The European Parliament and the Council of the European Union have adopted a new regulatory framework for online banking and payments. This new framework is known as the Payment Services Directive 2 (PSD2), which is set to replace the existing Payment Services Directive (PSD1) and to bring more competition and innovation to the financial sector.

One of the key elements of PSD2 is the requirement for strong customer authentication (SCA). This means that customers must be authenticated using at least two of the following means:

- Knowledge (e.g., password)
- Possession (e.g., mobile phone)
- Inherence (e.g., fingerprint)

SCA is designed to increase security for online payments, and it is mandatory for transactions over €30. It is important to note that the requirement for SCA applies to transactions initiated by the customer, whether online or mobile.

The RTS (Regulatory Technical Specifications) are the technical standards to be implemented by the European Payments Council (EPC) in November 2017. The RTS list a number of possible exemptions, to keep the application of strong customer authentication as limited as possible.

The RTS are © the RTS. They are therefore more concrete than PSD2, and to enable the RTS to be understood, the European Parliament and the Council of the European Union will publish answers to clarify some grey areas of the RTS, and will consult the national competent authorities (which, in the case of the United Kingdom, will be the FSA and the FCA).

The ASPSP has to provide the AISP or PISP a dedicated API to get access to their online interface. The API should:

- Provide a 'fall-back mechanism' if the API meets the security requirements of the RTS
- Provide information on the performance of the security mechanisms
- Be adapted to the security requirements of SCA

The role of the RTS is to define specific application and implementation as well as major principles in PSD2, and to implement the strong customer authentication standards of communication and security.