January 2018

Consultation Paper on Open API Framework for the Hong Kong Banking Sector

HONG KONG MONETARY AUTHORITY
香港金融管理局

Table of Contents

ABOUT THIS CONSULTATION PAPER

1 This consultation paper is published by the Hong Kong Monetary Authority (HKMA). It sets out the HKMA's intended approach to Open API for the banking industry in Hong Kong.

2 The HKMA is conducting this as an industry consultation. The banking industry and the information and communications technologies (ICT) industry are welcome to provide comments on all parts of the consultation paper. Any person submitting comments on behalf of an organisation is requested to provide details of the organisation they represent.

3 Comments should be submitted in writing no later than 15 March 2018, by any one of the following means:-

By email to: apiconsultation@hkma.gov.hk

By mail to: Fintech Facilitation Office
Hong Kong Monetary Authority
55/F, Two International Finance Centre
8 Finance Street
Central
Hong Kong

I. INTRODUCTION

Background

1 As part of the seven initiatives of the New Era of Smart Banking, the HKMA is formulating a framework for facilitating the development of Open Application Programming Interfaces (API) for the banking industry. Open API, in this context, can serve many purposes. For example, they may allow users of online discussion forums and social media platforms to obtain information about products and services of banks for comparison and analysis. Many lifestyle websites and apps may make use of Open API to integrate banks' foreign exchange and payment services to offer end-to-end holiday or health care packages. A bank customer may benefit from Open API by using third party applications to consolidate for analysis purposes his/her cash flow and investments kept in several bank accounts.

2 However, the key benefits of Open API can be reaped only if it is widely adopted in the banking sector. This is precisely the reason why some jurisdictions are taking steps to encourage or, in the case of the EU including the UK, even mandate through legislation financial institutions to adopt Open API. In Hong Kong, the HKMA aims to facilitate the banking industry in adopting Open API effectively, securely and without any delay by providing the necessary leadership and guidance given the fast development of Open API in many developed markets. An Open API framework is the first and a key step to guide and enable the banking sector to implement Open API in order to stay competitive.

Policy Objectives

3 In light of the rapid development of fintech and the increasing demands from customers on innovative and convenient banking services, Open API can help to

3.1 ensure the competitiveness of the banking sector;

3.2 encourage more parties to provide innovative/integrated services that improve customer experience; and

3.3 keep up with worldwide development on delivery of banking services.

II. OPEN API

4 According to the Euro Banking Association[1], API can be seen as the interfaces between software applications, both within and between organisations. API enable communication between software applications where one application calls upon the functionality of another application.

5 API enable secure, controlled and cost-effective access to data and/or functionality of systems. Open API, in the context of this paper, refers to API that allow third party access of systems belonging to an organisation. However, Open API for the banking industry does not necessarily mean that any third party can freely access a bank's system without restriction. Banks should impose controls in order to preserve security, privacy and contractual assurance.

III. FRAMEWORK DEVELOPMENT

Industry Engagement

6 In July 2017, 20 retail banks and three foreign banks were asked to nominate Open API contacts in order to work with the HKMA on formulating a framework.

7 All Open API contacts were invited to a workshop held on 15 August 2017 to hear experts from technology firms that have successfully implemented Open API on their development

[1] "Understanding the business relevance of Open APIs and Open Banking for banks" May 2016

journeys, how Open API has changed their ecosystem and the lessons learnt.

8 Throughout September and October 2017, all Open API contacts were invited to discussions with the HKMA to explore their readiness, views and plan on Open API.

Industry's Readiness

9 The technology and business readiness of banks for deploying API in Hong Kong was found to vary widely from "already launched Open API" to "without any concrete plan". Among the banks met, only one launched Open API for external parties to use, three deployed API for internal use, nine planned road map for implementation or were working on API developments, and ten were without a concrete plan.

Industry's Views

Benefits

10 None of the banks expressed doubt on the benefits of Open API as helping them to maintain competitiveness, being an opportunity to acquire new business or reaching out to untapped markets, offering customer-friendly services and speeding up internal system development time.

11 Regardless whether or not an Open API plan had been formulated in their respective banks, Open API contacts acknowledged the strategic importance and the need for deploying Open API in their banks in the near future.

Standardisation

12 The vast majority of banks (21 out of 23) supported the need for standardisation on the functions and data definitions of Open API among banks. They were of the view that the maximum benefits of Open API could be obtained if, ideally, all banks offered

exactly the same set of Open API functions so that third party service providers (TSP) only need to develop their software once, and then it could be used to connect to all banks without the need for further customisation.

Open API Categorisation

13 All banks agreed the importance of categorising the types of Open API in order to assess the implications, opportunities, risks and priority of selecting and implementing them.

14 It was agreed that, in terms of increasing priority and risks, Open API may be categorised as:

14.1 product and service information – "read-only" information offered by banks on details of their products and services;

14.2 new applications for product/service – customer acquisition process such as allowing online submission/application of credit cards, loans or certain insurance products;

14.3 account information – retrieval and alteration (where applicable) of account information (balance, transaction history, limits, payment schedules, etc.) of authenticated customers for stand-alone or aggregated views; and

14.4 transactions – payment or scheduled payments/transfer by authenticated customers.

15 It was further agreed that the types of protection needed for each of the four categories of Open API should be:

Categories of Open API	*Protections required*
Product and service information	Authentication of bank sites and integrity of data

Categories of Open API	*Protections required*
New applications for product/service	Authentication of bank sites, integrity and confidentiality of data, and authentication of TSP
Account information	Authentication of bank sites, integrity and confidentiality of data, authentication of TSP and authorisation of customers
Transactions	Authentication of bank sites, integrity and confidentiality of data, authentication of TSP and authorisation of customers

16 It was also agreed that further categorisation of Open API by product types should be devised in the process in order to better understand and prioritise their developments.

Implementation

17 In terms of implementation, banks expressed the need to exercise caution because of the potential risks of cybersecurity, data privacy, customer protection, and liability when allowing TSP to access bank systems and data. Furthermore, some banks also expressed concerns about the potentially large investment in building an Open API infrastructure as to whether there would be clear business and/or use cases to justify the investment. In total, seven out of the 23 banks expressed concerns about the challenges of implementation, the possible considerable investment involved and the yet-to-be-proven business cases to support the investment.

18 All banks specifically suggested that a progressive and phased approach, where each phase would be built on the success and lessons learnt from the previous phase, would be a prudent approach to this new area of opening up systems and data.

19 More than half of the banks (15 out of 23) clearly expressed that the product/service information and/or those related to business

acquisition areas should be opened up first. Apart from the information is generally "read-only" and has less security concerns, the infrastructure required to support their adoption would also be less complex.

20 Furthermore, it was believed that this progressive approach could allow the industry to accumulate sufficient knowledge and the overall ecosystem to develop and mature. The risk of opening up customer data later could, therefore, be built on a solid foundation of previous experience. Finally, a phased approach would also allow the various imminent implementations of Open API in the European Union (EU) and the UK to settle and share their experience in the near future.

Use of Technical Standards

21 All banks agreed that international or industry technical standards should be referenced and used whenever possible. These could include areas such as architecture (how to connect between systems), security (authentication, integrity, confidentiality and authorisation protections), and data definition (how to interpret information accessed).

TSP Certification

22 As TSP may require to access bank data and present them to the general public (in the case of product and service information) or access bank systems to extract customer data or execute transactions, TSP certification in terms of due diligence, monitoring and contractual engagement should be seriously considered.

23 Among the 14 banks that expressed a clear view on TSP certification, 11 expressed the desire to see a central entity to take up the role of TSP certification so that TSP can "certify once, access to all banks". Banks believe that this could reduce the efforts of both banks and TSP during the onboarding process of TSP. However, banks also acknowledged that they are ultimately

responsible for the confidentiality and integrity of the data held, and therefore wished to retain control over which TSP they would be working with. Furthermore, banks believed that the resource investment in forming, running and agreeing on common practice in a central certification entity at the initial stage could not be justified without the support of a successful and growing Open API ecosystem.

Open API Ecosystem

24 All banks agreed that Open API is not a one-off exercise but would require an ecosystem to ensure that Open API is being developed, adopted, reviewed and maintained on an ongoing basis.

25 Banks expressed desire to see an environment that helps TSP to gather information and assistance on the implementation of Open API offered by banks. Furthermore, banks have also expressed desire to see a central entity that would coordinate and manage the life cycle of Open API, including further review of and selection on Open API as the needs and applications of Open API develop, as well as to review the various technical standards and practice in use in Open API.

Worldwide Developments

26 There have been some worldwide developments in Open API. Most noticeably are the UK, the EU, Singapore and Japan. Their relevant scopes and details are summarised below.

The UK

27 As a result of its retail banking market investigation in 2016, the Competition and Markets Authority (CMA) has mandated nine banks in the UK to enable personal customers and small businesses to share their data securely with other banks and with third parties, allowing them to compare products on the basis of their own requirements and to manage their accounts without

having to use their banks. This is called Open Banking in the UK.[2] This scope was expanded in November 2017 to cover other payment accounts such as credit cards, e-wallets and prepaid cards.[3]

28 In order to deliver this objective, an implementation entity was created to define and develop the required API, security and messaging standards that underpin Open Banking.

29 The Open Banking delivery is split between March 2017 and January 2018, with the former focusing on open data, making available information on ATMs, branches, personal current accounts, business current accounts (for SMEs) and SME unsecured lending and commercial credit cards. January 2018 is aligned to the upcoming European Union's payment services directive 2015/2366 (commonly known as PSD2), where authorised third parties can be given consent by the account holder to access their bank accounts to extract statement information and to initiate payments, without having to use the banks' online services.

30 Detailed standards on Open API functions, architecture, security and data were developed to an execution level so that there is a uniform implementation across all banks. The result is that when a TSP has developed a piece of software, a mobile app or a website for connecting to one bank, the same programme can be used to access all other banks conforming to the standards.

31 A certification model has been developed for TSP; TSP need to be 'whitelisted' by a central body before being allowed access to banks' Open API. In addition, they have to accept and conform to a number of standards, rules and guidelines.

32 Finally the implementation entity is also responsible for maintaining a website to host all Open API from all participating

[2] https://www.openbanking.org.uk/about-us/
[3] https://www.openbanking.org.uk/about-us/news/uks-open-banking-project-expanded/

banks, and be responsible for their review, update and maintenance.

33 In short, the Open API mandated in the UK is focused on a number of limited functions (product and service information, and account information) and execution details are standardised.

The EU

34 The EU's PSD2 aims to provide the legal foundation for the further development of a better integrated internal market for electronic payments within the EU.[4] Among many things, it seeks to require banks to grant third party providers access to a customer's online account/payment services in a regulated and secure way. Member States must enact national legislations by 13 January 2018 to implement PSD2.

35 PSD2 does not explicitly mention or require API but it is widely expected that API is the way to fulfil the requirements of the PSD2 for payment service providers. Currently the requirements are at high-level and there is no uniform implementation detail available.

Singapore

36 The Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore published the "Finance-as-a-Service: API Playbook" (Playbook) in November 2016. The Playbook identified 411 API covering banks, insurers, asset management companies and government agencies. The 411 API are also categorised into product, marketing, sales, serving, payments and regulatory in terms of functions. These scopes are a lot wider than those of the UK Open Banking.

37 The adoption of the API in Playbook by financial institutions is voluntary and there is no official timeline. As of 15 November

[4] https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

2017, 270 API have been made available by the Singapore financial industry as a whole.

38 Other than the 411 identified API, the Playbook specifies the architecture and security standard of all API and the data standard of some API. It does not, however, cover any TSP certification or API ecosystem development/maintenance.

Japan

39 The Japanese Banking Act was amended in May 2017. Banks in Japan are required to announce support on Open API by March 2018 and have it deployed by middle of 2020. TSP need to register officially, establish contracts with banks for using their Open API and publish their measures on how to secure and safeguard customer information. A detailed framework is to be published in relation to security issues, user protection and specifications regarding the provision of API.

40 The Japanese Bankers Association (JBA) published a report on Open API in July 2017 to provide guidelines, security and user protection principles for the implementation of Open API.[5] It is up to individual banks to decide whether to comply with the API development and electronic message specification standards in the report. For security and user protection measures, the report provides a basic approach addressing generic risks that are likely to be shared between various business models and services.

41 It is expected that banks and TSP would need to refine or agree on the actual function and control measure during implementation. The initial general scope of API identified for implementation covers deposit-related activities in account balance enquiries, account activity enquiries and interbank transfers.

[5] https://www.zenginkyo.or.jp/fileadmin/res/news/news290713_3.pdf

IV. PRINCIPLES

Scope

42 This Open API framework is initially applicable to retail banks in Hong Kong as it can directly affect the services offered to and the experience of the largest group of customers. Banks are naturally welcome to extend this to any other banking businesses.

Guiding Principles

43 The following is a set of high-level principles and assumptions that guides the development of the Open API framework.

44 To ensure speedy implementation and results to be seen by users and the industry quickly, a small list of frequently-used and granular Open API functions should be selected. The advantages of frequently-used and granular Open API are the high flexibility and low maintenance cost. These advantages allow banks to concentrate resources in updating and ensuring the robustness of a small number of Open API functions where complex operations can be built by combining the simple Open API functions.

45 Also, Open API functions should be selected on the basis of their potential benefits to banks and customers, and identified with priority.

46 Existing international or industry practice should be leveraged in order to ensure wide adoption and speedy development of Open API.

47 As the banking industry sees the need for banks to stay competitive and the demands of their customers for better services, banks are expected to adopt Open API once the policy framework and implementation timeline are finalised. The HKMA shall therefore monitor the implementation closely, and act accordingly to ensure market adoption and encourage use cases.

V. THE PROPOSED OPEN API FRAMEWORK

48 The proposed Open API framework comprises the following parts:

48.1 Selection of Open API functions and deployment time frame;

48.2 Open API technical standards on architecture, security and data;

48.3 TSP certification model;

48.4 Open API facilitation measures; and

48.5 Open API maintenance model.

49 The HKMA recognises that Open API involves management commitment on one end and hands-on experience of practical implementation on the other end. While management commitment needs to meet changing business priority and customer demands, practical implementation experience is also required to adapt as technology and best-practice continue to evolve. Flexibility is therefore of paramount importance in an Open API framework if it is to stay relevant.

50 A broad framework with high-level objectives is therefore proposed so that banks can exercise flexibility on the implementation details and decide on the schedule in light of the proposed time frame. This outcome-driven approach allows banks to build the Open API ecosystem as an industry effort while the HKMA may monitor the progress and further consider the need for regulatory intervention if necessary.

Selection of Open API functions

51 The selection of Open API functions is a key and the first step. The correct identification could lead to early adoption. At the same time, the industry's desire for a progressive and step-by-step approach to implement Open API starting from a less risky set of functions is recognised.

A phased approach

52 The increasing protection needed for each of the four categories of Open API functions is discussed earlier and recapped in the following table. Due to the increasing risk of more sensitive being allowed to be accessed, a phased approach starting from Product and service information is recommended.

Phase	*Categories of Open API*	*Protections required*
1	Product and service information	Authentication of bank sites and integrity of data
2	New applications for product/service	Authentication of bank sites, integrity and confidentiality of data, and authentication of TSP
3	Account information	Authentication of bank sites, integrity and confidentiality of data, authentication of TSP and authorisation of customers
4	Transactions	Authentication of bank sites, integrity and confidentiality of data, authentication of TSP and authorisation of customers

Timeline

53 It is envisaged that the deployment of Product and service information will be similar to an open data initiative which the

information technology industry is already familiar with. The timeline for the deployment should therefore be relatively short.

54 Transparency in details of products and services to customers is critical to the banking industry. Banks are therefore expected to adopt Open API in product and service information within six months after the release of this framework.

55 Subsequent phases of Open API that involve more security and authentication infrastructure, however, may require further development efforts by banks and therefore the timeline is likely to be longer. On the other hand, given each subsequent phase will be built on the experience gained from the previous one, the timeline is not expected to be disproportionately long.

56 For the second phase of New applications of services, banks are expected to have them deployed 12 months from the release of this framework in order to stay competitive and provide convenience to their customers.

57 For the third and fourth phases, Open API would allow even more innovative and convenient services, such as aggregation of account information across multiple banks, and completion of banking transactions in third party apps or web pages. As the complexity and risk of opening up data of all customers increase, the infrastructure to support, monitor and secure the Open API access becomes more complex and mission critical. It will be necessary to develop a set of governance measures such as due diligence, onboarding, control, monitoring, roles and responsibilities, consumer protection, data protection, security, resilience incident handling etc. Setting a timeline for the adoption of the third and fourth phases at this stage may therefore be premature. However, the HKMA will work with the banking and the ICT industries on these important issues, taking into account implementation experience of Open API for the Product and service information and similar experience overseas. The HKMA aims to release around Q4 2018 a more detailed timetable for implementing Open API for the two remaining phases.

58 **The Open API deployment timeline is proposed as followed:**

Phase	*Categories of Open API*	*Expected timeline from the release of the Open API framework*
1	**Product and service information**	**Six months**
2	**New applications for product/service**	**12 months**
3	**Account information**	**To be reviewed in Q4 2018**
4	**Transactions**	**To be reviewed in Q4 2018**

59 **Comments are sought on the proposed timelines and whether there are reasons that they could not be met.**

Selection of Open API

60 There are generally two approaches to overseas implementation of Open API on the selection of Open API functions – the detailed and standardised approach, and the industry-led approach.

61 The UK and Singapore are taking the detailed and standardised approach. The UK needs to adopt this model because there is a specific mandate to address – to allow personal customers and small businesses to compare products and switch between banks – and therefore a set of focused and standardised Open API could be specified. In Singapore, the industry was able to agree on and recommend a set of 411 standardised Open API functions for financial institutions which were published in the Playbook.

62 Owing to the CMA mandate, all nine banks concerned in the UK have complied with the requirement and implemented the relatively small number of standardised Open API. Under Singapore's voluntary model, banks have started to deploy Open API a year after the Playbook was published but they do not all

conform to the Playbook in terms of the Open API functions and data standard.

63 The EU and Japan take an industry-led approach and only high-level requirements have been set for the industry to implement. As their developments are relatively new with a timeline set in the future, the lessons to be learnt from the implementation conformance is not yet available.

64 Each jurisdiction's approach has been adopted with respect to its own circumstances. The HKMA recognises the industry's desire to see a set of detailed and standardised Open API to be agreed so a TSP application or website designed for one bank can interoperate with other banks. However, the policy objectives of Open API for the Hong Kong banking sector to maintain its competitiveness and to offer innovative/convenient service to improve customer experience are general in nature. Furthermore, a number of international banks operating in Hong Kong have already adopted their group standard for implementing Open API at global or regional levels, and have demonstrated elsewhere that requiring adherence to a specific local standard could be challenging.

65 Some opinions from the technology sector also indicate that, while standardisation is welcomed, there is also a desire to see banks deploy Open API as quickly as possible. Furthermore, it was also indicated that the programming efforts for connecting Open API to each individual bank is a relatively small part of an overall product development cycle so it would still be acceptable if full interoperability between banks is not a priority and can be achieved at a later stage. Based on these circumstances, prescribing Open API functions in detail at the start is unlikely to be the best-fit for Hong Kong. In order to drive the desired outcome for banks to deploy Open API quickly, a flexible, inclusive approach is needed.

66 It is therefore proposed that only high-level Open API functions are identified for banks to deploy, subject to their own business

offering and priority. However, if banks have already developed a road map, they are welcome to deploy similar functions particularly if it means they can meet the expected deployment timeline. It is believed that once an ecosystem is developed and matured, convergence to standardised Open API may occur due to the need of the market.

67 A set of high-level Open API functions is, therefore, proposed in Annex A as a starting point. The list has drawn reference from the functions specified by the UK Open Banking, the list of Open API functions proposed by MAS, the areas suggested by JBA and common functions found in Hong Kong's e-banking services. In order to introduce a conducive environment for banks to adopt these Open API functions, examples of information provided by each Open API function under the first category of Product and service information are also listed for banks to refer to.

68 Banks are expected to provide the HKMA with road maps of Open API adoption (one within two months for product and service information, and one within seven months for new applications after the release of the formal framework). Banks are also expected to explain how their road maps meet the general scope described under Annex A (and in the case of gaps, the reasons).

69 **Sets of high-level Open API functions for each of the four categories are recommended under Annex A. Banks are free to roll out similar functions that suit their business needs, particularly if this means they can meet the deployment timeline. Nevertheless, banks are expected to provide a road map and explain whether and how the general scope of Open API functions described under Annex A will be covered. Convergence of functions, if demanded by the market, is expected to take place as the ecosystem matures.**

70 **Comments are sought on this approach that allows banks flexibility on the scope of Open API while making sure that**

the industry generally moves in tandem to create an Open API ecosystem.

Architecture, Security and Data Standards

71 Standards in Open API allow software designers and programmers to adhere to a set of common practice without the need to spend extra time in learning and applying a different practice for each bank that offers Open API. As mentioned previously, standards relevant to Open API are architecture, security and data.

72 There appears to be a general consensus on architecture and security from the three jurisdictions (Japan, Singapore and the UK) that have published the relevant Open API standards. It is believed that such standards are a reflection of the industry norm or best practice, and therefore can be implemented practically. It is therefore recommended to follow similar standards as detailed under Annex B.

73 While certain technical standards have been prescribed, they cannot be considered as the only standards that cover all security requirements. More holistic controls on information and cybersecurity risk should always be considered on a risk- and principle-based approach to protect banks' systems as well as bank and consumer data.

74 On the other hand, there is no consensus on data standard. The only standard mentioned which is considered relevant to Open API for the Hong Kong banking sector is the open standard Open Financial eXchange (OFX) advocated in the Singapore Playbook. However, OFX only covers account-related information and there is no evidence that this is widely used for banking Open API.

75 A similar approach to Open API functions is therefore proposed, that OFX be used where it is applicable. However, banks may use other means to define the data they will provide to those who uses their Open API, so long as banks publish such definition (often

called "data dictionary") transparently using industry practice such as OpenAPI Specification (also known as Swagger). The HKMA particularly welcomes views on whether there are other options on setting the data standard.

76 **Sets of industry best-practice architecture and security standards are recommended under Annex B. Banks implementing Open API are recommended to follow them in order to provide uniform interfaces to TSP in these areas. For data standard, OFX is recommended under Annex B for relevant Open API such as those related to account information. However, banks are free to use their own data descriptions (provided that they publish the definitions transparently) that suit their business needs particularly if this means they can more readily meet the timeline. The HKMA particularly welcomes views on the approach suggested for the data standard.**

77 **Comments are sought on the approach and the technical standards recommended in order to reduce development efforts.**

TSP Certification

78 TSP certification covers a range of governance activities such as due diligence, onboarding, control, monitoring, roles and responsibilities, consumer protection, data protection, security, infrastructure resilience, incident handling etc. Three possible approaches may be considered:

78.1 Bilateral – Banks carry out their own risk assessment and due diligence on any bilateral engagement with TSP covering governance, controls and security issues according to the nature of the engagement, and established policies and procedures of the banks.

78.2 Central certification entity – A central body is funded and formed with agreement by all the banks involved to

develop a common set of risk-based and due diligence criteria for TSP so that TSP may be certified by the central entity once and be able to gain access to all banks.

78.3 Bilateral with common baseline – A set of risk-based and due diligence baseline criteria is developed and agreed by banks. While banks may add in their own unique requirements, the baseline approach streamlines the certification process for both banks and TSP.

79 Among the three approaches, the bilateral engagement may allow more flexibility for banks and involve fewer changes as some banks are already engaging their contractors in a similar way. It also allows banks to quickly engage, and have more options in dealing, with TSP.

80 The centralised approach, however, may facilitate better access by TSP because once approved, a TSP may access all banks that offer Open API. That said, working out a set of risk-based common standard on TSP governance among banks is a complex process and an uncharted territory, and is expected to take some time. Furthermore, banks have expressed concerns on investing resources in a central entity in the early stage prior to a mature ecosystem being established.

81 The bilateral with commonly agreed baseline criteria approach reduces the repetition of going through common processes when TSP seek certification from multiple banks. While banks agree on a set of risk-based baseline processes, banks can make reference to the baseline and are free to set and control their own additional assessment criteria. TSP, nevertheless, should be able to reuse parts of the documents prepared for one bank when applying to subsequent banks.

Options

82 Against this background and that the Open API ecosystem needs time to reach maturity and become sustainable, it is suggested

that a phased approach may be taken. Initially during the growth cycle of banks offering Open API and TSP entering the market, the flexible, risk-based bilateral approach is suggested to encourage agile and flexible engagement between banks and TSP. However, when the ecosystem has grown to a sustainable size, resources may be contributed by banks to form a central entity to manage TSP certification.

83 If there is sufficient support from the industry, the HKMA may explore to work with the industry, developing a set of risk- and principle-based common baseline criteria for banks to refer to. However, the expected timeline for deployment would not be changed as a result so banks are not expected to wait for the baseline criteria to be formed before onboarding TSP.

84 **The establishment of a central entity on TSP certification should be a long-term goal. In the meantime, risk-based bilateral agreements between banks and TSP are expected at the early stage. If there is sufficient support, the HKMA may explore to work with the industry to develop a set of risk- and principle-based common baseline criteria for banks as a reference to onboard TSP. Nevertheless, banks should not wait for the baseline criteria to be formed before onboarding TSP and proceeding with their implementation plan. The HKMA welcomes comments on whether the risk- and principle-based common baseline criteria should be developed by the HKMA. In particular, comments from banks are sought on the areas risk- and principle-based common baseline criteria should cover that banks will adopt.**

Open API Facilitation

85 The facilitation of an Open API ecosystem is an important aspect of its development. The following steps are recommended to ensure a healthy and sustainable growth of the market:

85.1 As a start, it is suggested that a central repository (also known as a dashboard) of all Open API from banks be

listed under the Data Studio website of the Hong Kong Science and Technology Parks so that a single point of reference is available for all TSP interested in using Open API to develop their websites or mobile applications. Other similar repositories, if available, may also be used.

85.2 For details on how to use each Open API, banks may host the information on their own website or leverage the Data Studio. However, details of the Open API functions, architecture, security and data definition are required to be clearly published using Open API Specification or similar standards when supported.

85.3 Furthermore, banks should provide sample codes and sandbox (testing environment with data, including artificial customer data if necessary) to assist TSP in using the Open API.

85.4 The HKMA plans to facilitate adoption activities such as partnering with the Data Studio on promotion, and organising educational events and competitions on the use of Open API. The HKMA will also consider hosting seminars and workshops for banks to meet relevant vendors that are involved in the building of the Open API ecosystem, as well as meeting aggregators that have use cases ideas or experience gained elsewhere.

Open API Maintenance

86 Once Open API are implemented by banks, there needs to be a body to review the relevance of the architecture, security and data standards on an ongoing basis. The body may also take on other industry-wide tasks of coordination where needed.

87 In the longer term, if harmonisation of Open API functions is desired by the industry, the body can also take on this task to work with the industry to achieve interoperability.

88 Owing to the evolving scope of this body, it is recommended that a working group be set up under the Hong Kong Association of Banks, with members initially drawn from road map banks which have in-depth knowledge and experience in Open API.

Way Forward

89 The Open API ecosystem is evolving and this Open API framework is only a directional and initial guide to help the commencement of the building of the underlying fabric. The HKMA intends to work with the industry to create a sustainable ecosystem, and to ensure the adoption by banks and the development of innovation products to meet the needs of customers.

Annex A – Open API Functions

A 1. The four phases of Open API functions are suggested below. For each of the phases, high-level functions of Open API are suggested based on those required by the UK Open Banking, the list of Open API proposed by MAS, the activities suggested by JBA and common functions found in Hong Kong's e-banking services.

A 2. The functions suggested are high-level in order to allow flexibility for banks to develop services that best fit their offering, business priority and existing business/technology plan. Banks may consider implementing additional or similar sets of Open API according to their business needs.

A 3. Banks are required, however, to publish the technical and engagement details on how to use their Open API using industry practice such as OpenAPI Specification (also known as Swagger).

Phase 1 - Product and service information:

Deposits	Loans	Investments	Insurance	Other bank products
• Retrieve saving account product details • Retrieve current account product details • Retrieve time deposit product details • Retrieve foreign currency account product details	• Retrieve credit card product details • Retrieve mortgage loan product details • Retrieve unsecured loan product details • Retrieve secured loan product details	• Retrieve retail investment fund product details • Retrieve structured investment product details • Retrieve precious metal product details • Retrieve stock trading product details	• Retrieve general insurance product details • Retrieve life or long-term insurance product details	• Retrieve safe deposit box product details

A 4. For illustrative purposes, non-exhaustive examples of the request and response of the high-level Open API functions under the Product and service information category are listed under Annex C for reference.

A 5. Banks are expected to deploy Open API functions to cover the above product and service information six months after the formal release of the Open API framework. They are also expected to provide the HKMA with a road map of API adoption covering the general scope of these functions before the end of the second month after the release of the formal framework. Any gap should be explained when providing the road map.

Phase 2 – New applications:

Deposits	Loans	Investments	Insurance	Other bank products
• Process saving account opening request • Process current account opening request • Process time deposit creation request • Process foreign currency account opening request	• Process credit card application request • Process mortgage loan application request • Process unsecured loan application request • Process secured loan application request	• Process investment funds account opening request • Process precious metal account opening request • Process stock account opening request	• Process general insurance application request • Process life or long-term insurance application request	• Process safe deposit box application

A 6. Banks are expected to deploy Open API functions to accept the above new applications, subject to service offering, 12 months after the formal release of the Open API framework. They are also expected to provide to the HKMA a road map of API adoption covering the general scope of these functions before the end of the seventh month after the release of the formal framework. Any gap should be explained when providing the road map.

Phase 3 – Account information:

Deposits	Loans	Investments	Insurance	Other bank products	Customer Service
• Retrieve deposit account details • Retrieve deposit account transaction details • Process time deposit maturity instruction	• Retrieve credit limit details • Retrieve credit card payment due date • Retrieve credit card outstanding payment details • Retrieve credit card transaction details • Retrieve outstanding loan details • Process credit limit increase request • Process credit limit decrease request • Process report credit card loss request • Process loan term change request	• Retrieve retail investment fund holdings information • Retrieve precious metal holdings information • Retrieve stock holdings information • Process customer instructions on corporate actions for stock holdings	• Retrieve general insurance policy details • Retrieve life or long-term insurance policy details • Process non-financial policy change requests	• Retrieve bill payment history • Process EBPP registration request • Process EBPP de-registration request • Retrieve registered electronic bill details and payment history	• Retrieve customer contact information • Process customer cheque book request

A 7. The timeline of Open API deployment to allow account information to be accessible will be reviewed in Q4 2018.

Phase 4 – Transaction:

Deposits	Loans	Investments	Insurance	Other bank products	Customer Service
• Process fund transfer request • Process e-Cheque issue request • Process e-Cheque deposit request • Process stop payment of issued cheque request	• Process credit card loyalty reward point redeem request • Process credit card cancellation request • Process credit card repayment request • Process loan repayment request	• Process retail investment fund transaction orders • Process precious metal transaction orders • Process stock trading orders	• Process financial policy change requests • Process claim request	• Process bill payment request • Process electronic bill payment request • Process direct debit authorisation setup request • Process direct debit authorisation cancellation request	• Process customer maintenance request of overseas ATM cash withdrawal limit • Process customer contact information update request

A 8. The timeline of Open API deployment to allow for transactions will be reviewed in Q4 2018.

Annex B – Architecture, Security and Data Standards

B 1. When considering the architecture, security and data standards, compatibility with industry best practice or requirements in other jurisdictions is important to reduce the adoption and implementation friction by banks and TSP. Accordingly the following standards are recommended.

Architecture:

B 2. Architecture refers to how TSP website or mobile applications connect to banks' Open API. Representational State Transfer (REST) and Simple Object Access Protocol (SOAP) are two common communication protocols in use for Open API. Under these respective communication protocols, data formats of JavaScript Object Notation (JSON) and eXtensible Markup Language (XML) are usually used.

B 3. The UK Open Banking initiative, the MAS Playbook and the JBA have all recommended REST as the communication protocol and JSON as the data format due to their practicality and wide acceptance by the industry. They are therefore recommended to be the basis for the Open API architecture.

B 4. **REST and JSON are recommended as the architectural basis unless there is an overriding reason for banks not to use them. In any case, conversion from SOAP to REST, and from XML to JSON is possible, so banks should consider providing such conversion where necessary.**

Security:

B 5. Security, including authentication, integrity, confidentiality and authorisation, is required for all four categories of Open API for the reasons indicated under paragraph 15 in the main paper.

B 6. For authentication of bank site and TSP, and integrity and confidentiality checks of data transmitted, properly registered and configured X.509 digital certificate is recommended to ensure

that product and service information is extracted from genuine bank sites.

B 7. TLS, on the other hand, provides integrity checking and encryption protection to the data being transmitted, regardless whether it is transmitted from bank to TSP or vice versa.

B 8. These security practices/standards are generally required by the UK Open Banking initiative, the MAS Playbook and the JBA.

B 9. Banks should continue to use their own authentication methods (such as username/password and two-factor authentication where appropriate) for bank customers while OAuth 2.0 is recommended as the authorisation method as it is an industry standard and suggested by the UK Open Banking initiative, the MAS Playbook and the JBA.

B 10. **The various recommended security protection requirements and technologies are summarised below:**

Protection required	*Technology*
Authentication of bank site and TSP	**X.509**
Integrity and confidentiality of data	**TLS**
Authentication of customer	**Bank's own method**
Authorisation of customer	**OAuth 2.0**

Controls:

B 11. **In addition to these prescribed security measures, banks should also observe any relevant risks and controls over the use of technology with applicable internal and/or HKMA guidelines to safeguard bank and consumer data.**

Data:

B 12. **For data standard, OFX is recommended for relevant Open API functions such as those related to account information. However, it is acknowledged that OFX is not widely used, so**

banks are free to use their own data descriptions (provided that they publish the definitions transparently) that suit their business needs particularly if this means they can meet the timeline. For other Open API functions that are not covered by OFX, banks are free to use their own data descriptions. In any case, banks should publish their data definition (often called "data dictionary") transparently using industry practice such as OpenAPI Specification (also known as Swagger).

B 13. **The HKMA particularly welcomes views on the approach suggested for the data standard.**

Annex C – Illustrative examples: Product and service information

Deposits

Retrieve saving account product details
Request - Product ID or name to identify a particular product (optional, if specified, only information of the specified product will be returned)
Response - List of Product IDs or names of saving account products being requested - Prevailing saving deposit rates for different tiers of account balance - Interest calculation methodology and deposit frequency (e.g. daily calculated and monthly deposited) - Eligibility for opening an account (e.g. account holder age requirements, minimum initial balance) - Availability of statements, passbooks, ATM cards, internet banking services, phone banking services, etc. - Minimum balance requirements and service fees if the minimum balance is not maintained - URLs of product-specific disclosure documents

Retrieve current account product details
Request - Product ID or name to identify a particular product (optional, if specified, only information of the specified product will be returned)
Response - List of Product IDs or names of current account products being requested - Prevailing interest rates for different tiers of account balance - Interest calculation methodology and deposit frequency (e.g. daily calculated and monthly deposited) - Currency of the account - Eligibility for opening an account (e.g. account holder age requirements, minimum initial balance) - Availability of statements, e-Cheques, ATM cards, internet banking services, phone banking services, etc. - Minimum balance requirements and service fees if the minimum balance is not maintained - Fees of cheque books and fees of returned cheques due to insufficient

funds/other reasons - URLs of product-specific disclosure documents

Retrieve time deposit product details
Request - Product ID or name to identify a particular product (optional, if specified, only information of the specified product will be returned)
Response - List of Product IDs or names of time deposit products being requested - Prevailing deposit rates for different tiers of account balance and deposit period - Interest calculation methodology and deposit frequency (e.g. daily calculated and monthly deposited) - Currency of the time deposit - Eligibility for opening an account (e.g. account holder age requirements, minimum initial balance) - Availability of statements, passbooks, ATM cards, internet banking services, phone banking services, etc. - Fees of early uplift of time deposit before maturity - URLs of product-specific disclosure documents

Retrieve foreign currency account product details
Request - Product ID or name to identify a particular product (optional, if specified, only information of the specified product will be returned)
Response - List of Product IDs or names of foreign currency account products being requested - Prevailing deposit rates for different tiers of account balance - Interest calculation methodology and deposit frequency (e.g. daily calculated and monthly deposited) - Currency of the account - Eligibility for opening an account (e.g. account holder age requirements, minimum initial balance) - Availability of statements, passbooks, ATM cards, internet banking services, phone banking services, etc. - Minimum balance requirements and service fees if the minimum balance is not maintained - URLs of product-specific disclosure documents

Loans

Retrieve credit card product details
Request - Product ID or name to identify a particular product (optional, if specified, only information of the specified product will be returned) - Applicant annual income or other information (optional, if specified, only information of applicable products will be returned)
Response - List of Product IDs or names of credit card products being requested - Welcome gifts or offers - Conditions and rates of cash rebates, miles or reward points on spending - Currency of credit card - Eligibility of application (e.g. cardholder age requirements, minimum annual income, etc.) - Availability of statements, internet banking services, phone banking services, etc. - Credit card related fees (e.g. annual fees, payment overdue fees, charges and interest rates) - URLs of product-specific disclosure documents

Retrieve mortgage product details
Request - Product ID or name to identify a particular product (optional, if specified, only information of the specified product will be returned) - Property valuation, type and age - Loan amount and tenor - Borrower age, annual income and whether a first-time-home-buyer (optional, if specified, only information of applicable products will be returned)
Response - List of Product IDs or names of mortgage products being requested - Loan interest rates (and its cap if applicable) - Loan amount and tenor - Welcome offers and their conditions, e.g. cash rebates, saving account with higher interest rates - Monthly repayment amount (or repayment amount under other repayment frequency)

- Availability of statements, internet banking services, phone banking services, etc. - Related fees (e.g. valuation fees, handling fees, early repayment charges) - URLs of product-specific disclosure documents

Retrieve unsecured loan product details
Request - Product ID or name to identify a particular product (optional, if specified, only information of the specified product will be returned) - Loan amount and tenor (if applicable) - Borrower age and monthly income (optional, if specified, only information of applicable products will be returned)
Response - List of Product IDs or names of products being requested - Loan interest rates, handling fees and annualised percentage rates - Loan amount and tenor - Welcome offers and their conditions, e.g. cash rebates - Monthly repayment amount (or repayment amount under other repayment frequency) (if applicable) and total repayment amount (if applicable) - Availability of statements, internet banking services, phone banking services, etc. - URLs of product-specific disclosure documents

Retrieve secured loan product details
Request - Product ID or name to identify a particular product (optional, if specified, only information of the specified product will be returned) - Value and type of pledged assets - Loan amount and tenor (if applicable) - Borrower age and monthly income (optional, if specified, only information of applicable products will be returned)
Response - List of Product IDs or names of products being requested - Loan interest rates, handling fees and annualised percentage rates - Loan amount and tenor - Welcome offers and their conditions, e.g. cash rebates - Monthly repayment amount (or repayment amount under other repayment frequency) and total repayment amount (if applicable)

- Availability of statements, internet banking services, phone banking services, etc. - URLs of product-specific disclosure documents

Investments

Retrieve retail investment fund product details
Request - Product ID or name to identify a particular product (optional, if specified, only information of the specified product will be returned) - Code or name of a retail investment fund, unit trust or mutual fund (optional, if specified, information of a specified fund will be returned)
Response - List of Product IDs or names of products being requested - Eligibility for opening an investment fund account (e.g. account holder age requirements, minimum initial investment amount) - Related fees like subscription, redemption, management, fund switching fees, monthly investment plan handling fees - Availability of statements, internet banking services, phone banking services, etc. - Information of a particular retail investment fund if specified in the request (like investment objective, strategy, portfolio, price, fees and charges, etc.) - URLs of product-specific disclosure documents - URLs of portal showing available investment fund choices

Retrieve structured investment product details
Request - Product ID or name to identify a particular product (optional, if specified, only information of the specified product will be returned)
Response - List of Product IDs or names of products being requested - Underlying assets of the structured products - Key product information like potential returns and the scenarios to generate these returns, offer period, issue date and price, maturity date, principal protection at maturity, condition of early termination by issuer - Eligibility for opening a structured investment product account (e.g. account holder age requirements, minimum initial investment amount) - Fees and charges

- Availability of statements, internet banking services, phone banking services, etc. - URLs of product-specific disclosure documents

Retrieve precious metal product details
Request - Product ID or name to identify a particular product (optional, if specified, only information of the specified product will be returned) - Code or name of an underlying reference asset (optional, if specified, only information of the specified asset will be returned)
Response - List of Product IDs or names of products being requested - Underlying reference assets - Key product information like settlement currency of the product, trading and pricing mechanism, minimum transaction amount - Eligibility for opening a precious metal product account (e.g. account holder age requirements, minimum initial investment amount) - Fees and charges - Availability of statements, internet banking services, phone banking services, etc. - Information of a particular underlying reference asset if it is specified in the request (like trading prices and units of trading) - URLs of product-specific disclosure documents

Retrieve stock trading product details
Request - Product ID or name to identify a particular product (optional, if specified, only information of the specified product will be returned) - Code or name of a stock (optional, if specified, only information of a specified stock will be returned)
Response - List of Product IDs or names of products being requested - Applicable stock markets or stocks being traded (e.g. Hong Kong listed stock market, China A shares) - Eligibility for opening a stock trading account (e.g. account holder age requirements) - Related fees like brokerage fees, custody fees, fees related to corporate actions, monthly investment plan handling fees

- Availability of statements, internet banking services, phone banking services, etc. - Information of a particular stock if specified in the request (like quotation of trading prices) - URLs of product-specific disclosure documents

Insurance

Retrieve general insurance product details
Request - Product ID or name to identify a particular product (optional, if specified, only information of the specified product will be returned) - Information applicable to the quotation of a general insurance product (like destination and period of travel for travel insurance, age of insured for health insurance)
Response - List of Product IDs or names of products being requested - Insurance coverage and premium details - Eligibility of the proposed insured or conditions (e.g. age of proposed insured, maximum coverage days of single trip travel insurance plan) - Availability of statements, internet banking services, phone banking services, etc. - URLs of product-specific disclosure documents - URLs of detailed terms and conditions of insurance plans

Retrieve life or long-term insurance product details
Request - Product ID or name to identify a particular product (optional, if specified, only information of the specified product will be returned) - Information applicable to the quotation of a life or long-term insurance product (like age, gender, smoking habit of the insured, sum insured)
Response - List of Product IDs or names of products being requested - Insurance coverage and premium details - Eligibility of the proposed insured or conditions (e.g. age of proposed insured, health conditions) - Availability of statements, internet banking services, phone banking services, etc.

- URLs of product-specific disclosure documents - URLs of detailed terms and conditions of insurance plans

Other bank products

Retrieve safe deposit box product details
Request - Product ID or name to identify a particular product (optional, if specified, only information of the specified product will be returned) - Size and location of safe deposit box (optional, if specified, only information of applicable product will be returned)
Response - List of Product IDs or names of products being requested - Size, location and availability of safe deposit box - Eligibility of the applicant (e.g. age requirement) - Rental fees and related charges - URLs of product-specific disclosure documents

The examples are for illustrative purpose only. The information in the examples does not represent an exhaustive list of information to be included in an Open API endpoint nor a minimum requirement for that Open API function.