

UNDERSTANDING THE FINAL REGULATORY

ıropean

Strong

of SCA is to

protection via an increased

When carrying out

any action through

a remote channel which may imply a

risk of payment

fraud or other

abuses.

How is SCA applied?

two of the following items:

Inherence

Something the user

is (biometric

identification like

fingerprint, iris or voice recognition...).

At unattended

payment terminals

for transport fares

and parking fees.

When the online

payment account is

consulted, SCA is

needed only the

first time and every

90 days.

A unique authentication code which dynamically links the transaction to a specific amount and a specific payee

(for remote internet and mobile

payments).

The customer's identity has to be verified, using at least

ensure

level of

customer

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

The Regulatory

Technical Standards (RTS*) for strong

TECHNICAL STANDARDS for strong customer authentication and common and secure open

standards of communication under PSD2

(PSD2). PSD2 aims to make payments safer, increase consumers' protection, version of the Payment Services Directive.

foster innovation and competition while ensuring a level playing field for all actors, including new ones which were not regulated by the first

The RTS are implementation

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

transposed in national law.

requirements between the relevant actors. They are for payment

therefore more concrete than PSD2. providers to They are directly applicable in the Member

service PSD2.

States of the EU and do not have to be

comply with

customer authentication The principle

security of electronic payments. When does SCA have to be applied?

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

accounts).

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

For remote payments (online and mobile)

of low value (up to

€30).

EXCEPT:

When a cumulative

value of €100 is

• Or when 5 payments

of up to €30 have

For online

transactions (credit

transfers, card-

based) towards a

trusted beneficiary

(i.e. already

identified by the

payer).

reached.

been made.

application?

possible:

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

all remote

transactions

What are the possible exemptions to SCA The RTS list a number of possible exemptions, to keep electronic payments as convenient and seamless as

For contactless card

payments up to €50.

When a cumulative

value of €150 is

payments of up to

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 fraud rates observed by the payment

was no SCA measure in place and if the

payer did not act fraudulently.

reached.

• Or when 5

contactless

€50 have been made.

Who is responsible for SCA application? PSD2 foresees that the payer can claim The payment full reimbursement from their PSP in service case of an unauthorised payment if there



and secure

is the second

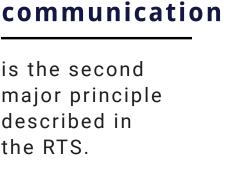
described in

the RTS.

major principle

(PSPs)

providers



The different players in the new PSD2 world

place, to help them better manage their money)

online banking to make a payment)

• 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

- AISP | Account information service provider (aggregation

- PISP | Payment initiation service provider (facilitation of

of online information for multiple payment accounts in order to offer a global view of the customer's daily finances, in a single

service provider are lower than the pre-set reference fraud rates (as described in an Annex to 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

information services).

It can act as:

PISP.

Consent

online banking interface

Specific TPP

authenti

cation

The ASPSP knows

when the access to

the account is

initiated by the

customer or the

TPP.

Between December 2015

The EBA drafts the RTS,

subject to several rounds

European Commission. A final version of the RTS is adopted by the Commission

and November 2017

of reviews with the

in November 2017.

Via the

adaptation of

the customer



Transition period What is likely to happen between implementation as

the PSD2

2019?

and the RTS application in September

from January 2018

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. EBA to clarifications

© European Payments Council AISBL

No RTS

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.

make their competent the EBA.

Secure communication channel making it possible for them to propose their services. Two possible secure communication channels (provided by the ASPSP to the AISP or PISP) Via a dedicated This is concretely translated into the creation of an Application communication Programming Interface (API), a interface sort of messenger enabling information exchanges, taking a request from the TPP, and returning an answer. The API should: The ASPSP has to provide a 'fall-back • Offer at all times the mechanism', i.e. same level of measures that availability and should be taken to performance as the restore access to customer's the customer online interface. payment account if the API happens Enable the TPP to to not be available. properly provide payment initiation or **EXCEPT:** account information services, without any • If the API meets the quality criteria obstacle. 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

 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 The RTS regulate how the access to the customer's account is shared between the ASPSP and the AISP or Customers have to give their explicit consent to the AISP or PISP to share their payment account data or to initiate a payment transaction. The ASPSP has to provide the AISP or PISP a secure communication channel to provide access to the payment account and therefore



of 'screen scraping'. **GDPR** The requirements of the General Data Protection Regulation (which

applies in May

2018)

strengthens the consumer's protection.

Formal

agreement

The customer formally

agrees on the access,

use, and processing of

their payment account

information.

European Banking Authority (EBA), to

quality criteria for

The TPP accesses the customer's payment account by using their

interface and their personalised

It can be described as a more

security credentials, with however a secure authentication of the TPP.

secure and sophisticated version

consistency of

ensure a

APIs).

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

> ASPSPs can already exemption requests (to implement SCA) to their national authority, which will have to consult with

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,

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

Calendar

The creation of the RTS is the result of a

process involving

institutions and many

payment stakeholders.

13 January 2018

apply.

European Union

Exemption requests

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.