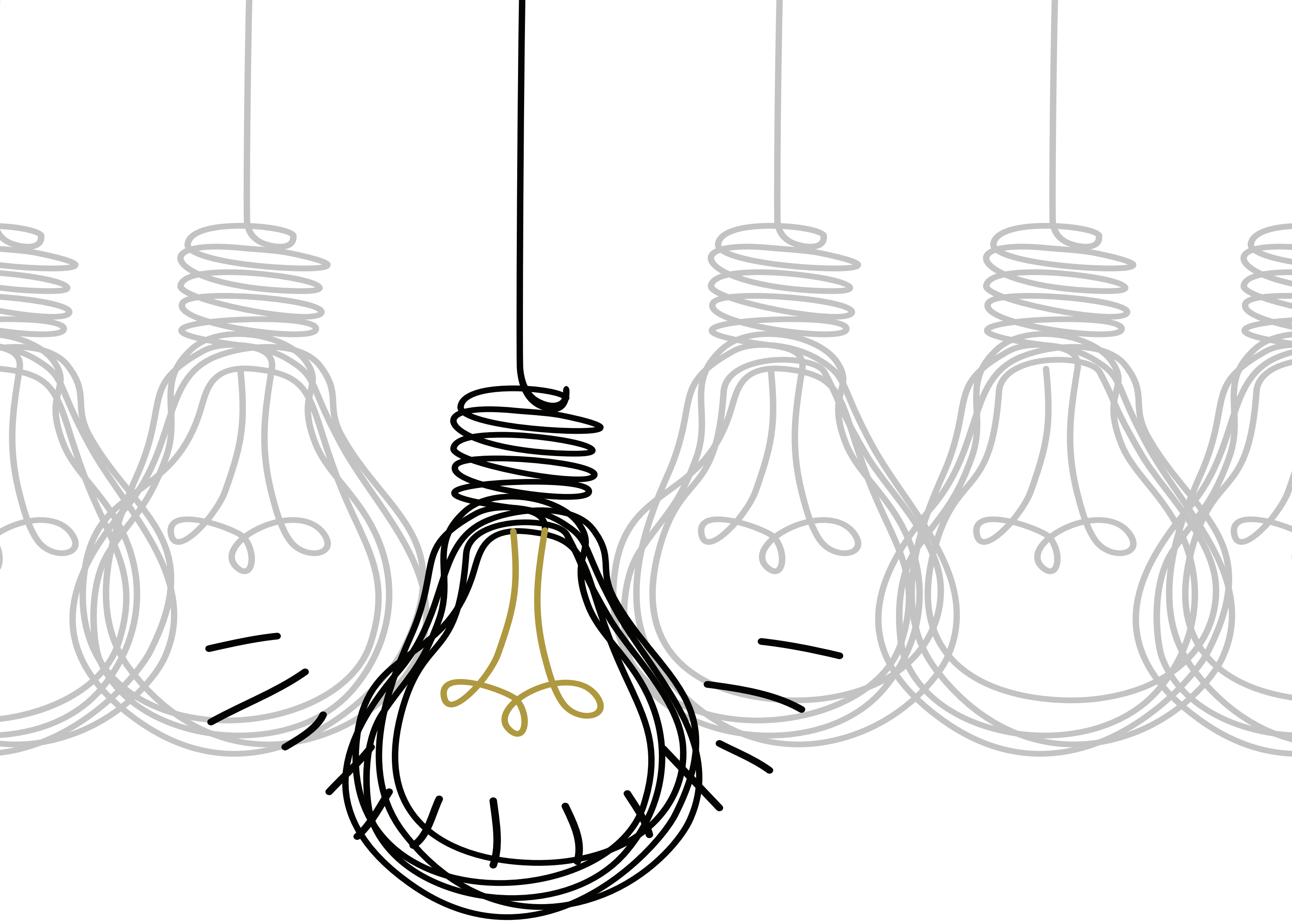

THE FINAL PSD2 RTS ON SCA AND CSC IS HERE WITH CHANGES

WHAT SHOULD WE RETHINK?

On the 27th of November the European Commission published the final version of the PSD2 RTS on SCA and CSC (Regulatory Technical Standard on Strong Customer Authentication and Common and Secure open standards of Communication – you can find it here in the links below), the most crucial element of them all for ASPSPs and FinTechs as well. Now it is up to the Parliament and the Council to accept or refuse it during the 3 months of scrutiny, if nothing changes we can expect it to go live in September 2019 fully.

Online
BUSINESS TECHNOLOGIES

www.online.hu/contact

HISTORY

Originally, the creation of the RTS was mandated to the EBA and due to the large interest of the public, with the lengthy consultations they ended up publicating it February 2017. After the amendments suggested by the commission, the EBA reflected that according to their professional opinion most of the changes are not to be implemented in the RTS. And now, in November it seems like the Commission shoved aside many of the opinions of the EBA. What has changed in contrast to the RTS version of February 2017?

CHANGES

THE FALLBACK MECHANISM

The change we can read most about is the ban of screen scraping, now officially, which is more than welcome by the banks. Although if you read deeper, you can find a little thing called the fallback option, which is mandatory to provide, even if one decides to put a dedicated interface in place. This means several things:

- If an ASPSP doesn't have a dedicated interface, it shall allow the TPPs to use the customer facing interface with the additional feature of TPP identification and the restrictions to data access mandated by PSD2 (Article 31 – Access interface options)
- If an ASPSP decides to make a dedicated interface they have to make the above changes as well as a fallback option to TPPs (Article 33 – Contingency measures for a dedicated interface)

In our view the first option is basically screen scraping with the identification of the TPP. As an ASPSP you can be exempted from maintaining this fallback mechanism, if your competent authority, after consulting with the EBA, decides you comply with the mandated requirements. This exemption can be revoked after noncompliance for 2 consecutive calendar weeks. Some of the requirements are quite hazy and might lead to inconsistencies among the member states, like this one:

- "it has been designed and tested in accordance with Article 30(5) to the satisfaction of the payment service providers referred to therein"

This one raises some interesting questions about what the satisfaction can and should mean in this context…

What is also interesting, that how will national authorities decide on the exemptions, and what tools and methods will they be using to monitor and stress-test the performance of the dedicated interfaces in all the ASPSPs. It is important to keep in mind, that this is an EU level regulation with the passporting behind it, so national level rules are supposed to be compatible with each other.

REDIRECTION IN APIS AND OTHER OBSTACLES

Many of the standards that have been created up until today (NextGenPSD2, Open Banking UK, STET etc.) are based on the OAuth standard, which is based on the concept of redirection. This is the solution behind using a Google/Facebook account for different services and it was the obvious choice for PSD2 for allowing TPPs to use banking services using the payment users' accounts. In the latest changes there is a section in article 32 that describes in some details what is expected from a dedicated interface.

One such interface, for it to be compliant with RTS, "shall … not create obstacles to the provision of payment initiation and account information services". What might these obstacles be, you might ask. Well here the RTS seems to be more clear than on other use, though the use of the word "may" leaves us wondering how forbidden these methods are ("Such obstacles, may include…"). One of the no-no-no-s is redirecting to the ASPSP for authentication or other functions, which was the fundamental concept of banks, having most of the responsibilities according to PSD2, to make sure that security credentials are staying confidentially within their boundaries. It is not quite understood what this exactly means, there are some speculations about this, that it might be illegal in some cases and legal in some other cases, we will see how it turns out, now it is very uncertain how TPPs under PSD2 can and are allowed to perform the strong customer authentication for their users at their ASPSPs.

Similar to redirection, there are some other named obstacles in the new text, such as:

- "preventing the use by payment service providers referred to in Article 30(1) of the credentials issued by account servicing payment service providers to their customers,
- requiring additional authorisations and registrations in addition to those provided for in Articles 11, 14 and 15 of Directive 2015/2366,
- or requiring additional checks of the consent given by payment service users to providers of payment initiation and account information services"

This can also be interpreted in many ways, some might understand it as ASPSPs are not allowed to make TPP registrations for their services, they have to trust the EIDAS certificates (which are not yet standardised) and also they have to trust the user consent as provided by the TPP, although by creating the API definitions for the different types of user consents, the latter can be made very clear and easy to check. The first one on the other can mean, that by no means can an ASPSP forbid the TPP from submitting the security credentials of the payment services user as a means of authentication, which might concern some bank IT security officers.

QUESTIONS UNANSWERED

Starting from the earliest version of the RTS there were some debates about how much this document is going to be Technical or even Standard while being definitely Regulatory. It was publicly stated that it is the basic concept for it to remain technology independent, but not having any standards is quite risky and not what the banking world is used to having. In this hazy environment some questions arose with the texting being crystal clear in some places and very questionably so in others.

The first and foremost question about SCA is who decides to exempt from it. Basically you would say it is the TPP, because the direct client contact is there but there can be some catches here. One is if the TPP is relying on the authentication of the ASPSP and the other is if the TPP decides to exempt from SCA and the ASPSP's internal mechanisms decides it is mandatory to do SCA. Not unsolvable, but not too clear and obvious.

The other question is also related to exemptions, it is still not clear whether ASPSPs will be allowed to calculate the fraud rate by channel, or is there room for more distinctive calculations like forming several groups or even individual fraud rates if the computational capabilities allow it (and why wouldn't they?).
These are only just part of the questions that might have arisen as many internal discussions are happening across the EU and we are to see what is coming out of those.

CONCLUSION AND LOOKING AT THE FUTURE

What is sure that the publication of the final RTS is definitely not the end of the discussions on RTS of SCA and CSC. I expect to see some clarification from the regulator side and also on some parts it is not as necessary as one might think. The market will decide how to respond to the challenges of the RTS and the open APIs, they are going to happen, it is going to be huge, and the playing field is changing.