Meeting date and place

Meeting held on 18/04/2017 in SPA2

Participating organisation(s) & representative(s)

[redacted] Accredited person - [redacted]
[redacted]
[redacted] Apple
[redacted] Apple
[redacted] Apple

Main issues discussed

Meeting with Apple to discuss the latest developments of their electronic wallet, called Apple Pay and the potential usages that PSD2 would provide for in expanding this product.

Apple Pay is a wallet solution that allows for the storing of multiple payment cards, loyalty and brand cards in one single app on your IPhone or MacBook. Apple Pay considers itself not a payment service provider. It acts as a technical platform that allows the payment to be made by the respective PSP. Apple Pay does not have access to funds or to the transactional data, nor does it store the card number associated with each of the cards. The personal credentials attributed to the cardholder by the issuer of these cards are stored locally on a standalone chip in the IPhone or MacBook and is not accessible to Apple. Through the use of touch ID for each and every payment, a unique code is created for each individual payment transaction. There is a triangle relationship between the cardholder, Apple Pay and the card issuer; the card issuer has to agree to the use of the wallet for making payments with the respective card and the use of touch ID for the authentication of the transactions.

Apple enquired about the possibilities under PSD2 for Apple Pay to be used as a platform by TPPs. The Apple Pay technology would allow them to make use of their own authentication mechanisms (or in fact Apple's touch ID), instead of relying on the authentication mechanisms used by banks, which often take much longer. We explained that PSD2 is technology neutral and also does not require that TPPs rely on the authentication mechanisms of the banks, but in practice banks may oppose to this in the current business climate.

Apple raised also some technical issues in relation to the audit obligations of PSPs under the RTS. The relevant provisions would not acknowledge situations where security is not provided by the PSP itself but is outsourced to a third party. In such a case, the PSP should not audit the security itself but should be allowed to rely on the results of the external audit called in by the third party itself. Apple would send drafting suggestions on this point.

Directorate or unit

FISMA D/3

Author of minutes

[redacted]

Validator and validation date

[redacted] validated the minutes on 29/05/2017