Summary of the 5th Meeting of the API Evaluation Group

27 March 2018, 9h00-17h00 CEST

EPC, Cours Saint-Michel 30A, 1040 Brussels

(Approved by the API EG Members)

1. Welcome

The co-chair J. Whittle (NPSO Ltd) welcomed the participants to the fifth meeting of the API Evaluation Group (EG) and conveyed the apologies of the other co-Chair, O. Berglund (Trustly Group AB) who was exceptionally unable to attend this meeting (Please see Annex I for the list of attendees).

J. Whittle informed that the goal of this meeting would be to i) ensure that the work on the 'hot topics' is progressing, ii) review in detail the input documents received in relation to the redirection 'hot topic', ii) review the list of API standard requirements and iv) provide a status update on the activities of the technical expert evaluation subgroups. In view of the time pressure he suggested to assess whether the API EG could meet more frequently.

2. Approval of the agenda (API EG 016-18)

The agenda was approved unchanged.

3. Approval of summaries of previous meetings (API EG 017-18; API EG 018-18)

The summary of the third meeting held on 27 February 2018 was approved subject to the inclusion of the change suggestions provided by the EBA and one editorial clarification in section five.

The summary of the fourth meeting held on 28 February 2018 was approved unchanged.

The approved minutes will be published in due course on the EPC website.

4. Approval of the summary of the API Evaluation Workshop (API EG 019-18)

The summary of the API Evaluation Workshop held on 28 February 2018 was approved unchanged. The approved summary will be published in due course on the EPC website.

Note in editing: The API standard initiatives will be invited to review an excerpt from these minutes related to the respective status update they provided during the workshop.

5. Regulatory updates

The European Commission (EC) representative R. Jacob informed that the final Regulatory Technical Standards (RTS) on strong customer authentication (SCA) and common and secure open standards of communication (CSC) (the RTS) had been published in the Official Journal of the EU on 13 March 2018. The RTS will come into effect on 14 September 2019. This also means that the account-servicing payment service providers (ASPSPs) have 12 months to build dedicated interfaces in case they wish to obtain an exemption from having to provide a fallback solution.

An update was provided on current developments on a national level such as in France and Finland. For example, in France the national competent authority (NCA) is currently contemplating to make the use of dedicated interfaces mandatory before the 18-month deadline, subject to APIs passing the necessary tests. It was clarified that an API that is used before the effective date of the RTS will need to fulfil the same requirements as APIs that are implemented after the RTS has come into effect. In practice this would however mean that an ASPSP would be able to close the access to its online interface before the RTS are effective. Moreover, in France they are also discussing to open up the access to all types of bank accounts.

The EBA representative informed that the EBA continues to act as the linking pin between the API EG and EBA members (the NCAs). To this end, the EBA had already invited the API EG co-chairs to provide further information in relation to the 'hot topics'. The EBA is very conscious of the timing for implementation and firms obtaining an exemption from building the fallback (the 6 months has no timeline built in for assessment; application to NCA; consultation with EBA; final decision) and would want to factor into their engagement with NCAs as much clarity from the API EG as possible.

6. Review list of key topics which require further clarification ('hot topics') (API EG 020-18)

At is previous meeting, the API EG had agreed on a list of key topics (the so called 'hot topics') for which further clarification would be needed. For each 'hot topic' a dedicated task force had been allocated.

A status update was provided for each of these 'hot topics' by the respective dedicated task forces. A detailed discussion took place in relation to the redirection topic.

Topic 1: Redirection vs other authentication methods

Two input documents on the topic of 'redirection' had been provided to the API EG members prior to the meeting. One had been prepared by the ASPSP participants in the dedicated taskforce and the other one represented the view of the TPPs. It is however still a work in progress and the idea would be to merge the two documents into one. As a first step the aim is to be able to frame the issue.

J. Whittle commented that ideally the API EG would be able to reach a conclusion during today's meeting which could then be provided as input to the EBA.

Reference was made to a meeting that had taken place recently in The Hague where the EC had made some comments in relation to redirection. R. Jacob informed that

redirection had initially been included in the RTS as an example of an obstacle but that all depends on how redirection is operated. He clarified that the EC does not have an issue with redirection on the condition that it supports the business models of the TPPs and ensures a convenient customer journey. The discussion should however not be limited to redirection as there are also other solutions that can be looked at.

TPP representatives expressed their concerns with redirection and the implications for their sector. The assumptions that redirection increases security were particularly unclear. There was a view expressed that no existing redirection solutions were considered acceptable because the implementations were overly complex and therefore resulted in customer drop-off. It was agreed to inform why customers are dropping off in these scenarios.

The EuroCommerce representative informed that convenience and security are key for the customer. One-click authentication is what the customer and retailer will expect.

The EBA representative remarked that discussions focused on current business models and all parties should be mindful of new actors to the market. The aim of this initiative and PSD2/RTS was to move to APIs. If too many authentication solutions are expected to put in place by ASPSPs will this not impact the business case for a dedicated interface? J. Whittle agreed that this is indeed the problem statement and that the API EG goal is to get the API standard initiatives in a space where they will be able to increase the chances of the ASPSPs implementing their standard of getting an exemption from having to provide a fallback solution. It was clarified earlier that redirection is not prohibited as such, but it should also be taken into consideration that the implementation of redirection could have undesirable consequences for payment service users (PSUs) and for TPPs.

From the ASPSP side it was commented that ASPSPs would at least need to offer one authentication method. Whatever that solution would be, the ASPSP will want to ensure that it is widely used by the TPP market as otherwise it will not obtain an exemption and hence will need to offer a second solution.

On the use of redirection in a mobile context the views of the ASPSPs versus TPPs are getting closer. However, in relation to the use of redirection to a PC web-browser this represents challenges as was explored in the ERPB PIS report. Use by the TPP of the personalised security credentials issued by ASPSPs cannot be prevented (note: to be read in conjunction with the ‘hot topics’).

The definitions of the three authentication methods were reiterated as follows to ensure that everyone had the same understanding:

- Redirection: the PSU is visibly redirected from the TPP domain to the ASPSP(s)domain (webpage, app, separate device etc.) for the sole purpose of authentication. The PSU may, or may not, be redirected back to the TPP domain.
- Decoupled: the PSU experience is decoupled from the technical facilitation of the authentication between the TPP and ASPSP domains. The PSU would ideally not be visibly redirected from the TPP to the ASPSP domain.
- Embedded: the personal security credentials of the PSU are transmitted to the ASPSP by the TPP.

The BEUC representative raised a concern that the TPP transmitting the PSU personalised security credentials should not lead to bad customer outcomes and that

BEUC had concerns about consumers using their ASPSP issued credentials with TPPs in particular due to a perceived risk of increased fraud.

A presentation was provided in relation to a Swedish mobile payment solution whereby the PSU is authenticated via BankID in order to initiate a payment via a specific app. Whether this is a decoupled or redirection method is in essence a question of semantics and it depends on the channel that is used. It was a useful illustration of what a good customer authentication journey might look like and highlights the challenges in this area.

According to R. Jacob the key question is about who is allowed to get the credentials. The ASPSP could offer a redirection solution as long as it does not create an obstacle. In addition, some ASPSPs impose on themselves the redirection approach such as in Sweden. In this case redirection seems to be widely accepted by the market in Sweden. However, where redirection might prevent TPPs from offering a better PSU service this would be counter to the intent and purpose of PSD2.

The ECB representative invited ASPSPs and TPPs to further detail their concern in order to find a way forward. From the ASPSP side it was commented that ASPSPs will support one method depending on the channel used. Minimum requirements or compliance is a topic that needs to be discussed by the NCAs (and not the API EG). ASPSPs believe that redirection is PSD2 compliant if it provides a good customer journey. Moreover, some ASPSPs are concerned that, from the perspective of risk management and fraud the embedded approach is not secure enough and that hence redirect and decoupled would be a better alternative. Responding to the suggestion that the TPP license should mitigate this risk the response was that a license does not prevent fraud and that all other counterparties are treated the same way. TPP representatives on the other hand are not in favour of redirection as it undermines the whole purpose of PSD2. It may even use different screens and is unpredictable. Moreover, TPPs believe they cannot be prevented from transmitting the PSU credentials created by ASPSPs. If ASPSPs are however not issuing transmittable credentials (e.g. using fingerprints) then the TPP cannot receive them from the PSU.

The EMA representative added that it should be ensured that the API standard allows for a range of authentication approaches. ASPSPs may choose a preferred authentication method to avoid friction. If it however would present a barrier then TPPs will need to reach out to the NCAs.

J. Whittle summarised that range of authentication processes and design of those to enable SCA are to be standardised by the API initiatives and implemented by the ASPSP. The API EG will expect that the API initiatives define standards that support a wide range of authentication processes – a spectrum of options. This will support the ASPSP to be able to implement one, or more, authentication processes in a standardised uniform way and facilitate market choice. The spectrum of options and the decision of the ASPSP to implement one or more authentication process inherently involves trade-offs between risk, liability, space to innovate, business models etc.

Redirection, for example, could be implemented in a way that will maximise the likelihood of market acceptability. For example, designs that decouple the front-end PSU experience from the back-end ASPSP authentication process are likely to offer a slicker and more frictionless PSU experience, while helping to maximise the innovative space for the TPP. Use by the TPP of the credentials issued by ASPSPs to their customer is also to be considered a relevant option on the spectrum referred to above, and again an API initiative may like to consider supporting this requirement

J. Whittle concluded that the ASPSPs would be advised from day-one to aim at providing at least a slick redirection, ideally decoupled authentication process. As authentication processes will need to evolve as technology and customer interfaces evolve this is not a static situation.

As a next step and to further clarify this topic there would be need for diagrams that depict possible customer journeys in order to help illustrate what 'good' looks like. J. Whittle, together with R. Ohlhausen and G. Boudewijn agreed to work on this and O. Berglund will also be invited to join this taskforce.

As a first step J. Whittle will prepare a generic template (including headings such as problem statement, key principles; diagrams etc.) which the dedicated taskforce could use when formulating their input in relation to redirection. The suggestion would be that this template is also used for the other hot topics that are described below.

Topic 2: AIS data

The dedicated workface had succeeded in incorporating the ASPSP's and TPP's views into one document. The document gives an overview of the:

- The legal context of PSD2 and the scope of account information that results from it (which could be in scope of the API evaluation work).
- The additional information that account information service providers (AISPs) would like to use and the viewpoints of AISPs and ASPSPs in this context respectively.

The conclusion in this draft document is that all information included in a designated payment account and the related payment transactions as far as it does not constitute sensitive payment data and follows the principle of data minimisation is in scope of AIS data. The ASPSPs believe the focus should be on information in scope of PSD2. The AISPs on the other hand argue that information on non-payments account should be included as well in view of the fact that currently 80% of the accounts aggregated are not payment accounts. Indeed, AISPs argue that the access through an API only makes sense if they can access all types of accounts.

The EC representative, P. Pellé however informed that whether or not an API also covers other accounts will not be a criterion that is taken into account to assess the quality of the API. It could however be a plus. The reason being that the PSD2 focuses on payment accounts.

The ECB representative suggested that since the PSD2 scope is limited to payment services and payment accounts, and considering the tight time line, it would be beneficial to focus on issues related to the PSD2 and the RTS.

The EBA representative also noted that the competence of the NCA in this context is limited to the evaluation of PSD2 matters.

Topic 3: Access to payment account information by AISPS (four times a day; 90-day period SCA)

J. Burkovic who was assigned to this topic informed that in his view the fact that the AISP can only check four times a day is disadvantageous as in the ASPSP's interface the information is updated in real time.

The 90-day period SCA topic was not included in the document he had prepared as it is covered by the dedicated interface that is looking at who can apply SCA (i.e. Topic 5).

Topic 4: Consent in scope of PSD2 in the context of the GDPR

G. Boudewijn had shared a document on this topic from his community which was meant as constructive input to the debate.

R. Jacob commented that this was indeed a comprehensive document but that the EC experts would first need to have a look at it. Although it is not an official document, the EC will be able to share its comments or interpretation in case it would not be fully in line with the view of the EC.

A. Mac Dowell will share for information a briefing note to the Swedish Data Protection Authority by the Swedish FinTech Association.

Topic 5: Who applies SCA?

The dedicated taskforce is still busy preparing a document on this topic. The lack of clarity stems from the fact that in some clauses of the PSD2 reference is made to 'PSPs' and hence it is not specified whether it relates to ASPSPs and/or TPPs. The view of the ASPSPs is that PSPs issuing the credentials are in charge of the SCA and applying exemptions to SCA.

P. Pellé explained that the PSD2 allows PSUs to share credentials with TPPs issued by ASPSPs. However, for AISPs it could be a good alternative to use mandates (instead of credentials) to access as much information as allowed by the PSU's consent. The ASPSPs would need to be aware of this arrangement.

J. Whittle suggested that the dedicated taskforce would prepare diagrams in order to have a clearer view on the different scenarios (AIS vs PIS) the API EG is focusing on. A scenario could also be included whereby the AISP issues its own credentials.

Topic 6: The "what" question

J. Whittle noted that the document he and O. Berglund had prepared basically reframes what is already included in the November 2017 report of Euro Retail Payments Board (ERPB) Working Group on payment initiation services (PIS) in relation to the information (i.e. the "What") the ASPSP should provide to the PISP under PSD2.

The ASPSP representatives commented that they did not agree with all the recommendations that are included in the report of the ERPB WG. Moreover, they noted that the ERPB itself did not endorse the report but rather 'took note' of it.

The ECB representative remarked that the ERPB PIS WG report as such had been agreed by the ERPB during its November 2017 meeting without any comments. Moreover, it is in the interest of all actors to reach a conclusion on the guidance on APIs.

J. Whittle added that if the API EG proves to itself to have a view that is different than the view in the report and if it can justify this, that would be reasonable. It should

however be noted that the report is already in the public domain so the rationale to deviate or amend would need to be compelling.

Topic 7: Security

As a first step, the API EG tried to frame this topic. On the one hand it could cover the level of security the API EG expects to see built around an API and on the other hand the API EG should look at the perception of security in relation to the sharing of credentials. Although not everyone was convinced that this was a hot topic, a clear view would be needed on the requirements that the API standard initiatives need to support.

The BEUC representative commented that security is an important topic for the consumers. The goal of using a dedicated interface should hence be to improve security.

R. Jacob noted that it might be helpful to come up with a list of things that could go wrong when using APIs. This could for example be looked at by the technical expert subgroups.

A. Mac Dowell, E. Johansson and L. Gaston volunteered to work on the topic of security.

7. Review of the API standard requirements (API EG 008-18; API EG 013-18)

The ASPSP's representatives had prepared an updated version which clustered the API standard requirements in different categories. A distinction was also introduced between PSD2 related and other requirements. For PSD2 related requirements the relevant articles were also included in a separate column. The ASPSPs had also included additional requirements.

The API EG reviewed the updated list and identified for which requirements it was not yet feasible to reach a consensus. Some requirements were also deleted following this review.

Time is of the essence as a finalised list needs to be provided to the technical experts as soon as possible. The TPPs and ASPSPs representatives are hence invited to further review this document and to send their comments to the EPC secretariat by 10 April 2018 cob.

R. Jacob commented that the list as such does not necessarily need to be consensual and that it could further evolve as a result of the work of the technical expert subgroups.

8. Status update on the technical expert evaluation subgroups (API EG 0014-18; API EG 015-18)

A. Mac Dowell who is acting as a linking pin between the API EG and the technical experts informed that he had invited the five subgroups to provide a status update but that only a couple of subgroups had been able to provide a response. He also informed that several API standard representatives had issues with using Google Drive, which was initially the platform that was chosen to exchange information. To try to resolve the issue an Open Banking UK representative had offered to create a subsite on the 'Confluence' platform for each of the initiatives. Some API standard

initiatives however noted that information about their standard could already be found on their website.

So far, engagement was at the early stages and further coordination is needed. J. Whittle noted his concern to ensure this process works the way the API EG expects. It is critical. It was agreed to schedule a conference call on 12 April 2018 (10-11CEST) with the API standard initiatives and the coordinators of the technical subgroups to provide a status update on the list of API standard requirements and to assess how the engagement process is going so far and whether there are any further suggestions on the best way forward. The engagement with the API standard initiatives is to provide positive support for their work.

The EBA will continue to act as liaison between API EG and NCAs

9. AOB

The API EG had received questions from the Berlin Group and Open Banking UK as input to the 28 February 2018 API Evaluation workshop. J. Whittle suggested that O. Berglund and he would review the outstanding questions.

10. Next meeting date (API EG 004-18)

The following additional meetings were scheduled (see Annex III):

- 12 April 2018 (10-11 CEST): Conference call with the API EG, the representatives of the five API standard initiatives and the technical subgroup coordinators (to provide a status update on the list of API standard requirements and to discuss the way forward with regard to the engagement with the initiatives (via the technical expert subgroups).
- 16 April 2018 (10-17 CEST): Meeting at the EPC offices in Brussels, subject to the majority being able to attend.
- 14 May 2018 (9-17 CEST): Meeting at the EPC offices in Brussels.

Note in editing: The 16 April meeting was rescheduled to 23 April 2018.

11. Closure of the meeting

The co-chair J. Whittle closed the meeting around 16h50 CEST and thanked the participants for the constructive meeting and the positive spirit.

Annex I: List of attendees

Category	Name	Institution	Attendance
Co-Chairs	James Whittle	NPSO Ltd	Yes
	Oscar Berglund	Trustly Group AB	Apologies
TPP Members	Joan Burkovic	Bankin'	Yes
	Aoife Houlihan	Klarna	Yes
	Ralf Ohlhausen	PPRO	Yes
ASPSP Members	Marieke van Berkel	EACB	Yes
	Gijs Boudewijn	Dutch Payments Association (representing EBF)	Yes
	Emil Johansson	Swedbank (representing ESBG)	Yes
PSU Members	Jean Allix	BEUC	Yes
	Juliette Beaulaton[1]	Ecommerce Europe	Yes
	Pascal Spittler	IKEA (representing EuroCommerce)	Yes
Other Members	Thaer Sabri	EMA	Yes
	Krzysztof Korus	Polish Payment Institution Association (representing EPIF)	Yes
Observers	Ralf Jacob	European Commission	Yes
	Philippe Pellé	European Commission	Yes
	Krzysztof Zurek	European Commission	Yes
	Nilixa Devlukia	EBA	Yes
	Helene Oger-Zaher	EBA	Apologies
	Ann Börestam	ECB	Yes
Linking pin with technical experts	Arturo G. Mac Dowell	Eurobits	Yes
Guest	Lorenzo Gaston	Gemalto (Convenor ISO TC 68 / SC2 / SG1 TPP)	Yes
Secretariat	Etienne Goosse	EPC	Yes
	Christophe Godefroi	EPC	Yes

[1] Alternate to Just Hasselaar

Annex II: Action points

Item	Action	Owner	Status / Deadline
5-01	Circulate an updated version of the clustered list of API standard requirements	EPC secretariat	27 March 2018
5-02	Share for information a briefing note to the Swedish Data Protection Authority by the Swedish FinTech Association.	A. Mac Dowell	27 March 2018
5-03	Prepare a generic template to be used to formulated input in relation to the 'hot topics'	J. Whittle	29 March 2018
5-04	Invite the API standard initiatives and coordinators of the technical subgroups to the 12 April 2018 conference call of the API EG	EPC secretariat API EG co-chairs	29 March 2018
5-05	Review the updated version of the clustered list of API standard requirements & provide comments (if applicable)	API EG members	10 April 2018
5-06	Complete the 'hot topic' template	Dedicated 'hot topic' taskforces	12 April 2018
5-07	Review the outstanding questions received from the Berlin Group and Open Banking UK (as input to the 28 February 2018 API Evaluation Workshop)	J. Whittle O. Berglund	12 April 2018
5-08	Provide further background information on why customers are dropping off when using redirection.	A Houlihan	In due course

Annex III Meeting Calendar

2018	API EG Meetings
January	**29 January 2018 (11:00-16:00 CET)** EPC, Brussels
February	**22 February 2018 (10:00-12:00 CET)** Conference call
	27 February 2018 (13:30–18:00 CET) – preceded by lunch as from 12:45 CET EPC, Brussels
	28 February 2018 (9:00-10.30CET) **28 February 2018 (11:00-16:00 CET) API Evaluation Workshop with 5 API standards initiatives** EBF, Brussels
March	**27 March 2018 (09:00-17:00 CEST)** Brussels – EPC
April	**12 April 2018 (10.00-11.00 CEST) - Conference call** **23 April 2018 (10.30-17.00 CEST)[2] - EPC, Brussels**
May	**14 May 2018 (9.00-17.00 CET) - EPC, Brussels** **29 May 2018 (9.00-17.00 CET) - EPC, Brussels**
June	**25 June 2018 (10:30-16:00 CEST)** Brussels – Venue to be confirmed

[2] The 16 April 2018 meeting was later rescheduled to 23 April 2018.