Response to EBA Consultation

General feedback from Credit Kudos on EBA Draft Guidelines on the conditions to be met to benefit from an exemption from contingency measures under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)

For more information please contact compliance@creditkudos.com.

13th August 2018

Introduction

Credit Kudos is a regulated AISP authorised by the Financial Conduct Authority in the UK. Our mission is to build a new, fairer kind of credit bureau powered by Open Banking and the financial data made available through an Open Banking ecosystem.

Credit Kudos actively contributes to discussions with and debates within the Open Banking Implementation Entity on a regular basis. As one of the first AISPs to be authorised in the UK and having worked with all the banks on their deliveries under Open Banking, we have a high-fidelity view into how regulatory guidelines are implemented on the ground.

General Feedback

We support the principle of firm guidelines being introduced to the market in order to hold market actors to account. We believe these guidelines would move the market some way towards its intended destination of facilitating competition and innovation in the payments market.

These draft guidelines are opened for consultation at a critical juncture. With over 6 months of practical experience of how the CMA9 ASPSPs build towards PSD2 compliance in the UK, many issues remain unnoticed that should be of primary concern to regulators. The full extent of the issues will not be described in this document but the draft guidelines, as currently worded, touch on a number of them.

As written, we believe these draft guidelines would entrench incumbent market actors and stifle TPPs, rather than foster competition.

There are three key areas of concern within the guidelines:

1. The guidelines place far too great an emphasis on ASPSPs self-reporting performance metrics without consulting the TPP community who can highlight performance far more transparently. We believe this would likely lead to a “he-said-she-said” scenario between TPPs, ASPSPs and CAs.

2. There seems to be some misunderstanding in the guidelines as to how APIs function and which interactions between ASPSPs, TPPs and PSUs are comparable. As a consequence, we believe some guidance as written would further help incumbents and hinder challengers.

3. Whilst we support rigorously-defined KPIs through which to measure ASPSP performance, we believe the guidelines are not sufficiently precise in their definition nor wide enough in their scope as to be useful in holding incumbent market actors to account.

We elaborate on each of these points and other smaller points of agreement and disagreement with the guidelines in the following sections.

Issue 1: ASPSP Self-attestation of conformance

The majority of your consultation states that the responsibility for reporting on the functionality of the PSD2 ecosystem should be placed on ASPSPs. We believe this is ill-advised.

We support your view that “ASPSPs should have the same service level objectives and targets, contingency plans, monitoring and out-of-hours support for their dedicated interface as for the PSU interface” (para. 18). However, in our experience, statistics reported by ASPSPs can be misleading and we believe it naïve to assume ASPSPs would “do the right thing” and act in a transparent manner towards the market when KPIs may be embarrassing or where it is not in ASPSPs’ best interests to do so.

We believe it would be wise to seek attestation of ASPSP conformance to performance targets from both ASPSPs and TPPs.

Many TPPs, ourselves included, are building our entire business on PSD2-style Open Banking foundations. Without a functioning market, competition is impossible, incumbent entrenchment is inevitable and the goal of PSD2 will not be reached. Because of these simple facts, TPPs are extremely invested in making the ecosystem work and holding ASPSPs to account - a goal shared by CAs. We have gone farther than some in publishing statistics related to the CMA9 performance under the Open Banking specifications in the UK. We make these statistics public at https://creditkudos.com/obstats for your reference.

We believe other TPPs would be more than happy to contribute statistics related to the performance of the ASPSPs they work with in order to provide an objective cross-referencing tool for CAs to consult when assessing ASPSP conformance.

The benefits of such an approach are clear:

1. Reported metrics are objective, outcome-focused and impossible to obfuscate by ASPSPs

2. Providing assistance to CAs, TPPs take greater responsibility in the market and drive the ecosystem forward

3. Better ASPSP performance leads to better customer outcomes and increases competition in the market

We would offer to the EBA the opinion that measuring real-world performance of ASPSPs is the goal of the guidelines and any measurements derived solely from self-attested ASPSP data could end up being somewhat synthetic. It is highly unlikely that self-attestation would realistically cover all possible market scenarios.

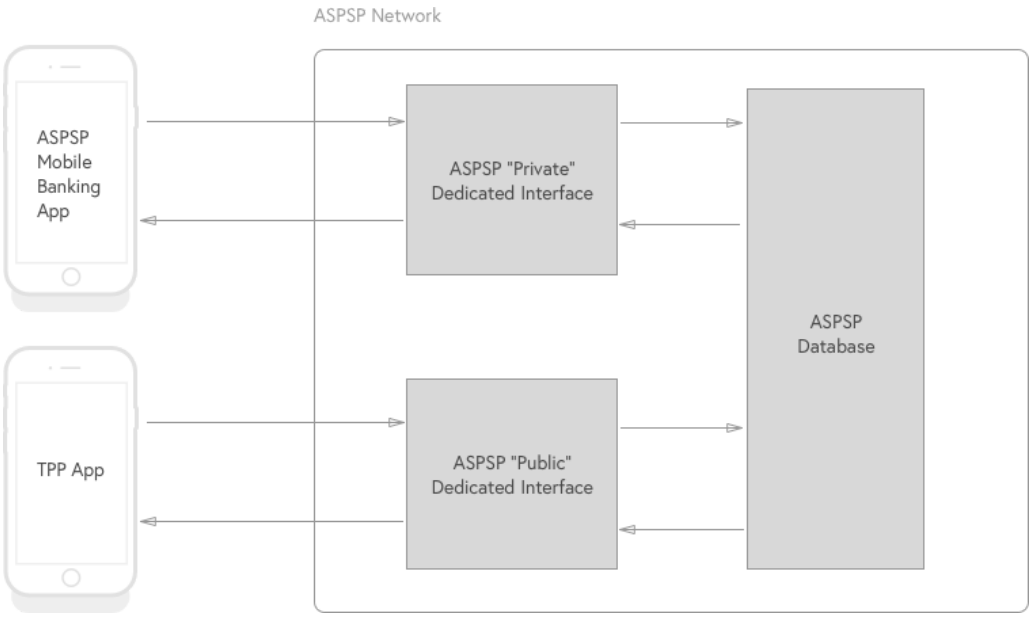
Issue 2: On the functionality of APIs

There seems to be some misunderstanding in the guidelines as to how APIs function and which interactions between ASPSPs, TPPs and PSUs are comparable.

"Furthermore, the EBA has arrived at the view that the ASPSP can have more than one PSU interface, and many will have a least two, online banking and mobile banking interfaces. ***This makes comparison of the dedicated and PSU interface difficult*** *as when access is via a dedicated interface it will not always be apparent to the ASPSP whether the PSP access to the dedicated interface is instigated via the PSU online or PSU mobile interface." (para. 24)*

Our first observation is that comparison **must** be possible here. Without comparability, we believe ASPSPs will hide behind this clause if the performance of their dedicated interface is not satisfactory to TPPs.

The second thing to point out is that **accessing data via the PSU interface and via the dedicated interface are two directly comparable methods of access**. Any web or mobile customer experience, or any other experience offered by an ASPSP to a PSU through another medium, are backed by *private dedicated interfaces* unavailable to TPPs. To stay within our terminology for a moment, one could describe APIs available to be consumed by TPPs as "*public dedicated interfaces*". We illustrate in the following diagram.



Transmitting data over the internet is not possible without a dedicated interface. As you can see in the diagram, in order for the ASPSP Mobile Banking App to be able to pull data from the ASPSP Database, there must be a dedicated interface in between.

What should be apparent is that both dedicated interfaces are performing precisely the same function (namely retrieving data from a database and passing it to an external client) and are therefore directly comparable.

For example, in a scenario in which a TPP wishes to show a PSU a detailed feed of transaction information in the TPP App, it is reasonable to demand that the dedicated interfaces that power the TPP App to be as performant as those that power the ASPSP Mobile Banking App.

It would be anti-competitive for it to take longer to load the transactions within a TPP App than it would for an ASPSP Mobile Banking App. Data on the performance of the *private dedicated interfaces* is available in the market, as at least two companies reverse-engineer ASPSPs' *private dedicated interfaces* and sell their own APIs to other TPPs. To date, there is gulf in performance between what the CMA9 ASPSPs provide in their own apps, and what TPPs are able to consume via Open Banking APIs. This must be addressed.

Issue 3: KPIs must be more precise and wider in scope

We believe KPIs and other performance indicators are vital for a functioning ecosystem. We support the direction of travel outlined by the EBAs draft guideline 2.3 but feel the requirements should go further.

"2.3. The ASPSP should have in place at a minimum, the following indicators for the performance of the dedicated interface:

a. the time taken for the ASPSP to provide to the payment initiation service provider (PISP) all information on the initiation of the payment transaction as required by Article 66(4)(b) of Directive(EU) 2015/23667 (PSD2) and by Article 36(1)(b) of the RTS;

b. the time taken for the ASPSP to provide to the account information service provider (AISP) all payment related data as required by Article 36(1)(a) of the RTS;

c. the time taken for the ASPSP to provide to the card based payment instrument issuer (CBPII) and PISP a yes/no message as required by Article 65(3) of PSD2 and by Article 36(1)(c) of the RTS."

To offer an AIS example, most AISPs require many different data points to be collected to perform their function (such as a PSU's accounts, transactions, direct debits and the PSU's list of beneficiaries). The duration of ASPSP responses to TPP requests for each of these different data points vary widely both within an ASPSP and between ASPSPs. This is natural in the former case, as one is likely to have far more transactions than beneficiaries. TPPs would likely collect this information in parallel, meaning the completion time would likely be bound by the slowest-responding resource.

We feel that **request latency is an additional KPI** that can be benchmarked to an ASPSP's PSU interface. For instance, for a page of transactions, does the public dedicated interface respond in a comparable number of milliseconds to the ASPSP's private dedicated interfaces (web, mobile, etc). This should follow the logic identified for uptime when it comes to handling multiple interfaces as defined across paragraphs 22-24.

In addition, we feel that **error response rate is an additional KPI** that should be benchmarked to an ASPSP's PSU interface. This would address the chronic attitude problem exhibited by ASPSPs whereby simply because a PSU is engaged with a TPP, they are somehow deserving of second-class treatment. It would not do for an ASPSP to have patchy responses for customers of their own application. This should be mirrored for responses to TPPs communicating via the ASPSPs dedicated interface.

Further, it is important to distinguish "downtime" from "degraded services". On many occasions dedicated interfaces have exhibited inconsistent behaviour across users due to the nature of the underlying technologies. As such, we encounter cases where account information data cannot be accessed through the dedicated interface for a

given cohort of PSUs but this would not accurately be reflected in naïve uptime/downtime calculations.

Questions that remain for the EBA

The very vast majority of your consultation paper covers metrics related to performance and availability. These are features which can be focussed on in the context of a mature ecosystem of functioning services.

Question 1: How do you plan to address the lack of ASPSP functionality given the very great number of problems that have been experienced, and continue to be experienced in the UK to date, and will likely be experienced as the wider European market move towards adopting dedicated interfaces under PSD2?

Article 98 (d) of PSD2 mandated the EBA to develop regulatory technical standards on "the requirements for common and secure open standards of communication for the purpose of **identification, authentication, notification, and information, as well as for the implementation of security measures**, between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers".

Paragraph 27 of your Opinion on the implementation of the RTS on SCA and CSC states: "Additionally, the EBA clarifies that the scope of data to be shared with AISPs and PISPs by the ASPSP under PSD2 and the RTS on SCA and CSC **does not include the PSU's identity** (e.g. address, date of birth, social security number) given that those are not data that are necessary or requested to initiate a payment or access account information under PSD2."

Question 2: Are you aware that the vast majority of AIS use-cases - and indeed a functioning API-based ecosystem - depend on confirmation of some aspects of a customer's identity (such as name, email address, postal address, phone number, collectively "Account Holder Information") in order to avoid bad customer outcomes?

(For instance, if PSU data is delivered via a dedicated interface to a TPP for the purposes of carrying out a credit affordability calculation, without the TPP being able to assert that the collected account information applies *to the intended PSU*, there can be no guarantee that the end user has not used credentials belonging to a *different PSU*. This could lead to money being lent fraudulently - a concern raised by almost all of our clients.)

Question 3: How do you plan to develop a standard for the purpose of "identification" if, in your Opinion, the scope of data to be shared with AISPs and PISPs does not include the PSU's identity?

Question 4: Are you aware that, as a consequence of your Opinion, UK ASPSPs will likely not provide *any* identity-related information via their dedicated interfaces, even if that information is made available to a PSU via the ASPSP's PSU interface?

Question 5: Do you realise, as another consequence of your opinion, you have struck material blows to the competition objective of PSD2 as ASPSPs will, in the TPP role, be able to accurately tie account information to identity information where non-ASPSP TPPs will not?

Question 6: As a corollary to question 5, are you aware that, as a consequence of your Opinion, you have created a potentially unregulated market for the screen-scraping of account holder identity information that might exist outside of PSD2 regulations? The market is not functional without PSU identification meaning many TPPs will continue to screen-scrape this information and not require regulation to do so.