

The Regulatory Technical Standards (RTS\*) for strong customer authentication (SCA) and common and secure open standards of communication (CSC) are a key text for the implementation of the revised Payment Services Directive (PSD2).

## UNDERSTANDING THE FINAL REGULATORY TECHNICAL STANDARDS

for strong customer authentication and common and secure open standards of communication under PSD2

PSD2 aims to make payments safer, increase consumers' protection, foster innovation and competition while ensuring a level playing field for all actors, including new ones which were not regulated by the first version of the Payments Services Directive.

1

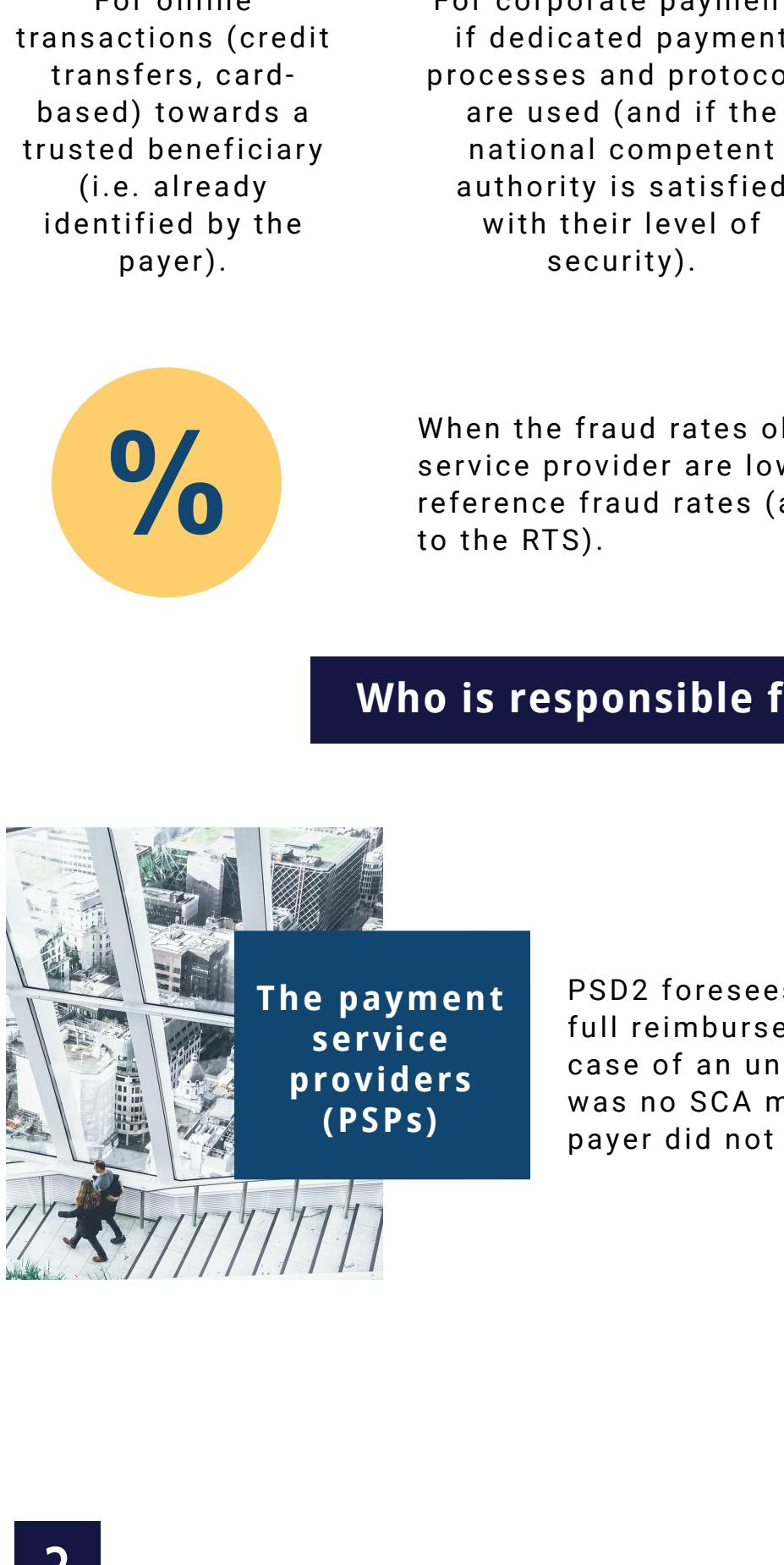
### The RTS are implementation requirements

for payment service providers to comply with PSD2.

The role of the RTS is to define specific security measures that were only addressed through general principles in PSD2, and to ensure effective and secure communication between the relevant actors. They are therefore more concrete than PSD2.

They are directly applicable in the Member States of the EU and do not have to be transposed in national law.

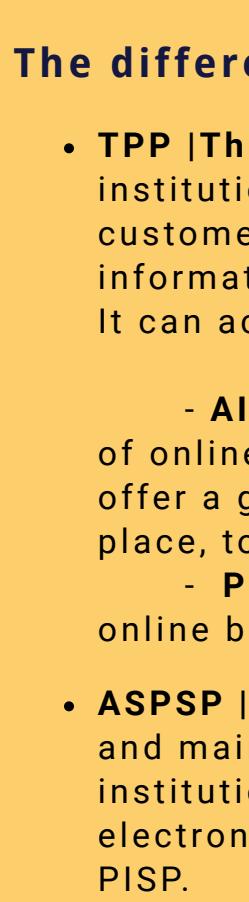
2



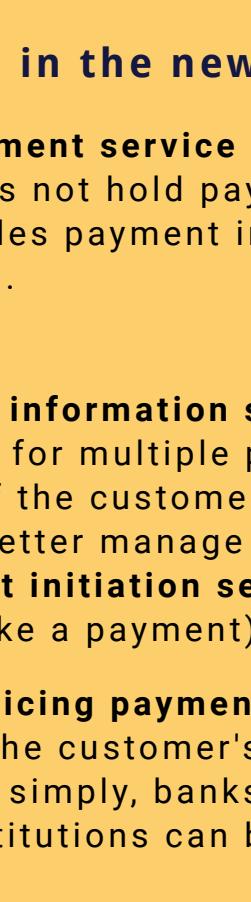
### Strong customer authentication

The principle of SCA is to ensure customer protection via an increased level of security of electronic payments.

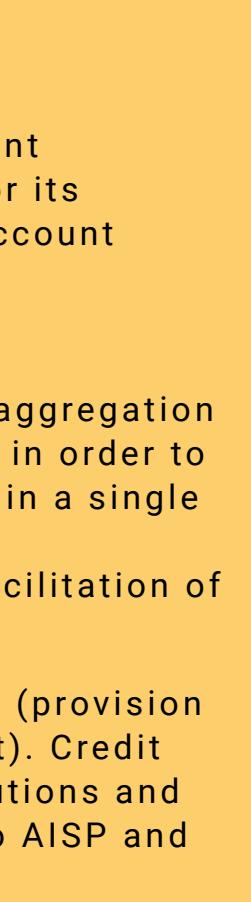
### When does SCA have to be applied?



When a customer - individual or corporate - accesses their payment account online (incl. an aggregated view of their payment accounts).



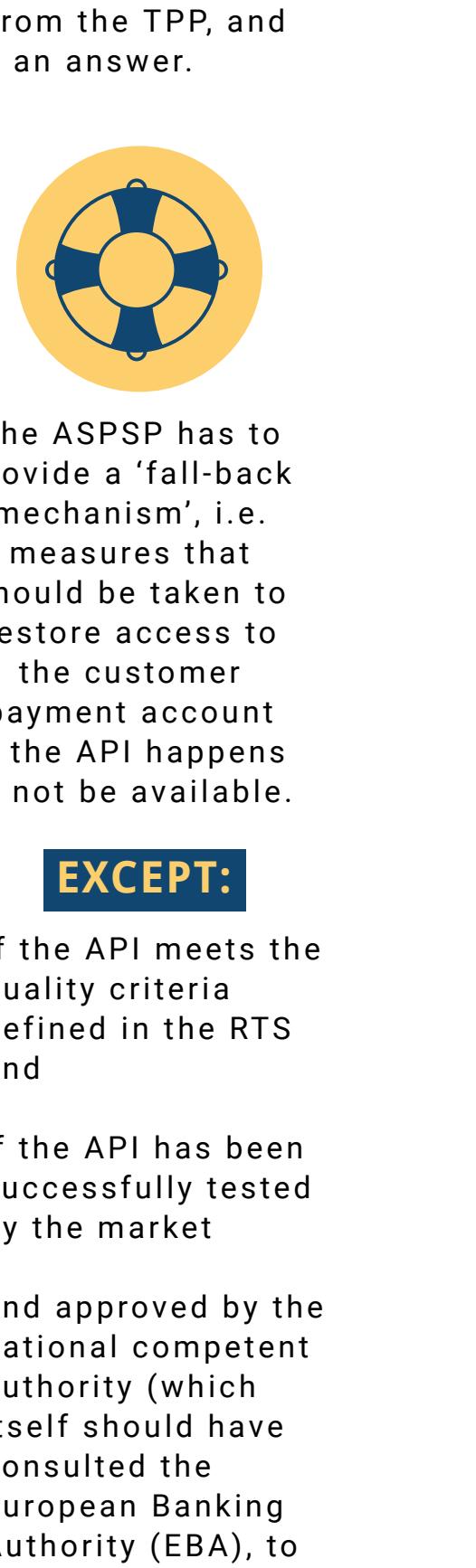
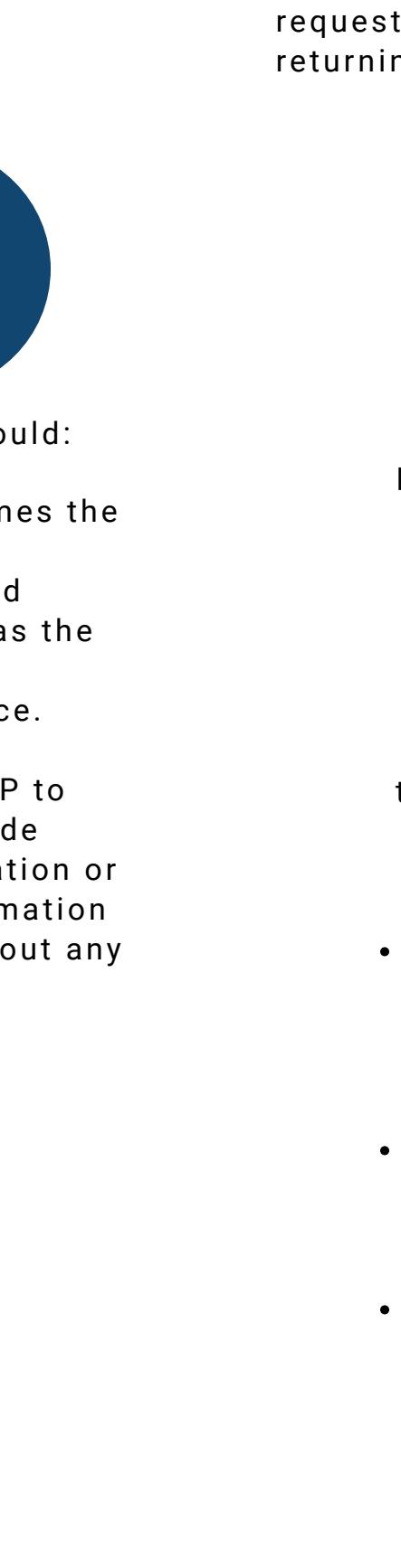
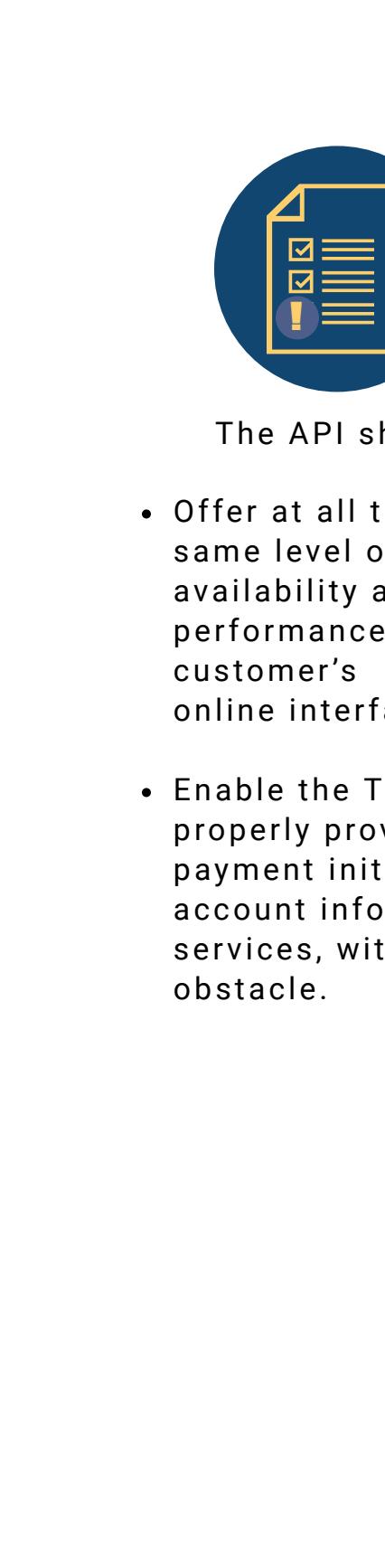
When making an electronic payment.



When carrying out any action through a remote channel which may imply a risk of payment fraud or other abuses.

### How is SCA applied?

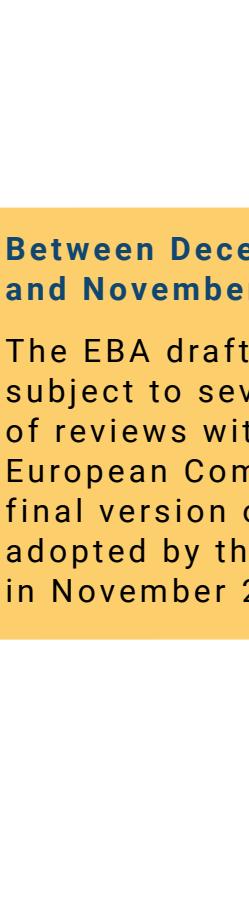
The customer's identity has to be verified, using at least two of the following items:



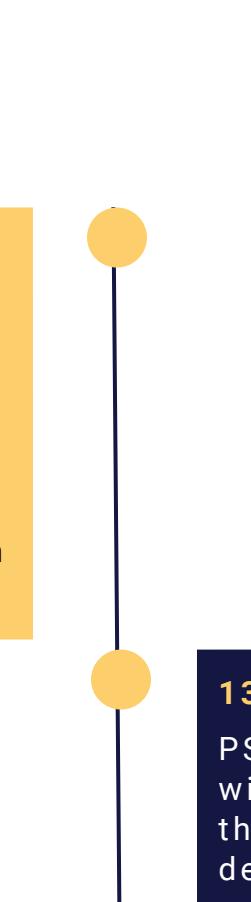
A unique authentication code which dynamically links the transaction to a specific amount and a specific payee (for remote internet and mobile payments).

### What are the possible exemptions to SCA application?

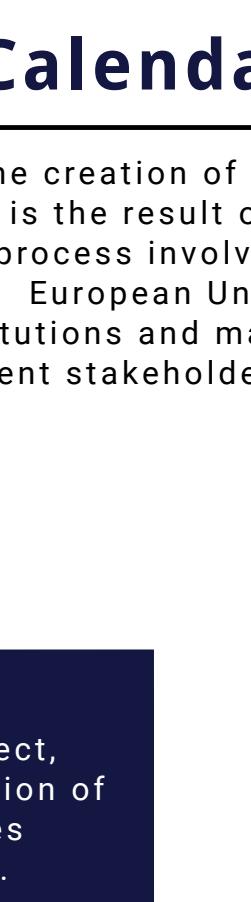
The RTS list a number of possible exemptions, to keep electronic payments as convenient and seamless as possible:



For remote payments (online and mobile) of low value (up to €30).



For contactless card payments up to €50.



At unattended payment terminals for transport fares and parking fees.

1

### Via a dedicated communication interface

This is concretely translated into the creation of an Application Programming Interface (API), a sort of messenger enabling information exchanges, taking a request from the TPP, and returning an answer.



The API should:

- Offer at all times the same level of availability and performance as the customer's online interface.
- Enable the TPP to properly provide payment initiation or account information services, without any obstacle.

The ASPSP has to provide the AISP or PISP a secure communication channel to provide access to the payment account and therefore making it possible for them to propose their services.

### EXCEPT:

- When a cumulative value of €100 is reached.
- Or when 5 payments of up to €30 have been made.

- When a cumulative value of €150 is reached.
- Or when 5 contactless payments of up to €50 have been made.

2

### Via the adaptation of the customer online banking interface

The TTP accesses the customer's payment account by using their interface and their personalised security credentials, with however a secure authentication of the TPP. It can be described as a more secure and sophisticated version of 'screen scraping'.



The customer formally agrees on the access, use, and processing of their payment account information.

The requirements of the General Data Protection Regulation (which applies in May 2018) strengthens the consumer's protection.

3

### Common and secure communication

is the second major principle described in the RTS.

Customers have to give their explicit consent to the AISP or PISP to share their payment account data or to initiate a payment transaction.

PSD2 foresees that the payer can claim full reimbursement from their PSP in case of an unauthorised payment if there was no SCA measure in place and if the payer did not act fraudulently.



The customer formally agrees on the access, use, and processing of their payment account information.

The requirements of the General Data Protection Regulation (which applies in May 2018) strengthens the consumer's protection.

4

### Calendar

Between December 2015 and November 2017

The EBA drafts the RTS, subject to several rounds of reviews with the European Commission. A final version of the RTS is adopted by the Commission in November 2017.

The creation of the RTS is the result of a process involving European Union institutions and many payment stakeholders.

By 27 February 2018

The European Parliament and the European Council approve (or reject) the final RTS.

13 January 2018

PSD2 enters into effect, with the main exception of the security measures described in the RTS.

18 months after their publication in the Official Journal of the EU, the RTS apply.

In September 2019

The EBA invites all stakeholders to remain grey areas of the RTS, and will publish answers to clarify some points.

The TPP is authorised in its home country under PSD2 it should be able to propose its 'passing' even in countries not having yet transposed PSD2.

If a TPP is authorised in its home country under PSD2 it should be able to propose its 'passing' even in countries not having yet transposed PSD2.

5

### Transition period

What is likely to happen between the PSD2 implementation as from January 2018 and the likely RTS application in September 2019?

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.

The requirements of the General Data Protection Regulation (which applies in May 2018) strengthens the consumer's protection.



The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.

6

### Transition period

What is likely to happen between the PSD2 implementation as from January 2018 and the likely RTS application in September 2019?

The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.



The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.

7

### Transition period

What is likely to happen between the PSD2 implementation as from January 2018 and the likely RTS application in September 2019?

The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.



The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.

8

### Transition period

What is likely to happen between the PSD2 implementation as from January 2018 and the likely RTS application in September 2019?

The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.



The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.

9

### Transition period

What is likely to happen between the PSD2 implementation as from January 2018 and the likely RTS application in September 2019?

The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.



The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.

10

### Transition period

What is likely to happen between the PSD2 implementation as from January 2018 and the likely RTS application in September 2019?

The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.



The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.

11

### Transition period

What is likely to happen between the PSD2 implementation as from January 2018 and the likely RTS application in September 2019?

The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.



The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.

12

### Transition period

What is likely to happen between the PSD2 implementation as from January 2018 and the likely RTS application in September 2019?

The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.



The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.

13

### Transition period

What is likely to happen between the PSD2 implementation as from January 2018 and the likely RTS application in September 2019?

The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.



The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.

14

### Transition period

What is likely to happen between the PSD2 implementation as from January 2018 and the likely RTS application in September 2019?

The strong customer authentication and secure and common communication rules do not apply. TPPs do not have to use an API to get access to the customers' payment accounts.

The ASPSPs can already make their exemption requests to their national competent authority, which will have to consult with the EBA.