payments
strategy
forum

Horizon Scanning Working Group

Working Group Solution Description:

API Governance

Working Group Objective:
'informing the forum of relevant market, technological and regulatory developments'

Document History & Control

Version Control

Name	Role	Version	Update Reason	Date
Team		v0.1		Unknown
Team		v0.2		2nd April 2016
Team		v1.0	First Publishing	7th April 2016
Sailesh Panchal		v1.0	New Template Design	23trd May 2016
Team		V8	Full review	27th May 2016
Ian Ellis, Sailesh Panchal		V10	Updated comments	30th May 2016
Otto Benz		V11	Consolidated comments	31st May 2016
Sailesh Panchal/ Otto Benz		V12	Consolidated comments	2nd June 2016
Chris Higham		V13	Applied further comments	1st July 2016
Chris Higham		V14	Further comments	6th July 2016

Contributors

Name	Title	Organisation
Otto Benz	HSWG Chair	Virgin Money
Faith Reynolds	HSWG Member	Independent
Sailesh Panchal	HSWG Member	Lloyds Banking Group
Esme Harwood	HSWG Member	Barclaycard
Carlos Sanchez	HSWG Member	Orwell Group
Michael Maier	HSWG Deputy Chair	COO, Fidor Bank
Tim Yudin	HSWG Member	Payments UK
Tim Piggot	HSWG Member	Nationwide Building Society
Sulabh Agarwal	HSWG Member	Accenture
Chris Higham	HSWG Member	Virgin Money

Bibliography

Title	Author	Date Published

Executive Summary

The transformative potential of Application Programming Interfaces (APIs) is recognised in a range of sectors. Close to home, the Open Banking Working Group (OBWG) which reported to HM Treasury in December 2015 set out how an open API standard could be developed in UK banking. Its objectives were to give customers more control of their data and herald a new era of innovation and competition. The report included a proposal for a governance framework to support the evolution of open data and APIs over time, and authentication and security protocols that are critical to engendering customer confidence. The Competition and Markets Authority's provisional remedies for retail banking in May 2016 endorses this work and goes on to propose the mandatory formation of an "Implementation Entity" which would need to put forward plans for the approach for adoption and maintenance of open standards for banking APIs.

In this paper we set out the case for tying together the proposals for API governance relating to the OBWG and the CMA with the requirements laid out in the second EU Payment Services Directive (PSD2) which gives customers new rights to use payment initiation and aggregation services. With customer permission, payment account data and payments functionality will be opened up to the third parties (TPPs) who will provide these services, though the mechanism is yet to be determined. We propose that using APIs to meet the requirements of PSD2 will result in the greatest benefit to all parties – account providers, third party users of those services, as well as ultimately, customers.

In this paper, we also set out proposals to introduce API governance and hence API implementation standards into the collaborative payments infrastructure to address a number of detriments identified by the End User Needs (EUN) Group. While PSD2 and Open Banking Initiatives make reference to payments functionality, their focus is in the PSP to customer space. We recommend payments APIs be developed for use in the PSP to PSP and PSP to market infrastructure space. The payments API capability outlined in this paper would enable new propositions such as Request To Pay, Confirmation of Payee, Payments Assurance Data, and richer or enhanced data. These are initial use cases frameworks, which support the needs of different customer groups, but the underpinning capability is intended to support other use cases frameworks over time. As such, the ongoing governance framework for APIs is of vital importance.

Recommendations:

1. There should be a single harmonised payments and banking **API Governance framework** and common set of standards (API Governance) for the UK to support the PSD2, Open Banking and Payments Strategy Forum EUN API initiatives. This should encompass the payments API capability described in this paper and the development of open banking standards in the UK (which may be pursued by HM Treasury and the CMA), and so ensure alignment between them. This will reduce risk and cost for all parties, and ensure that areas such as customer consent and security, which are critical to a successful open API landscape, are addressed in a consistent way.
2. The API Governance framework should define the Open API standards and data specifications and operational measures and controls covering all of: *customer to PSP* to fulfil requirements under PSD2, *commercial entities to PSP* to meet the aims of the CMA and Open Banking Working Group and *PSP to PSP APIs* to fulfil the use cases for End Use Needs capabilities set out by the PSF. The framework should be designed in such a

way to allow for APIs' **evolution over time** and creation of additional use cases models.

3. The **Implementation Entity**, in line with CMA report should be created and funded to set up the overarching Governance Framework in first instance and to define the initial set of standards required, manage and monitor their use, and further support their evolution to support innovation and address customer issues. The implementation entity **must include end user representation** in addition to the expected PSP/FI population.
4. The Implementation Entity will be expected to **supervise the technical creation and operation** of the Open API Standards, created with industry participants, balancing the co-operative/ and competitive elements arising whilst meeting the objectives set by the PSD2, Open Banking and End User Needs initiatives.
5. The Implementation Entity will **set the timeline** for API standards adoption and registration of participants to meet the necessary levels of ubiquity and critical mass for effective operation of the eco-system to meet the desired objectives.
6. While it will be the role of the Implementation Entity to ensure stakeholders (including FCA and Treasury) are properly managed and to ensure APIs are suitable for supporting the propositions required by PSD2 and the CMA, we suggest that in light of its co-competition powers with the CMA and the applicability of APIs to the payments domain, that the **Payments Systems Regulator should play an active role in supervising the Implementation Entity**, alongside CMA. With its expertise and competition powers, the Payment Systems Regulator should bring a payments regulatory 'lens' to these initiatives, including working with other regulatory and political stakeholders as appropriate.
7. A key aim of the API governance framework should be to **avoid fragmentation** of API definitions between institutions and standards in order to reduce effort for PSPs wishing to make use of API access into accounts

Solution name: API Governance

Document Purpose:

This document sets out the objectives, scope and recommended solutions for creating an API Governance Framework. The API Governance framework will cover the work of the OBWG, the requirements of the CMA, and PSD2. In addition, it will seek to address a number of detriments identified as a part of the PSF EUN Working Group assessment and to set out a model that enables extension to future requirements.

This document intends to define the key API governance principles and objectives for the UK industry, and it is expected that more detailed work will be undertaken to define the API Governance Framework following the public consultation starting in July 2016.

Background:

There are multiple regulatory and industry initiatives in the financial services industry to solve for customer problems associated with access to information in bank accounts and to allow easier access for companies to provide value-add services on behalf of customers, including the ability to make payments. Some of these propose or mandate the use of APIs, and others would benefit from a collaborative approach to using APIs.

- The Open Banking Working Group (OBWG), which reported to HM Treasury in December 2015, set out how an open API standard could be developed in UK banking. Its objectives were to give customers more control of their data and herald a new era of innovation and competition. The report included a proposal for a governance framework to support the evolution of open data and APIs over time, and authentication and security protocols that are critical to engendering customer confidence.

- The Competition and Markets Authority's provisional remedies for retail banking in May 2016 endorses the work of the OBWG and goes on to propose the mandatory formation of an "Implementation Entity" which would need to put forward plans for the approach for adoption and maintenance of open standards for banking APIs.

- The second EU Payment Services Directive (PSD2) gives customers new rights to use payment initiation and aggregation services. With customer permission, payment account data and payments functionality will be opened up to the third parties who will provide these services, though the mechanism is yet to be determined.

- The use of a framework of Open APIs would also address a number of detriments identified as a part of the EUN Working Group assessment, specifically Request To Pay, Confirmation of Payee, Payments Assurance Data, richer or enhanced data. A framework of APIs would be also be useful to develop a model that enables extension to future requirements.

We propose that using APIs to meet the requirements of PSD2 will result in the greatest benefit to all parties – account providers, third party users of those services, as well as ultimately, customers. We therefore recommend the creation of a governance framework that goes across these initiatives so that the industry can maximise the potential solutions from the API technology.

Key Timelines:

The HSWG, in defining the API Governance Framework solution, is operating to a two-year horizon from completion of the PSF overall strategy. The expected timeline would include the assessment of solution proposals, outline solution design, requirements gathering, development, testing and implementation. This timeline would be subject to refinement of requirements definition and a thorough sizing appraisal as part of the group's discussion and agreement process, and details of the solution will evolve as solution definition progresses.

It is expected that the delivery of the API Governance would be developed by industry, and overseen by a yet to be appointed governance vehicle (the "Implementation Entity" referenced by the CMA).

The initial Open API standards will be defined and ratified by the Implementation Entity and provided to PSPs and other relevant industry participants incrementally over the next 12 months, understanding the industries deadline for implementation being aligned with the mandates expressed by the CMA and under compliance with PSD2, by January 2018.

Scope:

The scope of the API Governance Framework should cover the following aspects:

- The scope of the industry initiatives - OBWG, PSD2, CMA
- Payments Strategy Forum EUN working group requirements for an enhanced data framework and capability (Request to Pay, Customer assurance for misdirected payments and Richer/ enhanced payments data)
- Payments Strategy Forum Financial Crime working group requirements for an enhanced data framework and capability (Richer/ enhanced payments data for financial crime detection)
- Payments Strategy Forum HSWG requirements to move UK to modern payments messaging standards

Strategic Objectives:

The expected outcomes from the introduction of an API Governance Framework that covers aspects of the OBWG, CMA requirements and PSD2 include:

- A more open and competitive market place as PSPs will have to complete on customer services and consumers will have a consistent level of transparency of products and more choice of experience as to how to access financial services.
- Payments innovation will accelerate as niche vendors, TPPs and PSPs will be able to leverage APIs to create new competitive aggregation service not currently available beyond a single PSP.
- Technology providers will be able to innovate to the provision of services to PSPs, increasing the innovations levels of PSPs.
- A lower cost overall for the industry (for both account providers as well as TPPs) by serving multiple access needs under one common, secure API framework, rather than multiple conflicting approaches.

- Elimination or reduction of fragmentation risk inherent in API introduction

Problem Statement:

A number of factors pose a significant risk to achieving the aims of EU Payments Services Directive 2, the CMA recommendations and to resolving the market detriments identified by the PSF:

- The lack of a single governance framework for standards setting necessary to achieve the goals of the regulator, detriments to the user community and the interoperability between the parties
- The lack of implementation entity to create scope, roles, responsibilities and rules for management and monitoring of the parties required to cooperate to make the eco-system of banking and payments APIs for consumption and production to limit delivery risks and market uncertainty.
- The short timescales required for the creation of common open standards across multiple stakeholder groups to still allow for implementation, continued evolution, without disruption and educating consumers, nor operating at the pace of the slowest participants or diluting the value proposition.
- The necessary technical open standards of web APIs for banking and payments industry have yet to be consistently defined and JSON and ISO 20022 data types as well as the communication models need to be developed to ensure interoperability with existing/new schemes, security of access and describe consumer products, to remove the risk of market fragmentation

Vision Statement:

A Governance Framework needs to be defined covering the API standards, data specifications and operational measures and controls covering all of: *customer to PSP* to fulfil requirements under PSD2, *commercial entities to PSP* to meet the aims of the CMA and Open Banking Working Group and *new PSP to PSP APIs* to fulfil new use cases for end user capabilities set out by the PSF. The framework should be designed in such a way to allow for APIs' evolution over time and creation of additional use cases models.

An Implementation Entity should be created and funded to set up the overarching Governance Framework in first instance and to define the initial set of standards required. It will be the role of the Implementation Entity to ensure stakeholders (including FCA and Treasury) are properly managed and to ensure APIs are suitable for supporting the propositions required by PSD2 and the CMA

In light of its co-competition powers with the CMA and the applicability of APIs to the payments domain, we suggest that the Payments Systems Regulator should play an active role in supervising the Implementation Entity, alongside CMA. With its expertise and competition powers, the Payment Systems Regulator should bring a payments 'lens' to these initiatives, including working with other regulatory and political stakeholders to ensure the API standards as applicable to payment use cases.

It would be expected that the technical implementation of the open standards would be created by industry participants in a distributed and competitive manner.

Solution Development Principles:

The Governance Framework will facilitate the creation and management a single banking and payments API framework of Open API standards and associated data, which itself will meet the following objectives:

- Create **accountable entity** for a) governance, responsible for creating and maintaining the API specifications b) overseeing the implementation of the specification and monitoring of participants
- **Ensure the standards are open**, available and can be implemented consistently, by providers of facilities to support PSD2, the requirements of the CMA, Open Banking and the Payments Strategy Forum Report (including the recommendations to support new end user needs requirements and those measures to combat financial crime) to allow use by PSPs or third parties on their behalf.
- Establish the necessary technical standards **in time to meet the regulatory objectives** and those of the PSF Strategy Forum and align with other industry initiatives.
- Ensure the standards established are a**ligned, where possible, with international and industry standards**
- Ensure that the standards can be used by all participants to **facilitate safe, secure and reliable communication**
- **Establish the rules and necessary legal constructs** necessary to support the APIs and the roles and responsibilities of the parties which will use or implement the standards
- **Manage the development and innovations of the standards** so that change impact is minimised and the standards can continue to evolve for future innovation with minimal disruption.
- Enable parties to register as a provider or consumer and efficiently communicate valid parties to **facilitate rapid on-boarding**, independent implementation, innovation and safety and security of the resulting network, and ensure that parties joining or leaving the eco-system do not impact the other members. The registration, certification and testing services as well its control management could itself be implemented to a specification by a technical provider.
- Create the entity **aligned with CMA recommendations** for funding its activities - operating on a not-for-profit basis encouraging participant implementations of the standards.
- **Oversee a base reference open implementation(s) of the standards** which will maximise participation for all sizes of parties and enable innovation and competition
- Maintain **a public release schedule** of the specification features and detail so participants and provide input, like the Open Source community model
- The following implementation sequence of the standards and reference implementations is suggested:
  - Participant registration and security
  - Data and resource identification standards based on the agreed schedule of delivery. That is: Open Banking MVP, Midata, Confirmation of Payee … PSD2,

Open Banking Closed Data, EU GDPR, Request 2 Pay, Assurance Data, Richer Data, Open Banking Aggregated/Anonymised data

- Access API enabling access to Simplified Payments Platform

Some further considerations for API Governance include:

1. Embrace and extend the work of existing initiatives like PSD2 (APIs between third party payment service provider (TPP) and AS Payment Service Provider (PSP)), and Open Banking (APIs between OB-TP and PSP) and the bodies that will oversee their work.
2. Operating framework and processes to implement new use cases and APIs beyond those identified under PSD2/Open Banking. Such us EUN APIs (e.g. Commercial to PSP such as a request to pay under utility providers), Person 2 Person/SME (e.g. confirmation of payee), Payments Assurance (Assurance Data) and Commercial 2 PSP/Government (e.g. payroll, payment purpose code – universal credit verification). Therefore the framework and the operating model should include:
   a. **API management:** Web APIs consist of data and actions on that data, so the data (resource) identification and specification is needs to be managed to allow for evolution without forcing all existing producers and consumers to update.
   b. **Transparency:** Open APIs and their usage will foster an open and innovative market allowing different consumers and providers use and develop different solutions as per their needs. This API governance initiative will be a central repository where end users will be able to contribute by defining standard procedures and information pages.
   c. **Fraud liability**: With the introduction of APIs to allow initiating payments via request to pay (RTP) transactions, fraud becomes a key aspect. This will require the Governance and Implementation entities to be aware of the Overlay services that are possible with API, with the related liability models which would be bought into scope and require additional regulatory oversight, based on industry requirements.
   d. **Security:** Openness via APIs within PSP to PSP, TPP to PSP and Commercial to PSP communication requires significant work in maintaining security. Proper security measures and protocol should be defined. At least, a minimum set of standard should be in place to allow a producers and consumers of APIs of safely engage and technical vendors to provide innovative solution as this is a rapidly evolving technology space.
   e. **Reconciliation:** Given the number of various participants in the ecosystem the standards and the framework need to address mechanisms for reconciliation and find a process to handle reconciliation errors, via APIs as the resulting PSP to PSP clearing systems may not contain the necessary data, for example in the case of matching a Request to Pay, with the received payment.

Available Solution Options:

The following high level solution approaches to API governance have been considered for framing a suitable governance model, we considered three possible models:

1. **Open Source approach:** An open approach to API management for the industry based on the '*Git Hub model*' which where all members/participants have full access to

systems and governance, by means of a charter agreed by participants. An open source approach could be seen to foster collaborative behaviour between suppliers and providers and foster rapid innovation of different parties. However the shortcoming is that an open source approach does imply self- governance and management of the content, preventing revenue generation.

2. **Proprietary approach:** A closed and restricted payment implementation like 'Faster Payments' where both the scheme and its governance is tightly controlled. This model allows a full control of the contents across industry and avoids unwanted governance that are to be dealt with in the open source approach. This model may also give an opportunity of generating revenue for the authority from the producers and consumers of the specification and implementation.
3. **Hybrid approach:** A hybrid approach operating under central guidelines but having sufficient flexibility for participants and members to contribute, collaborate and jointly innovate. Health Level Seven International (HL7), is a not-for-profit, ANSI-accredited standards developing organisation dedicated to providing a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information is a good example of this approach. This approach benefits from the good aspects of both Open Source and Proprietary models.

People Involvement and Action:

The following bodies are likely to have a role in the implementation of the PSD2 and Open Banking APIs, which will require further collaboration with existing schemes, processors, banks and regulators. Alignment on governance, creation and maintenance of processes and standards is key to adoption and innovation.

WHO	**WHAT**
HMT	• Provide guidance on Open Banking direction
CMA	• Oversee elements of API definition relevant to banking competition • Oversee set-up of Implementation Entity • Approve funding arrangements of Implementation Entity • Approve Plan of Implementation Entity
FCA	• Provide guidance on PSD2-related regulation compliance, including governance, registry of TPP/API providers, Testing/Sandbox
PSR	• Provide guidance on payments-related competition matters
PSPs	• Implementation of APIs
Payment Processors	• Implementation of Access APIs
PSPs, Payment Aggregators	• Implementation of Access APIs, Overlay APIs and custom APIs
Implementation Entity / body	• Co-ordination, definition, tendering and oversight
End user representation	• Ensure the needs of end users are represented and the required overlays are delivered with the correct functionality

Leadership:

Leadership for the API Governance Framework solution will be created in the Implementation Entity, which will create the mechanisms to set up the governance framework itself. It is expected that the Implementation Entity will be constituted from industry, and will have to liaise with multiple regulatory as well as political stakeholders to ensure that the scope of its work meets its multiple requirements.

Systems and Processes:

Key systems and processes required will include:

- Governance standards to manage the development of the API specification in combination with PSD2, Open Banking, W3C, CMA etc.
- Standardised processes and procedures for TPP registration including on boarding and certification criteria.
- Standardised approval and testing criteria for TPP developed solutions
- Enhanced data standards under ISO2022

Dependencies:

Key dependencies will include

- EBA : Co-ordination and Alignment with EBA working team and timelines for publishing RTS
- OBWG : Co-ordination and Alignment with the OBWG Steering Com
- CMA : Coordinate with the " Implementation Authorities " of the seven banks identified in the recent CMA report on "Retail banking market investigation"

Existing or In-development Solutions:

- PSD2 and Open Banking are the key industry and regulatory initiatives within UK which are already considering similar API based models. The Open Banking Standard document lays out supported view and guidance.
- Additionally the governance approaches taken by the following international industry initiatives will need to be further investigated into
    - GSMA API Exchange : The API Exchange enables operators to federate between their individual APIs to deliver cross-operator reach
    - US FHIR (Fast Healthcare Interoperability Resources) : APIs for data interchange between registered healthcare organisations, hospitals and doctors

Collaborative or Competitive:

Collaboration within the industry, regulators, vendors and industry standards forum will be required to specify the APIs in the common Open, Overlay and Access APIs scope. By doing so it will clarify how these can be extended to enhance competitive innovation and framework that will enable more rapid development of Customer APIs.

Implementation Approach and Timeframe (overall):

An initial assessment of the high level approach to implement this will include:

1. Identify members and participants for the proposed body – Q3 2016

2. Setup the new governing and delivery body – Q4 2016
3. Issue standards and guidelines for data interoperability, security, liability, fraud, API specifications etc. - Q1 2017
4. Live Pilots with members or PSPs - Q3 2017
5. Live Service Q2 2018

Security dependencies on PSD2 not needed – PSP-PSP only, so dependent on data standards

Impact: Success Metrics;

The success of the solution can be measured through

- Adoption of APIs by TPPs, PSPs.
- Creation of new customer facing propositions and applications for end users using these APIs
- Reduction in cost and time for on-boarding new PSPs into existing infrastructure

Next Steps:

This recommendation should be progressed into the overall strategy document being produced by the forum.
In addition, further work should be undertaken to consider the value of the governance model in the face of European and global standards that are current under development and this should be reviewed as these standards evolve.

Appendix

Risks to successful implementation of an API Governance Framework can be identified in the following three areas:

1. Payments regulation and coverage issues
2. Governance and management proposals
3. Governance and management of technical standards

1. Payments regulation and coverage issues

- EUN and Financial Crime (FinCrime) working group recommendations are more customer and AML oriented therefore will not be directly covered by PSD2 or Open Banking
- PSD2 and Open Banking do not require the use of ISO 20022 data types directly
- Without ISO being used mapping to UK and EU payments will more complex
- Web Standard format JSON mapping to ISO needs to be defined for EUN/Simplified platform and followed by PSD2/Open Banking
- ISO data types do not cover the needs of EUN, extension or new ISO may be needed
- PSD2/Open Banking have specific scope, any by their nature do not need a flexible extensible framework to resolve detriments
- A framework will need to be developed to express the EUN messages in a way that can be incrementally extended to cover more use cases
- PSD2 - may not realise the significance of the payment token - in the end 2 end reconciliation, needed by the EUN
- PSD2 may not cover the mapping to UK scheme in any standard way
- PSD2 may not realise the impact to the current schemes. Certainly this has not been voiced outside the schemes, as Simon Brookes indicated today
- PSD2 TPP registry will need to be more flexible to use for EUN
- PSD2 and Open Banking do not have the need for Service Discovery, that is does a PSP support a particular service for EUN
- Open Banking is limited to large banks covering 90%, PSD2 covers 100% of PSPs, EUN % to be recommended
- Open Banking provides for exposed SLAs for Customer and Service metrics related to competition but not necessarily those for EUN and Service availability
- PSD2 security and authentication model is for TPP-PSP customer, it may not recover the Confirmation of Payee security model

2. Governance and management proposals

- Implementation Entity to co-ordinate with FCA, EBA on the definition of PSD2 security and standards
- Implementation Entity to co-ordinate with Open Banking Initiative and Open Banking Project on data standards
- Implementation Entity to define a suitable governance and decision making model
- Agree with FCA, EBA that Web API are a suitable technical implementation of PSD2 regulation for the UK.
- Recommend Terms of Reference (ToR) for standard body(ies) to create and manage PSD2, Open Banking and other standards required

- Detail and map detriments to APIs, identify additional models as required
- Establish ownership of Registries and Catalogues
- Identify governance relationships between PSD2, Open Banking, Payments UK, et al
- On-board and management, including FinCrime black-listing, of entities using APIs in the network
- Identify role-type of Consumers and Providers, i.e. PISP, AISP, ASPSP, Open Banking, Certificate authorities, etc.
- Governance of API data structures and alignment to ISO and W3C work

3. Governance and management of technical standards

- URI structure – for APIs invocation at a PSPs to be defined. For example: https://customer.mybank.com/party-service/v1/involved-party/{party id}
- PSD2 security standards for Web APIs to be defined.
- API Data structures to be used, assuming XML ISO 20022 structure – is not suitable for the Web API, but that ISO data types will be used.
- Further extend the work of the Open Banking Standard
- Data format JSON-LD or JSON, and specification Swagger or RAML1.0 for the specification of APIs
- Additional capability required to specify APIs service description, i.e. security, SLAs, meta-data
- Data Types for APIs (PSD2, Open Banking, et al) definition and usage
- Recommend models that enables integration with mobile platforms
- Identify Cards use cases that can be converted to API models, aligned with PSD2
- Verify Mutual authentication technology, PKI/HTTPS and calling conventions
- Technology for the customer authorisation and consent, assumed oAuth2