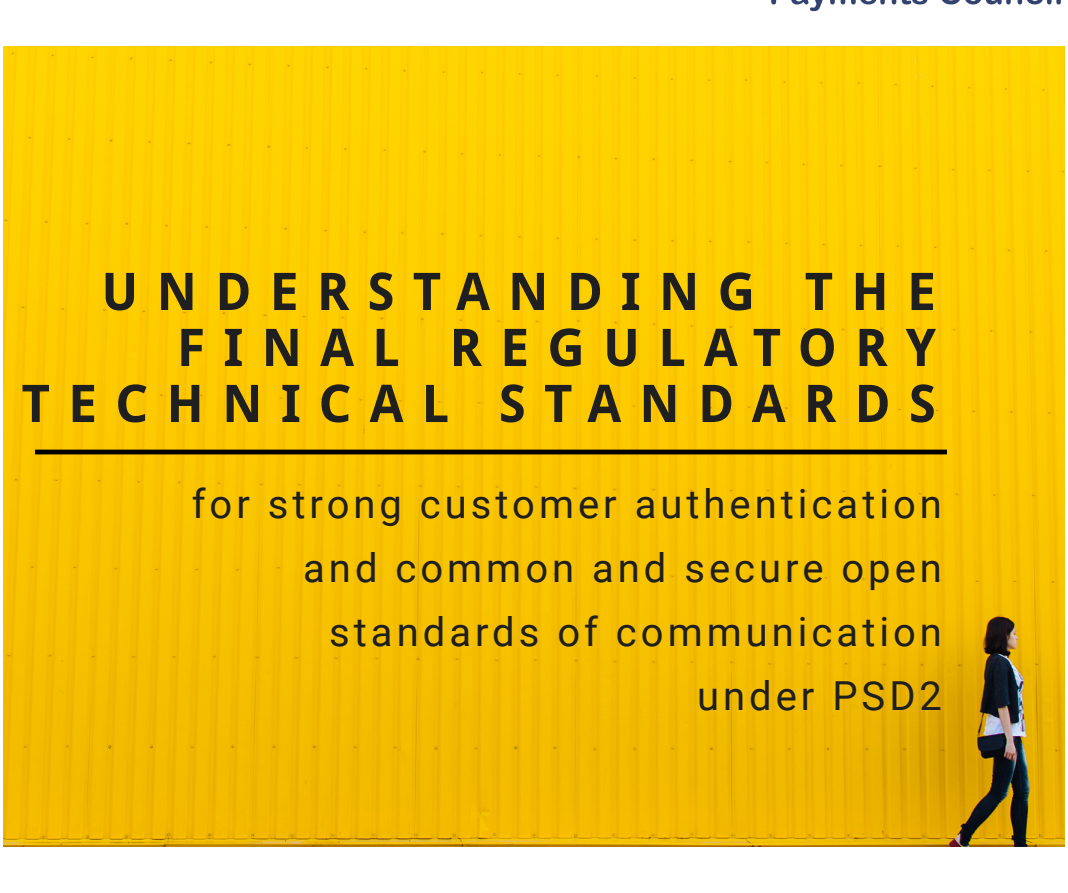
European Payments Council

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 Payment 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?

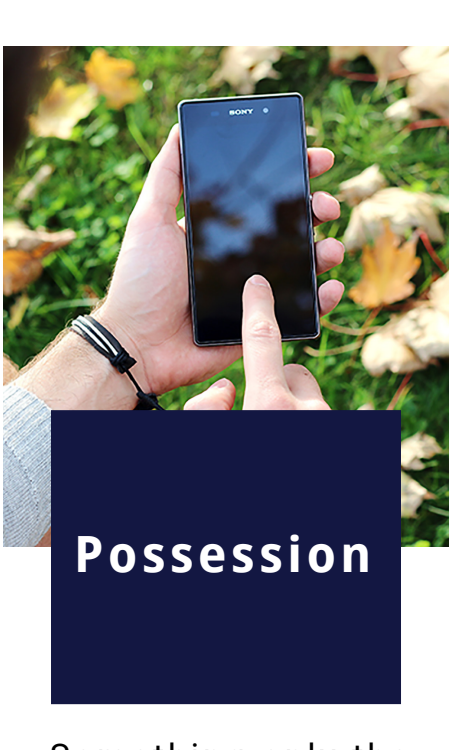
- When a customer - individual or corporate - accesses their payment account online (incl. an aggregated view of their payment accounts).
- When making an electronic payment.
- When carrying out any action through a remote channel which may imply a risk of payment fraud or other abuses.

How is SCA applied?

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

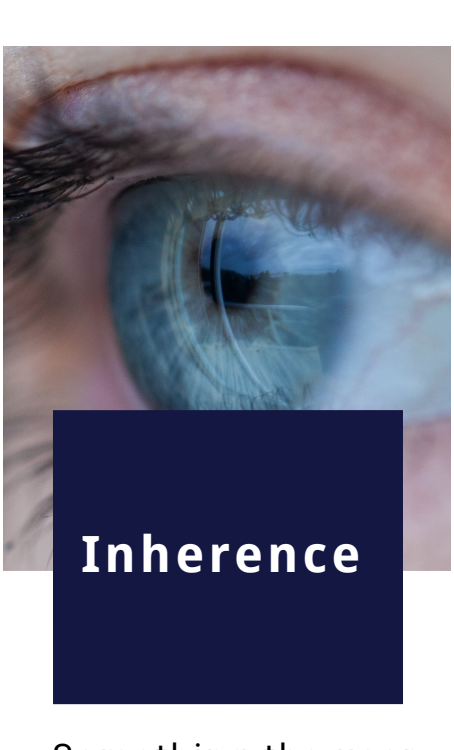
Knowledge

Something only the user knows (PIN, password…).



Possession

Something only the user possesses (a card, a mobile phone…).



Inherence

Something the user is (biometric identification like fingerprint, iris or voice recognition…).

+ Extra element for all remote transactions

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).

EXCEPT:

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

For contactless card payments up to €50.

EXCEPT:

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

At unattended payment terminals for transport fares and parking fees.

For online transactions (credit transfers, card-based) towards a trusted beneficiary (i.e. already identified by the payer).

For corporate payments if dedicated payment processes and protocols are used (and if the national competent authority is satisfied with their level of security).

When the online payment account is consulted, SCA is needed only the first time and every 90 days.

When the fraud rates observed by the payment service provider are lower than the pre-set reference fraud rates (as described in an Annex to the RTS).

Who is responsible for SCA application?

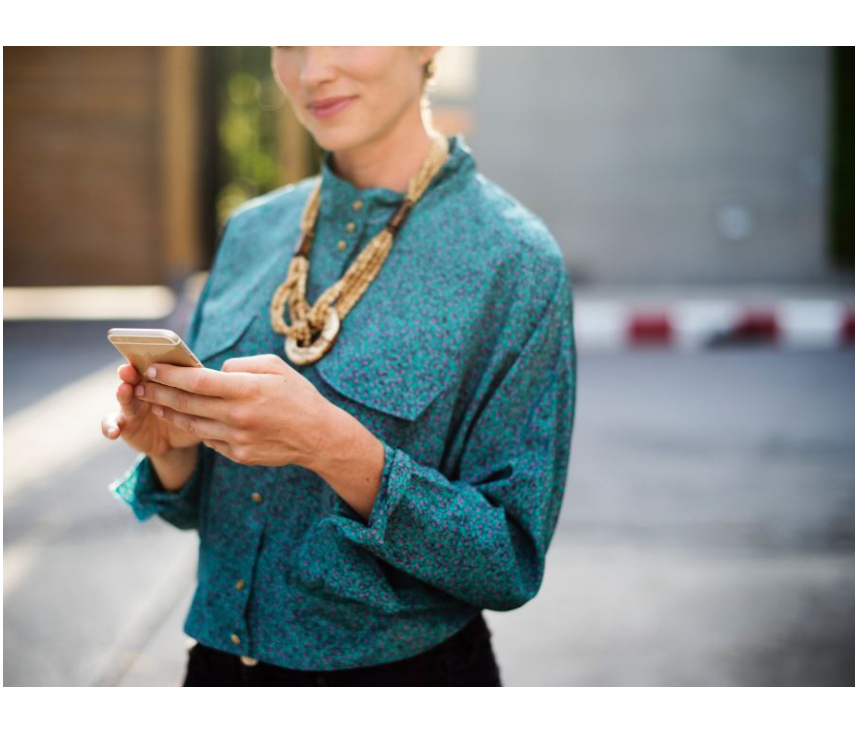
The payment service providers (PSPs)

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.

3

Common and secure communication

is the second major principle described in the RTS.



To bring more competition and innovation in the payment area, PSD2 provides for two main new types of payment services:

- Payment initiation services
- Account information services

The different players in the new PSD2 world

- **TPP |Third party payment service provider** (a payment institution which does not hold payment accounts for its customers and provides payment initiation and/or account information services).
  It can act as:
  - **AISP | Account information service provider** (aggregation of online information for multiple payment accounts in order to offer a global view of the customer's daily finances, in a single place, to help them better manage their money)
  - **PISP | Payment initiation service provider** (facilitation of online banking to make a payment)
- **ASPSP |Account servicing payment service provider** (provision and maintenance of the customer's payment account). Credit institutions (to put it simply, banks), payment institutions and electronic money institutions can be ASPSP, but also AISP and PISP.

The RTS regulate how the access to the customer's account is shared between the ASPSP and the AISP or PISP

Consent

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

Secure communication channel

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.

Two possible secure communication channels (provided by the ASPSP to the AISP or PISP)

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 a 'fall-back mechanism', i.e. measures that should be taken to restore access to the customer payment account if the API happens to not be available.

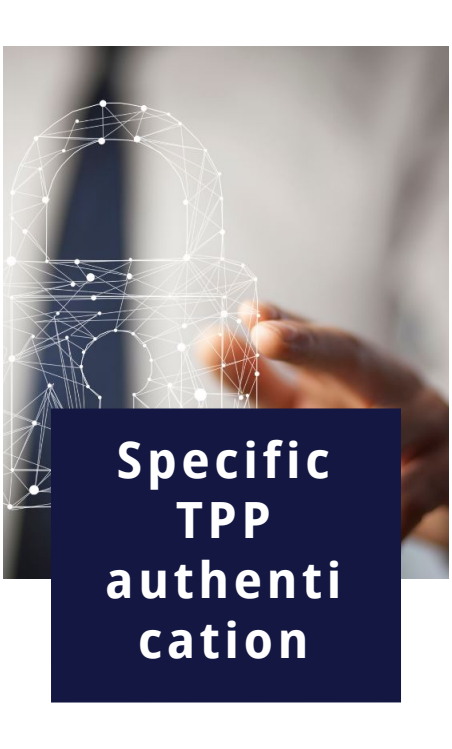
EXCEPT:

- If the API meets the quality criteria defined in the RTS and
- if the API has been successfully tested by the market
- and approved by the national competent authority (which itself should have consulted the European Banking Authority (EBA), to ensure a consistency of quality criteria for APIs).

2

Via the adaptation of the customer online banking interface

The TPP 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'.



Specific TPP authentication

The ASPSP knows when the access to the account is initiated by the customer or the TPP.

Formal agreement

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

GDPR

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

4

Calendar

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

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.

13 January 2018
PSD2 enters into effect, with the main exception of the security measures described in the RTS.

13 March 2018
The European Parliament and the European Council approved the final RTS.

In September 2019
18 months after their publication in the Official Journal of the EU, the RTS apply.

5

Transition period

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

No RTS application

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

Passporting

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

Exemption requests

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

EBA to provide clarifications

EBA invites all stakeholders to ask questions about potential remaining grey areas of the RTS, and will publish answers to clarify some points.

* Note that there are other complementary regulatory texts which further explain the PSD2's principles. The European Banking Authority is also responsible for delivering five other technical standards, five sets of guidelines, and a register. For the sake of simplification, when we mention in this infographic 'the RTS', we refer to the RTS on SCA and CSC (version approved by the European Commission on 27 November 2017), though there are other RTS.