Summary of the 7th Meeting of the API Evaluation Group

23 April 2018, 10h30-17h00 CEST
EPC, Cours Saint-Michel 30A, 1040 Brussels

(Approved by the API EG Members)

1. Welcome

The co-chairs, J. Whittle (NPSO Ltd) and O. Berglund (Trustly Group AB) welcomed the participants to the seventh meeting of the API Evaluation Group (EG). Please see Annex I for the list of attendees.

2. Approval of the agenda (API EG 025-18)

The agenda was approved unchanged.

3. Approval of the summaries of previous meetings (API EG 024-18; API EG 026-18)

The summary of the fifth meeting held on 27 March 2018 and sixth meeting held as a conference call on 12 April 2018 were approved subject to the inclusion of the change suggestions provided by the EBA, the ECB and additional comments provided by API EG members during the meeting.

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

4. Regulatory updates

The API EG was informed that the publication of the EBA "Q&A" tool in relation to PSD2 had been delayed.

5. Review list of key topics which require further clarification ('hot topics') (API EG 020-18; Input documents)

Topic 1: Authentication methods (Strong customer authentication (SCA))

An updated version of this document had been circulated to the API EG prior to the meeting. The API EG discussed and reviewed this document in detail during the meeting. An updated version, including high-level authentication method diagrams, will be distributed to the API EG for final validation, meaning that only showstoppers should be reported at this stage. The aim is to publish the finalised document by 4 May 2018 on the EPC website.

The different market participants provided their views on the range of identified SCA methods. The represented third-party providers (TPPs) are all in favour of the embedded authentication method. BEUC is however against the embedded method as

in this scenario PSUs are sending their credentials to a third party. Account-servicing payment service providers (ASPSPs) noted that as per their regulator they are not allowed to outsource without a contract but that contracts are not allowed under PSD2. Merchants on the other hand are strongly against the redirection method due to the inferior user experience. TPPs moreover argued that redirection does not increase security and does not accommodate e.g. POS payments or payments through other channels such as voice-enabled payments. In their view the latter is already a sufficient argument to conclude that redirection cannot be imposed on TPPs to use.

It was however reiterated that the API EG as such cannot mandate any specific authentication method given that the RTS/PSD2 does not mandate the use of any specific authentication method. The API EG concurred that in order to ensure a good payment service user (PSU) experience, the API standard initiatives would need to support a range of SCA methods (i.e. redirection, decoupled and embedded). In addition, ASPSPs that are building an interface will need to understand that in order to increase their chances of obtaining an exemption from having to provide a fallback solution, the API will need to be widely used. In order to be widely used they will need to ensure a good customer experience. J. Whittle noted however that it is not up to the API EG to say what 'widely used' would look like as it depends on many different factors that vary between ASPSPs and across different markets. The API EG should in general avoid being too prescriptive.

The European Commission (EC) representative noted that it is indeed the ASPSP's choice of how it wants to authenticate but that the API standards would need to accommodate the range of different authentication methods. In addition, the API EG should also give a signal to the ASPSPs regarding what channels are acceptable to the market. He understood from an earlier discussion that TPPs do not seem to be satisfied with redirection to a specific channel. He however clarified that the EC is agnostic with regard to which authentication method is used and that redirection is mentioned in the RTS only as a possible obstacle. The burden of proof is with the ASPSPs to provide something that would work for TPPs and end-users. It would however be unacceptable that the user journey of an existing TPP business model would be unduly impacted in a negative way. He also highlighted that "widely used" is not the only criteria. There might be other obstacles. He finally suggested that the API EG should come up with recommendations on how to make the proposed authentication methods as secure as possible.

Topic 2: AIS data

This topic is still a work in progress.

From the ASPSP side it was commented that the terms of reference of the API EG limit the scope of the work to "all services and data which are to be made accessible for online payment accounts as per PSD2". As a result, the data made available via APIs should focus on PSD2 related data. The account information service providers (AISPs) on the other hand expressed the need to extend the scope to other types of account data. If the scope is however limited and at some point in the future the NCAs would decide that screen scraping is no longer allowed, then this would mean that there is no longer a business case for AISPs.

The EBA representative reiterated that in the context of API evaluation, the NCAs can only assess against PSD2 scope data.

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 had provided a report to the API EG. His proposal was to build an API in such a way that every time there is an update it would be 'pushed' automatically to the AISPs.

The EBA representative commented that the RTS text clearly states that access to payment account information by AISPs is limited to four times in 24 hours if the customer is not in session. She also added that the PSPs could have contractual arrangements agreeing to higher frequency or push data. J. Burkovic disagreed with the legal requirement as discriminatory and suggested that the aim of the API EG should be to build a 'good' API.

The EC representative commented that the law cannot be changed at this point in time and that this topic could be discussed as part of the review of the RTS. He moreover clarified that discrimination would only exist in case an ASPSP would have a push service of its own.

A possible suggestion could be to recommend that the API standard initiatives would allow for flexibility in relation to the number of times AISPs can access payment account information, with the caveat that this could only take place if there was an agreement between all participants.

It was suggested to further explore what 'four times a day' looks like from an implementation point of view and to check with the API standard initiatives in order to better understand how they are facilitating this feature.

The API EG co-chairs agreed to provide further assistance to finalise this document in support of J. Burkovic.

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

Previously G. Boudewijn had shared a document (from the Dutch banking community) on this topic which was meant as constructive input to the debate. The API EG is now awaiting further guidance on this document from the EC representative.

Topic 5: Who applies SCA?

This is still a work in progress, but the dedicated team is close to presenting a consensus document.

Topic 6: The "what" question

The co-chairs had presented a document as input to the previous meeting which 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 document was not discussed due to time limitations and would still need to be reformatted in line with the hot topic template.

Topic 7: Security

There is a need to better understand the scope the dedicated team should focus on (e.g. security of technical solutions; security of the PSU?).

J. Whittle suggested to initially start with focusing on guidance for the exchange between the TPP and ASPSP in a PIS scenario (from a PSD2 point of view). He added that it should however be avoided to be too prescriptive. The idea is to first have a better understanding of how security in this context should look like without narrowing market choices and then to subsequently start the engagement with the API standard initiatives.

In addition, T. Sabri informed that he is working on a document which addresses the application of Anti-Money Laundering (AML) legislation to PISPs and AISPs.

The EC representative informed that both PISPs and AISPs are 'captured' by the AML Directive. The idea was that the Directive would be obligatory for PISPs as it decreases the risk of using 'false' merchants. Following a consensual read it did appear as if this Directive should not apply to AISPs. So far, only one Member State had requested further clarification on this topic. If more Member States raise issues then the EC will of course need to address this.

6. Review of the API standard requirements (API EG 023-18; input documents)

Further comments had been provided on the latest version of the list of clustered API standard requirements, in particular from the ECSAs and EPIF. The API EG agreed that the members that had provided these comments should set up a call to try to reconcile the comments.

In relation to one of the listed API standard requirements, the EBA representative asked whether there would be a need for two separate certificates (one for PIS and another one for AIS) or whether one certificate for both would suffice. The dedicated team that is working on security was invited to look at this topic. In addition, it was mentioned that the work of the 'identification' expert subgroup of the ERPB WG on PIS may also be relevant to consider.

7. Status update on the technical expert evaluation subgroups

The technical expert subgroups had provided a status update on their activities and in particular on the outcome of their engagement with the API initiatives in relation to the initial list of eight API standard requirements.

Several subgroups however expressed a need for further clarification (including a rationale) and some requirements were also being questioned by a number of API standard initiatives from a legal point of view even though the API EG itself had reached a consensus on these topics. The API EG was also concerned about the fact that there seemed to be different levels of responses.

The API EG hence discussed that the best way forward would be to support the API standard initiatives to get to where an ASPSP implementing their standard would significantly improve the certainty of obtaining an exemption from providing a fallback solution.

The API EG agreed that in order to make the engagement with the API standard initiatives more effective, the requirements should be rephrased into 'SMART' (yes/no) questions in line with a harmonised view of what a good API should look like. This way the initiatives will not need to assess whether they are compliant, they will only need to provide a factual response (i.e. yes/no and clarify why yes/no). In case API initiatives would not support certain features then the list of questions will provide an early warning system to identify potential issues.

The EC representative however noted that time is of the essence. He suggested reiterating to the API standard initiatives that the aim of this exercise is to increase the chances of ASPSPs of obtaining an exemption. He added that it would be helpful if the focus would be on identifying real showstoppers. If the API EG would have a list of concrete showstoppers, then the EC could for example help by illustrating the issues to the relevant stakeholders.

The team that is working to resolve the comments on the API standard requirements document (see section 6) was invited to focus on priorities and to start with the rephrasing of the requirements into SMART questions.

In addition, the co-chairs mentioned that they could formally ask the initiatives what clarifications they need.

8. AOB

No further topics were discussed.

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

The next meeting was scheduled for 14 May 2018 at the EPC offices in Brussels.

10. Closure of the meeting

The co-chairs closed the meeting around 17h00 CEST and thanked the participants for the constructive meeting.

Annex I: List of attendees

Category	Name	Institution	Attendance
Co-Chairs	James Whittle	NPSO Ltd	Yes
	Oscar Berglund	Trustly Group AB	Yes
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 (AM)
	Krzysztof Zurek	European Commission	Yes
	Regina Weber	European Commission	Yes
	Nilixa Devlukia	EBA	Yes
	Helene Oger-Zaher	EBA	Yes
	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 of the 7th meeting of the AP IEG

Item	Action	Owner	Status / Deadline
7-01	Redraw the diagrams related to hot topic 'authentication methods' in a more generic way and provide to API EG co-chairs + EPC secretariat	R. Ohlhausen	25 April 2018
7-02	Provide the updated hot topic template on authentication methods to the API EG in order to identify potential showstoppers	EPC secretariat	26 April 2018
7-03	Provide eIDAS related questions to the API EG	N. Devlukia	26 April 2018
7-04	Publication on the EPC website of the approved minutes of the 5th and 6th meeting of the API EG (and approved agenda of the 7th meeting)	EPC secretariat	27 April 2018
7-05	Review the updated hot topic template on authentication methods to identify potential showstoppers	API EG members	3 May 2018
7-06	Finalise hot topic template	Dedicated taskforces	7 May 2018
7-07	Reconciliation of the comments in relation to the list of API standard requirements + prioritisation of topics + inclusion of SMART questions	M. van Berkel A. Mac Dowell E. Johansson G. Boudewijn K. Korus O. Berglund	11 May 2018
7-08	Provide support on hot topic 'Access to payment account information by AISPS'	J. Whittle O. Berglund	In due course
7-09	Provide guidance on the document developed by the Dutch banking community in relation to the hot topic 'Consent in scope of PSD2 in the context of the GDPR'	R. Jacob	14 May 2018

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) - EPC, Brussels**
May	**14 May 2018 (10.30-18.00 CEST)[2] - EPC, Brussels**
June	**8 June 2018 (10.30-17.00 CEST) - EPC, Brussels** **25 June 2018 (10:30-17:00 CEST) – TBC**

[2] The meeting time was later changed to 10.30-18.00 CEST.