong authentication will be made by the issuing banks, with:

- + A new **3DSv2** protocol
- + Strong authentication requests **for all payments**
- + **Possible exemptions**



> Your new role: requesting exemptions

to offer a frictionless process to your customers.

1 /

You identify

the exemptions applicable to your business



2 /

You analyse

the risks linked to a transaction (TRA)* to justify your requests for exemptions



3 /

You share

data useful to the issuer for making decisions



ISSUER
ANSWER

YES



A frictionless process

Customer experience maintained

ISSUER
ANSWER

NO



Strong authentication

must be based on:

- **Knowledge** (e.g.: password)
- **Possession** (e.g.: telephone)
- **Inherence** (e.g.: biometrics)

* See Glossary p. 19





Contents

8

Context

10

What changes with PSD2

A new model to fight fast-growing fraud

A progressive adjustment of the method

12

What's happening from October 2020?

14

Our recommendations for merchants

Find out the exemptions you need to optimise your conversion

Swapping the right data

Developing your risk analysis

Correct framing of your exemption requests

16

Banks, PSPs and merchants, trusted partners

Context

The PSD2 (Payment Services Directive 2), which came into force in 2018, has the main objective of reducing fraud in on-line sales.

With the growth of e-commerce, fraud is also increasing on line, accounting for 70% of card fraud at a national level*.

New technical requirements, known as RTS (Regulatory Technical Standards), are being introduced with PSD2.

Their objective?

To strengthen the security of on-line sales throughout the payment value chain, with obligations of performance and results.

* Source: OSMP (Observatoire de la Sécurité des Moyens de Paiement) 2019 report

Major changes



Each payment initiated by the buyer must give rise to a request for strong authentication. Exemptions are possible.



It is now up to the customers' banks (the issuers) to decide whether or not to grant exemption requests.



Strong authentication can nevertheless be avoided through good cooperation between issuers and merchants.



Migration by April 2021

Initially announced for September 2019, the full application of RTS in France has been postponed until April 2021, giving banks, payment service providers and merchants time to comply.

As of 1 October 2020, banks have gradually been migrating to the new model, which means a significant increase in requests for strong authentication. From this date, transactions of €2,000 or more on French cards will be subject to a soft decline*.

From January 2021 this rule will be extended to transactions over €1,000, then in February to those over €500 and finally from April 2021, progressively, to all transactions under €500.

Merchants, banks and payment providers must therefore move at the same speed to avoid affecting sales or having a negative impact on the customer experience.



* See Glossary p. 19

**Consult dalenus.com for migration plans country by country



What changes with PSD2

A new model to fight fast-growing fraud

Until the RTS came into effect, triggering strong authentication was at your discretion; you alone decided where to strike the balance between optimum security and maximising your conversion.

Your payment service provider, using risk tools and machine learning, evaluated each situation with you. Depending on the result of the risk analysis, the authentication request was triggered on so-called suspicious transactions.

With the RTS, the initial model has been turned on its head, no longer leaving merchants with a choice. It is now up to the customer's banks (issuers) to systematically make the authentication request.

Depending on the additional information you are able to provide them with, including your exemption requests, banks will decide whether (or not) to grant the exemption from strong authentication of your customers. **Your conversion rate could be affected without expert support.**



Combining the expertise of the merchant and the issuer, for better fraud management

As a merchant, your fraud control can be improved through the expertise of the issuer. Indeed, you see fraud through the prism of chargebacks, which is merely the tip of the iceberg. Banks have a broader view of fraud.

For example, not all customer disputes result in chargebacks. This is particularly true for small transactions whose management costs are too high for a bank.

What is more, banks, which receive all card payments made by their holders, have extensive knowledge of their customers and are able to detect anomalies.

Therefore, data sharing between the merchant and the issuer will lead to a better control of the fraud rate, without negatively affecting legitimate customers.



A progressive adjustment of the method

Beyond the change of model, the RTS also mean a gradual evolution of the authentication method as of October 2020.

	Now	From October 2020
Protocol	3D-Secure (3DS)	3D-Secure v2 (3DSv2)
Responsibility	Merchant	Issuing banks
Authentication type	Simple authentication	Strong authentication vs. frictionless flow
Risks	A strong authentication failure rate estimated at 11% [*] .	A more significant decrease in acceptance and conversion rates

^{*} Source: OSMP 2018 Report

Strong authentication

All payments initiated by the customer must systematically be subject to a request for strong customer authentication (SCA), unless the exemptions provided for in the RTS apply. The SCA is based on three elements inherent to buyers, validated by the EBA (European Banking Authority), which must be combined to ensure their authentication:



What they know
e.g.: password



What they possess
e.g.: smartphone



Who they are
e.g.: biometrics

Thus, the single-use code sent by SMS (One Time Password, OTP SMS) will soon no longer be sufficient to authenticate buyers. Many flaws are found with this authentication method, which is based on only one factor, possession of the phone. The addition of another factor to the authentication method effectively minimises the risk of fraud, although it places restrictions on buyers (which may lead to a drop in conversion).

Frictionless flow

The greatest advantage for merchants is that it adds no extra step for the customer at the time of payment, thus providing greater fluidity and a good customer experience.

The frictionless flow is made possible thanks to new data exchanged between the merchant and the customer's bank (the buyer's IP address, the type of device used, the type of browser, the version of the operating system, etc.). After analysing this enriched data, the customer's bank will decide whether it is sufficient to grant an exemption from the purchaser's authentication.

However, certain transactions may be exempt from the rule of systematic authentication. The following in particular are excluded from the scope of RTS: payments initiated by merchants such as recurring payments, subscriptions with the exception of the first payment and payments by mail or telephone.

What's happening from October 2020?



The whole payment value chain will change, even if migration towards 3DSv2 will be carried out progressively.



Providers (PSPs)

Migration takes place above all from a technical viewpoint. Your payment and/or acceptance provider will integrate the new fields related to 3DSv2 so that they are ready when you send the new data in your payment flow.



Acquiring and issuing banks

With the main aim of complying with the fraud rate thresholds set by the regulator, your acquiring bank and the issuing banks will make use of strong authentication. As a merchant, you will therefore gradually see the emergence of a new type of rejection having a direct impact on your acceptance rate: the *soft decline*.

Soft decline: You have submitted a transaction for authorisation directly without authentication, and without an exemption being applicable. The issuing bank may ask you to present this transaction with a strong authentication.



Merchants

It is therefore in your interest to anticipate this progressive migration by starting to collect and send data using the new 3DSv2 protocol, at the risk of seeing your acceptance rate decline. When sending this data, you must also make sure you specify, for each transaction, whether or not you are requesting an exemption.

Our recommendations for merchants

1 Find out which exemptions are essential to optimise your conversion rate

Payments of less than €30

Although the decision will ultimately be taken by the issuer, you can request an exemption if the transaction is for less than €30.

However, this request for exemption will be refused regardless of the merchant if:

- it is used **more than 5 times without further authentication of the customer**,
- the sum of exempted payments **exceeds €100**.

Low-risk payments

Through your payment service provider, a Transaction Risk Analysis (TRA) can be carried out. It will enable you to justify your requests for exemption on low-risk transactions. The customer's bank is then responsible for granting the exemption or requesting strong authentication (soft decline) or even the transaction abandonment (hard decline).

What is more, your acquirer and the issuing banks will only be able to accept your exemption requests if they themselves manage fraud thresholds on their entire portfolio of cardholders:

- **0.13%** to exempt transactions **of less than €100**;
- **0.06%** to exempt transactions **of less than €250**;
- **0.01%** to exempt transactions **of less than €500**.

The rule concerning the fraud rate implies a strict fraud policy throughout the payment chain. Since each link in the chain is affected by fraud rates, stakeholders are de facto interdependent. Issuers, acquirers and merchants are already improving their fraud detection levels so they can offer exemptions to as many people as possible in the medium term.

2 Swapping the right data

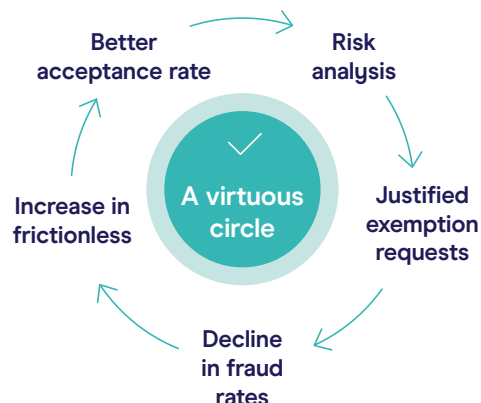
Take an active role in the decision to trigger by providing issuers with the information they need to make a decision. Below is some of the data that you will need to integrate into your payment flow and send to issuers:

- Device from which the transaction is initiated,
- Information about previous customer authentications on your site,
- Your risk assessment regarding the customer's order,
- Your request for exemption (or not) on the transaction.

3 Develop your risk analysis

The evolution of the model brought about by RTS also implies the evolution of risk analysis solutions. As these solutions are no longer intended to trigger the authentication request, they must be able to pass their analysis (and recommendation) on to issuers based, among other things, on new behavioural data.

To anticipate this change, make sure your payment provider has the capacity to assume this role, or check whether an external solution is needed.



4 Categorize your exemption requests appropriately

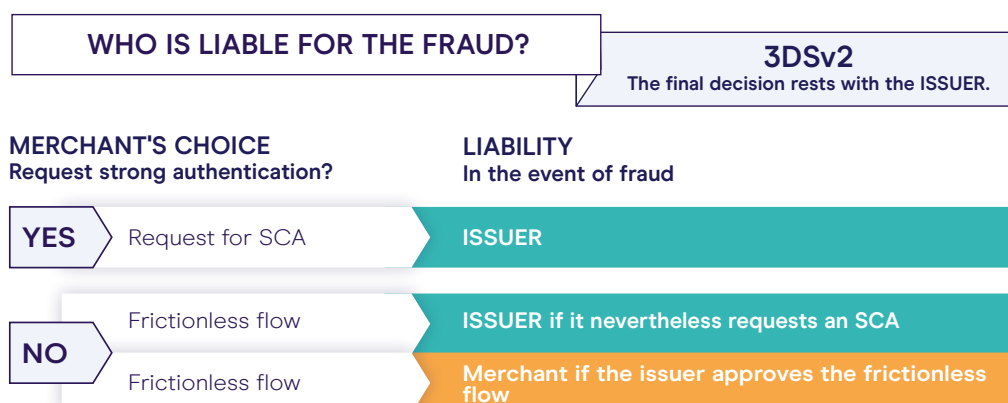
Your risk analysis will allow you to identify precisely which transactions could be exempted. You should nevertheless be careful with this lever, since it has a direct impact on your fraud rate, your acceptance rate and liability for chargebacks.

Indeed, if you apply for an exemption and the issuing bank follows your recommendation, you will be responsible for the chargebacks in the event of fraud, and will contribute to the increase in the fraud rate.

Issuing banks must then react, by triggering further requests for strong authentication on your customers, which can significantly reduce your acceptance rate. So the RTS highlights the necessary relationship of trust between merchants and issuing banks.

The latter are certainly the decision-makers when it comes to triggering strong authentication, but they cannot take this decision without the support of merchants. By providing additional information to the profiling of a fraudster, you help issuing banks to take decisions, and make triggering the process more efficient.

Thus, the more your exemption requests are the result of a thorough and effective real-time risk analysis, the more you will be perceived as a trusted partner in the eyes of issuers. A risk analysis that complies with the RTS and is reliable will subsequently ensure a better overall fraud rate and more exemptions for customers.



Banks, PSPs and merchants, trusted partners

As you will have understood, the changes brought about by RTS in fact require cooperation between the stakeholders in the payment chain who share the same objective: reducing fraud while optimising frictionless payment. The better communication is between banks, payment providers and you, the less impact strong authentication requests will have on your business.

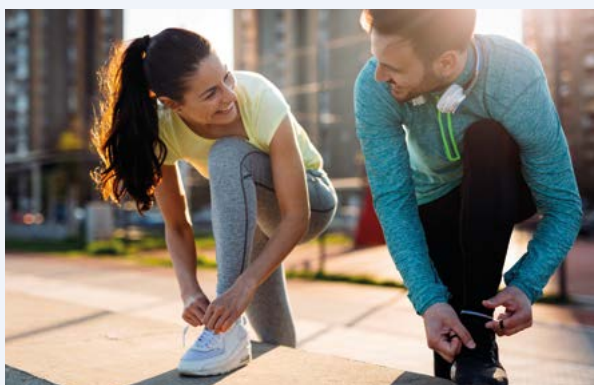
This cooperation is mainly based on the exchange of new data required by 3DSv2, but also on your requests for exemption. Directly affecting the fraud rate, requests for exemption, and the resulting risk analysis, can quickly become a virtuous circle for any merchant who understands the stakes involved in RTS and the role of everyone in detecting fraud.

With the advent of RTS, the following check-list should be followed if you wish to be proactive in the fight against fraud:

- 1** Decide whether the risk analysis will be internal or external (PSP, other stakeholders, etc.),
- 2** Identify the exemptions applicable to your business,
- 3** Start collecting data in 3DSv2 mode,
- 4** Make sure the new 3DSv2 fields are integrated by your PSP,
- 5** Progressively send your transactions into these new flows,
- 6** Monitor soft decline and its impact on your acceptance rate.



A responsive and proactive partner

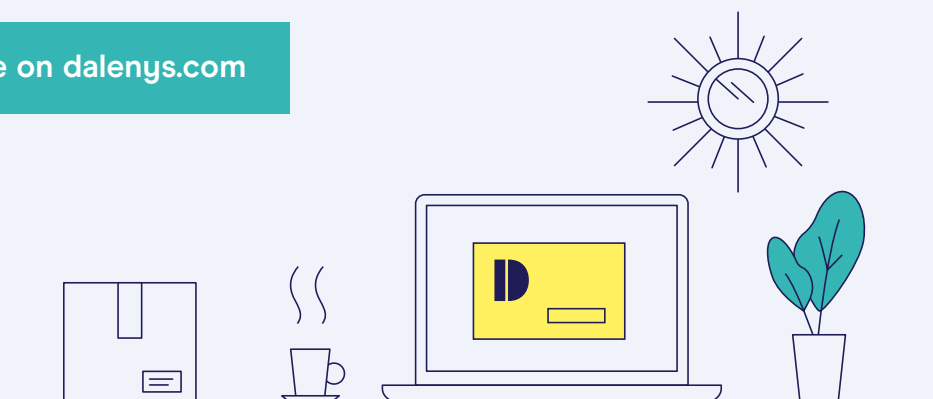


Dalenys will be a valuable partner when it comes to personalised management of the change and the new balance to be achieved.

A long-standing e-merchant partner, Dalenys is a payment solution for unified commerce, improving the customer experience and ensuring customer loyalty. Dalenys is developing a platform capable of connecting a retailer's entire ecosystem: sales channels, distribution networks, data and technology partners.

What is more, Dalenys understands how issuers will apply this new model thanks to its proximity to decision-makers. Dalenys is a solution from Natixis Payments, the payment specialist of Groupe BPCE, the 2nd largest banking group in France and the leading issuer of Visa cards in continental Europe. This gives it a 360° view of payment and a unique knowledge of issuer data modelling.

Find out more on dalenys.com







Glossary

PSD2

(European Payment Services Directive 2)

A Directive with two strands: one on opening up banking data to boost innovation and competition; the other on securing on-line payments to minimise fraud.

RTS

(Regulatory Technical Standards)

Technical requirements introduced by the PSD2 involving changes to the authentication model and method used to secure on-line payments.

3D-Secure

(3DS)

Secure protocol for on-line payments, the aim of which is to ensure the identity of the customer to minimise fraud. One of the applications of the 3DS today is to send a one-time use code by SMS to the buyer (One time Password, OTP SMS).

The new version of the protocol (**3DSv2**) strengthens the authentication method.

SCA

(Strong Customer Authentication)

Request for strong authentication that must be based on at least two independent elements linked to the buyer: knowledge (e.g. password), possession (e.g. telephone), inherence (e.g. biometrics).

Frictionless

Process that adds no extra step for the customer at the time of payment.

Data exchanged between merchants and banks is sufficient to ensure the customer's identity.

TRA

(Transaction Risk Analysis)

Analysis of the risks of the transaction or real-time analysis leading to a recommendation (request for exemption or strong authentication).

Hard decline

Categorical refusal issued by the client's bank. Payment must be waived.

Soft decline

The request for direct authorisation of the transaction without prior authentication is refused by the customer's bank.

The payment must be presented with strong authentication.

Dalenys, a solution from Natixis Payments, is a unified payment platform that helps merchants build an ongoing relationship with their customers

+33 1 84 07 07 07
hello@da1enys.com
@da1enyscorp

Payment is just the start
da1enys.com

Dalenys Payment - 110 avenue de France, 75013 Paris, France
SAS with capital of € 15,179,205.30 - 443 222 682 RCS Paris - NAF 6419Z
Payment establishment ACPR accreditation: 16378 - Intracommunity VAT No.: FR12 443 222 682
©Dalenys - October 2020