Publication date: 18 July 2018

Open API Framework for the Hong Kong Banking Sector

HONG KONG MONETARY AUTHORITY
香港金融管理局

Table of Contents

I. INTRODUCTION

Background

1 As one of the seven Smart Banking initiatives and following the receipt of the consultation feedback from the industry on the proposed framework for facilitating the development of Open Application Programming Interface (API) for the banking industry in Hong Kong, the Hong Kong Monetary Authority (HKMA) is now publishing the finalised framework and the related implementation plan.

2 The key benefits of Open API can be reaped only if it is widely, securely and cost-effectively implemented in the banking sector. The HKMA will therefore work closely with the banking industry in implementing Open API effectively, securely and smoothly through the development of the governance structure and necessary guidance during the implementation process.

3 In developing the proposed Open API framework, the HKMA invited nomination of Open API contacts from 20 retail and three foreign banks, hosted a workshop on 15 August 2017 and held discussions with Open API contacts throughout September and October 2017. A draft Open API framework was then proposed and opened for industry consultation from 11 January 2018 to 15 March 2018. This Open API framework contains the necessary revisions after the consultation. It becomes effective from the date of publication.

Policy Objectives

4 The policy objectives of the implementation of the Open API framework are to help:

4.1 ensure the competitiveness and relevance of the banking sector;

4.2 provide a secure, controlled and convenient operating environment to allow banks and their partners[1] (called third party service providers, or TSPs, in this framework), to work together and develop innovative/integrated banking services that improve customer experience; and

4.3 keep up with international developments in the delivery of banking services.

II. OPEN API

5 APIs can be seen as the interfaces between software applications, both within an organisation and between organisations. APIs enable communication between software applications where one application calls upon the functionality of or passes data to another application. [2]

6 APIs enable secure, controlled, cost-effective and granular access to data and/or functionality of systems. Open APIs, in the context of this document, refer to APIs that allow third party access to systems belonging to an organisation. However, Open APIs for the banking industry do not necessarily mean that any third party can freely access a bank's system without restriction, because banks still need to ensure adequate controls such as security and consumer protection.

III. OPEN API FRAMEWORK

Applicability

7 This Open API framework focuses only on the retail banking operation in Hong Kong at the initial stage as it covers the services offered to the largest group of customers. However,

[1] Including other banks
[2] "Understanding the business relevance of Open APIs and Open Banking for banks", Euro Banking Association May 2016

banks are welcome to extend the framework to any other banking business as they see fit.

Guiding Principles

8 In developing the Open API framework, the following high-level principles and assumptions were used:

8.1 The implementation of Open API would bring many benefits and efficiency gain to the banking industry and to its customers. Feedback from the banking industry indicates that it is desirable to implement Open APIs to provide better services to satisfy the demands of its customers. Banks are therefore expected to implement the Open API framework in the timeline set out in the framework. The HKMA will monitor the implementation closely, and act accordingly to ensure market adoption and encourage use cases.

8.2 The HKMA has taken note of the mandatory approach adopted by some jurisdictions such as the EU, the UK and Australia but has decided that a collaborative and phased approach is an appropriate approach for Hong Kong for the time being. The HKMA will monitor the progress of Open API implementation in Hong Kong and further consider the need for new regulatory measures if necessary.

8.3 The framework is intended to be high-level in order to allow banks the flexibility in implementing Open API as part of their strategy. The HKMA does not wish to prescribe how banks should adopt Open API down to implementation steps.

8.4 High-level Open API functions have been selected on the basis of their potential benefits to banks and customers, and identified in order of priority.

8.5 Existing international or industry practices have been leveraged in the framework in order to ensure ease of implementation and speedy development of Open APIs.

Scope of the Open API Framework

9 The scope of the Open API framework comprises the following parts:

9.1 Open API functions and deployment timeframe;

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

9.3 TSP governance model;

9.4 Open API facilitation measures; and

9.5 Open API ongoing development.

Scope and Development Timeframe of Open API Functions

10 The scope and selection of Open API functions are the key and the first step because the correct identification could lead to early implementation. At the same time, the industry's desire for a progressive and step-by-step approach to implement Open APIs beginning with a less risky set of functions is recognised.

Categorisation

11 During the discussions with Open API contacts, it was agreed that the implementation of **Open APIs should be prioritised into four categories** based on their implications, opportunities and risks:

11.1 **Product and service information** – "Read-only" information offered by banks on details of their products and services;

11.2 **Subscription and new applications for product/service** – Customer acquisition process such as allowing online submissions/application of credit cards, loans or other bank products;

11.3 **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

11.4 **Transactions** – Banking transactions and payment or scheduled payments/transfer initiated by authenticated customers.

12 It was further agreed that the types of protection required for each of the four categories of Open API implementation should be in a progressive manner as follows:

Categories of Open API	*Protections required*
Product and service information	• Authentication of bank sites • Integrity of data • Authentication of TSPs
Subscription and new applications for product/service	• Authentication of bank sites • Integrity and confidentiality of data • Authentication of TSPs
Account information	• Authentication of bank sites • Integrity and confidentiality of data • Authentication of TSPs • Authorisation of customers
Transactions	

A phased approach

13 Owing to the increased sensitivity of data and therefore the increased risks involved in each subsequent category, the protective measures required will be more complicated. Therefore,

a four-phased approach matching the four categories of Open API, is recommended.

14 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 implementation and timeline for the deployment should therefore be relatively simple and short.

15 Subsequent phases of Open APIs would involve more sophisticated technology, security and authentication infrastructure, and therefore may require more development efforts. However, as banks would have accumulated experience in prior phases, timelines of the subsequent phases are not expected to be disproportionately long.

16 Based on the comments received from the consultation, the proposed six-month timeline after the publication of this framework for launching Product and service information (referred as Phase I) Open APIs by banks remains. The proposed 12-month timeline for Subscription and new applications (referred as Phase II) is relaxed to 12 - 15 months to allow the industry more time for preparation.

17 For the subsequent phases, Open APIs would allow even more innovative and convenient services. As the complexity and risk of opening up data of all customers increase, the technology and infrastructure to support, monitor and secure the Open API access become more complex and critical. The HKMA will therefore closely monitor the situation and take into consideration local and international developments, and decide the timeline with the industry during the coming 12 months.

18 **The timeline of Open API deployment is summarised as follows:**

Phase	*Categories of Open APIs*	*Timeline after the publication of this Open API framework*
I	**Product and service information**	**Six months**
II	**Subscription and new applications for product/service**	**12 – 15 months**
III	**Account information**	**To be set out within the next 12 months**
IV	**Transactions**	**To be set out within the next 12 months**

19 It should be noted that the suggested timeline above represents the latest expected dates for banks to make available the Open APIs indicated. Individual banks are welcome to advance their own programme, either for completion of individual phases or for introducing Open APIs for those categories that have not yet been set out in the timeframe. For example, a bank may choose to make available Open APIs for conducting transactions on their products and services during Phase I at the same time as they launch their Product and service information Open APIs. However these banks should ensure that commensurate level of protections[3] and suitable TSP governance arrangements are in place with appropriate contracts to clearly define the responsibility, liability, control and customer protections.

Open API functions

20 Throughout the discussion and consultation period, the HKMA recognises the industry's desire to see a common set of Open

[3] Including, among others, implementation of appropriate measures by TSPs and banks for addressing the applicable requirements related to consumer protection (including applicable consumer protection provisions set out in the Code of Banking Practice) and the applicable regulatory requirements related to customer data protection.

APIs for better interoperability. However, a number of international banks operating in Hong Kong have already implemented their group standard for implementing Open APIs at global or regional levels, and have demonstrated elsewhere that requiring banks to adhere to a prescribed set of standardised Open API functions is challenging.

21 Some opinions from the technology sector also indicate that it would be more desirable for banks to quickly offer Open APIs than to wait for standardised Open APIs that would take time to emerge. Furthermore, it is believed that once an ecosystem has been developed and becomes mature, convergence to standardised Open APIs will likely occur in response to the needs of the market.

22 Taking into account the practices and experience of the UK, Singapore and Japan, and the feedback during the consultation exercise, high-level core-banking Open API functions are specified for deployment and further set out in Annex A.

23 In this connection, banks are expected to provide the HKMA with road maps of Open API implementation (Product and service information within two months, and Subscription and new applications within eight months from the publication of this framework). Banks are also expected to explain how their road maps meet the general scope described in Annex A (and in the case of gaps, the reasons).

24 The HKMA plans to publish a summary (covering at least the functions to implement and their timelines) of the road maps for individual banks so that the industry can better plan for service offerings. The publication will also reduce the workload of banks in providing such information to individual prospective TSPs.

25 Banks are always welcome to implement Open APIs ahead of time or implement functions that have not been specified in this framework.

Architecture, Security and Data Standards

26 Based on international practice and the feedback during the consultation exercise, the recommended architecture and security standards are listed in Annex B.

27 While certain technical standards have been prescribed, they cannot be considered as the only standards that cover all security requirements. Banks should always make reference to industry sound practices, relevant regulatory and internal requirements, and apply holistic controls on information and cybersecurity based on a risk- and principle-based approach to protect banks' systems as well as bank and consumer data.

28 To help speedy and timely implementation, banks may decide their own data specification. Banks, however, should publish such definition (often called "data dictionary") using industry practices normally in use, such as OpenAPI Specification (also known as Swagger).

TSP Governance

29 In order to strike a balance between innovation and customer protection, it is preferred that TSPs offer solutions under a partnership arrangement with banks. Banks are therefore expected to adopt a formal TSP governance process.

30 TSP governance process covers a range of activities such as due diligence, onboarding, control, monitoring, roles and responsibilities, consumer protection, data protection, security, infrastructure resilience, and incident handling. Three possible approaches were suggested during the discussions and the consultation exercise:

30.1 Bilateral – Banks carry out their own risk assessment and due diligence on bilateral engagements with TSPs covering all aspects of TSP governance according to the

nature of the engagement, and established policies and procedures of the banks.

30.2 Central entity – A central entity is funded and formed in agreement by all the banks involved to develop a common set of TSP governance criteria and assessment service so that the process may be streamlined and made more efficient.

30.3 Bilateral with a common baseline – A set of TSP governance common baseline is developed and agreed by banks. While banks may add in their own unique requirements, the baseline approach streamlines the onboarding process.

31 Based on the discussions held and feedback received from the consultation exercise where bilateral arrangement with a common baseline is preferred, the following TSP Governance arrangements are considered as the most appropriate:

31.1 The TSP governance processes for different categories of Open APIs are summarised below:

Open APIs	***TSP governance processes***
Those specified under Phase I	• Banks should establish simple TSP registration process with basic consumer protection measures in place.
Those specified under Phase II and beyond	• Banks should have in place: i. onboarding checks on TSPs; ii. ongoing monitoring on TSPs; and iii. bilateral contractual relationship with TSPs.

31.2 The aforementioned onboarding check process may be carried out as below:

31.2.1 A number of banks may agree on the scope of the common baseline onboarding checks among themselves to facilitate easier onboarding; and

31.2.2 TSP may re-use common baseline materials prepared for one bank to submit to another.

31.3 Banks may further streamline the onboarding checks by agreeing on a set of common baseline assessment benchmarks/criteria for the agreed common baseline. Banks may carry out TSP assessments by one of the following means:

31.3.1 Banks conduct their own assessments of TSPs. A bank may also, subject to its own risk evaluation, consider a TSP that has been successfully assessed by another bank;

31.3.2 Banks appoint their own assessors to carry out the assessments of TSPs. A bank may also, subject to its own risk evaluation, consider TSPs that has been successfully assessed by another assessor; or

31.3.3 Banks appoint common assessor(s) to carry out the assessments of TSPs.

32 Details of each of these processes, together with the recommended scopes for the onboarding checks and commercial contracts, are listed in the following sections.

Phase I

Registration

33 The HKMA wishes to clarify that the comprehensive TSP governance process is only necessary for Phase II and beyond.

For Phase I where banks open up Product and service information as open data, the HKMA expects banks to have a simple registration process in place for consumer protection purpose, unless a bank decides to implement more advanced functionalities.

34 The registration process should be simple and should not be used to impose unnecessary requirement to create entry barriers. The process is expected to achieve the following purposes:

34.1 Capacity planning – Banks can gauge the degree of interest and plan the necessary capacity on the infrastructure;

34.2 Relationship management – Banks can start engaging potential TSPs, and understanding their business models and plans to prepare for the implementation of phases II to IV; and

34.3 Consumer protection – Banks should have terms and conditions in place to address at least the following issues:

34.3.1 TSPs should notify banks of their products/services which fall within the scope of and are bound by the terms and conditions;

34.3.2 Since TSPs may collect customers' data for their own purposes, banks should require TSPs (i) not to misrepresent banks, (ii) to make it explicit to their customers that the collection of personal data is neither carried out by banks nor directly related to bank business, and (iii) comply with the applicable laws and guidance on the protection of personal data; and

34.3.3 TSPs should make clear the associated risk and liability of their services to their customers.

35 Banks are expected to have the registration process in place within the timeline of Phase I. Banks should allow TSPs Open API access to Product and service information only if the TSPs are registered and agree to the relevant terms and conditions.

Phase II and beyond

Onboarding check/common baseline development

36 Throughout the discussion and consultation period, respondents expressed clear preference for the bilateral arrangement with a common baseline as the preferred TSP governance approach during the initial period of rolling out Open APIs. Respondents indicated that this arrangement allows for maximum flexibility and shortest time-to-market for implementing Open APIs.

37 Given that the industry wishes to develop a common baseline, the HKMA expects that the industry will therefore put in the necessary efforts through, for example, the Hong Kong Association of Banks (HKAB), to develop and finalise the common baseline before Phase II implementation, which is 12 to 15 months after the publication of this Open API framework. The HKMA will provide facilitation as required.

38 The goal of developing a common baseline is to facilitate and streamline banks' engagement with TSPs through agreements and create a level playing field. The common baseline should therefore aim to simplify and encourage adoption of Open APIs by the banks with TSPs, and allow a greater variety of services and convenience that is beneficial to the customer. It is therefore in the interest of the banking sector to agree on the scope (a list of questions and requirements) of the common baseline as far as possible and endeavour to minimise any additional requirements. The common baseline should cover at least the elements listed in the recommended scope below. Banks may choose to carry out

additional checks that fit their needs but they should ensure that those checks are reasonable and not excessive.

39 With the common baseline in place, TSPs may prepare a set of standard documents or evidence to satisfy the common requirements of multiple banks during the due diligence process. This is expected to save efforts for both banks and TSPs.

Scope of the common baseline

40 It is suggested that the scope of the common baseline should cover at least areas on business and risk management in the following ways:

40.1 Business – Including financial soundness, reputation, quality of management, and appropriateness of business operations; and

40.2 Risk management – Including capabilities and controls of the TSPs in the areas of risk management, business and technical expertise in the field, customer and data protection measures (including the avoidance of excessive collection of personal data), cybersecurity and IT controls (including, among others, confidentiality, integrity and availability, monitoring and mitigation measures, and contingency planning).

41 However, given the objective of the common baseline as a means of facilitation, the requirements set out therein should be fair and reasonable, and compensate with the risks involved.

A streamlined assessment model

42 The industry, through its own initiatives and efforts, may develop a streamlined assessment model (including the involvement of a central entity/assessor) to assess the common baseline when the industry deems appropriate.

43 The streamlined assessment model is meant to reduce efforts for both banks and TSPs to carry out onboarding checks. The development and agreement by multiple banks on a set of common baseline assessment benchmarks/criteria would be the prerequisite for this model.

44 The industry may decide how it wants to implement this streamlined assessment model. Some possible options of implementation are set out below:

44.1 Banks agree among themselves on a bilateral or multilateral basis to recognise the common baseline assessment performed by each other; or

44.2 Banks appoint their own accessors (or a central entity/accessor) to carry out the common baseline assessment for them and agree bilaterally or multilaterally if they would recognise the common baseline assessment performed by these assessors.

Ongoing monitoring of TSPs

45 It is also suggested that there should be a risk-based ongoing monitoring mechanism for banks to ensure that TSPs continue to meet the relevant parts of the common baseline (or equivalent assessment) after the initial assessment process.

Commercial contract

46 Banks should negotiate bilaterally with TSPs on commercial contracts in addition to the TSP onboarding assessment and ongoing monitoring.

47 It is expected that the contract terms with TSPs should define, where applicable, areas on legal [4], business [5], security and

[4] Such as the roles and responsibilities, data ownership and governing law.
[5] Such as commercial terms and Open API charging model.

control[6], consumer protection[7] and any other relevant aspects. However, banks should not use commercial contracts to impose unnecessary requirements to create entry barriers for TSPs.

Publication of partnership for consumer protection

48 In order to ensure public trust and consumer protection, banks are expected to publish a list of partnering TSPs and their relevant products (such as mobile apps or websites) for Phase II and beyond. The HKMA may work with the industry to centrally provide to the public with a list of partnering TSPs and their relevant products. In this connection, banks should provide updates to the list in a timely manner.

49 In addition, banks should monitor the Internet regularly to see if there are third party websites, apps and similar scams which purported to be operated by the banks' partnering TSPs under the Open API framework or claimed to be partnering with the banks when they are not. Whenever banks become aware of these cases, banks should notify promptly their customers and the public through issuing press releases (or similarly effective means).

Liability

50 In line with the relevant clause in the Code of Banking Practice, a customer should not be responsible for any direct loss suffered by him/her as a result of unauthorised transactions conducted

[6] Such as the requirement for fulfilling the relevant parts of the common baseline by the TSPs and the consequences of failing to fulfil them, the right to assess TSP's relevant controls and their effectiveness in fulfilling the common baseline, and timely reporting and notification of significant incidents (e.g. data leakage).

[7] Such as fair treatment of customers, disclosure and transparency (including, among others, presenting to customers succinct and easy-to-understand summary on the use and purpose of collecting the personal data and key highlights of the terms and conditions of the services offered.), customer data protection (including, among others, appropriate control and safeguards in relation to the collection, use, holding and erasure of customer data for complying with the applicable laws and guidance on the protection of personal data, the consent model for storing or sharing customer data), commitment not to store customers' e-banking credentials, responsible conduct, protection of customers against fraud, complaint handling mechanism with accessible channels for interacting with customers to deal with their enquiries and complaints, redress measures, clear liability and settlement arrangement between the bank and the partnering TSP for compensating customers' loss arising from unauthorised transactions, and purchase of liability insurance by the TSP (where appropriate, such as when high-risk transactions are involved).

through his/her account attributable to the services offered by TSP using banks' Open API unless he/she acts fraudulently or with gross negligence. In these cases, banks and TSP should provide refund to customers according to the liability and settlement arrangement defined in their contractual terms.

51 Given the wide range of service offerings made possible with Open API, liabilities between banks and TSPs will be dependent on the actual mode of operation. Banks and TSPs should therefore define and agree a clear liability and settlement arrangement to protect customers in the cases of loss, and communicate clearly to customers.

Open API Facilitation

52 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:

52.1 A single point of reference (may also be known as a repository or a dashboard) of all Open APIs offered by banks will facilitate ease of access by TSPs. During the discussion process, some banks suggested that it would be desirable for the Data Studio of the Hong Kong Science and Technology Parks to take up this dashboard role. Hence, it is recommended that all Open APIs from Phase I onwards are listed under the Data Studio.

52.2 The listing of Open APIs under the Data Studio will not preclude banks from using other repositories. The industry or individual banks are free to list their Open APIs in multiple repositories.

52.3 For details on how to use each Open API, banks may host the information on their own websites or leverage the dashboard. However, details of the Open API functions, architecture, security and data definitions (as referred in

Annex B) should be clearly published using OpenAPI Specification or similar standards when supported.

52.4 Furthermore, banks should provide examples and testing environment with data (including artificial customer data if necessary) to assist TSPs in using their Open APIs.

53 The HKMA plans to facilitate adoption activities such as partnering with interested parties on promotion, and organising educational events and competitions on the use of Open APIs among the industry. The HKMA will also consider hosting seminars and workshops for banks and technology companies to share use case ideas or experience gained elsewhere.

Open API Ongoing Development

54 Once Open APIs have been 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, such as coordination and consumer education, where needed.

55 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.

56 As the Open API ecosystem is a partnership between banks and TSPs, the body that work on the continuous development of Open APIs is expected to maintain dialogues with the TSP community.

57 The HKAB have expressed full support for Open APIs as one of the HKMA's seven initiatives for "A New Era of Smart Banking" and confirmed that a committee will work on this continuous development of Open APIs with the HKMA to support the changing needs of the industry as technology evolves.

Way Forward

58 As the Open API ecosystem is evolving, this Open API framework aims to provide a directional guide to help the commencement of building the underlying fabric. The HKMA intends to work with the industry to review the framework from time to time, create a sustainable ecosystem, and ensure the implementation 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 listed below. For each of the phases, high-level functions of Open APIs are suggested based on local/international practice and experience. Banks are expected to make available the Open APIs in each category no later than the indicated dates, but they may choose to introduce Open APIs in any phase earlier. For example, subject to appropriate protections and security controls, a bank may choose to offer certain transaction Open APIs during Phase I.

A 2. Taking account of responses received, the HKMA agrees that banks may choose which functions under Investments and Insurance to implement according to business priorities and service offerings. However, banks are expected to provide all functions under the categories of Deposits, Loans and Other banking services, which are considered to be core-banking functions.

A 3. When banks launch their Open APIs, they should publish the technical and engagement details on how to use their Open APIs using industry practice normally in use, such as OpenAPI Specification (also known as Swagger).

Phase I - Product and service information

A 4. The Phase I high-level Open API functions are listed in the table that follows.

Core-banking functions			Others	
Deposits	**Loans**	**Other banking services**	**Investments**	**Insurance**
• 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 safe deposit box product details • Retrieve branch and ATM information • Retrieve foreign currency exchange rate	• 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

A 5. For illustrative purposes, non-exhaustive examples of the request and response of the high-level Open API functions under Phase I (Product and service information) are listed in Annex C for reference.

A 6. Banks are expected to deploy core-banking Open API functions within six months after the publication of this Open API framework. They are also expected to provide the HKMA with a road map together with the delivery dates of each Phase I Open API function within two months after the publication of this framework. Any gap in timeline and scope should be explained when providing the road map. If a bank plans to introduce additional Open APIs (e.g. Open APIs for account opening or executing transactions for product and services) or other supporting functions/features earlier than the timeline set in this framework, they are welcome to do so and they should set out such plan in their road map, as well as the security and control arrangements to be put in place. Please also refer to paragraph 19 for the expectation.

A 7. A summary (covering at least the functions to implement and their timelines) of the submitted road maps will be published so that the industry can better plan for service offerings. The banks' workload in providing such information to prospective TSPs of Open APIs can also be reduced.

Phase II – Subscription and new applications

A 8. The Phase II high-level Open API functions are listed in the table below.

Core-banking functions			Others	
Deposits	**Loans**	**Other banking services**	**Investments**	**Insurance**
• 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 safe deposit box application	• 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

A 9. Banks are expected to deploy Core-banking Open API functions to accept new applications 12 to 15 months after the publication of this Open API framework. The HKMA recognises the evolving nature of technology, particularly those that may assist non face-to-face account opening or know-your-customer processes, and will leave it to banks to decide on the level of automation and the technology they would adopt to handle new applications having regard to their risk appetite, business priority and maturity of technology.

A 10. Banks are also expected to provide the HKMA with a road map together with the delivery dates of each Phase II functions within eight months after the publication of this framework. Any gap in timeline and scope should be explained when providing the road map. Again, a bank may choose to introduce additional Open APIs and include its plan as well as security and control measures in its road map.

A 11. A summary (covering at least the functions to implement and their timelines) of the submitted road maps will be published so that the industry can better plan for service offerings. The banks'

workload in providing such information to prospective TSPs of Open APIs can also be reduced.

Phase III – Account information

A 12. The Phase III high-level Open API functions are listed in the table below.

Core-banking functions			Others	
Deposits	**Loans**	**Other bank products**	**Investments**	**Insurance**
• 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 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	• 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

A 13. The HKMA will closely monitor the situation and take into consideration local and international developments, and decide the deployment timeline of Phase III (Account information) with the industry during the coming 12 months.

Phase IV – Transaction

A 14. The Phase IV high-level Open API functions are listed in the table that follow.

Core-banking functions			Others	
Deposits	**Loans**	**Other bank products**	**Investments**	**Insurance**
• 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 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	• Process retail investment fund transaction orders • Process precious metal transaction orders • Process stock trading orders	• Process financial policy change requests • Process claim request

A 15. The HKMA will closely monitor the situation and take into consideration local and international developments, and decide the deployment timeline of Phase IV (Transactions) with the industry during the coming 12 months.

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 implementation friction faced by banks and TSPs. Accordingly the following standards are recommended.

Architecture:

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

B 3. Due to their practicality and wide acceptance by the industry, REST is recommended as the communication protocol and JSON as the data format.

Security:

B 4. Security, including authentication, integrity, confidentiality and authorisation, is required for all four categories of Open APIs for the reasons indicated in paragraph 12 in the main paper.

B 5. For authentication of bank sites and TSPs, 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 6. Transport Layer Security (TLS), on the other hand, provides integrity checking and encryption protection to the data being transmitted, regardless of whether it is transmitted from bank to TSP or vice versa.

B 7. Banks should continue to apply the risk-based approach to use their own authentication methods (such as username/password and two-factor authentication where appropriate) for bank customers. They should only grant access privileges to TSPs on customers' requests. OAuth 2.0 is recommended as the authorisation method as it is an industry standard.

B 8. The various recommended security protection requirements and technologies are summarised below:

Protection required	*Technology*
Authentication of bank sites and TSPs	X.509
Integrity and confidentiality of data	TLS
Authentication of customers	Bank's own method
Authorisation of customers	OAuth 2.0

Controls:

B 9. In addition to these prescribed security measures, banks should also observe any relevant risks and controls over the use of technology in accordance with applicable internal and/or HKMA guidelines to safeguard bank and consumer data.

Data:

B 10. Banks are free to use their own data descriptions for data standard. In any case, banks should publish their data definition (often called "data dictionary") using industry practice such as OpenAPI Specification (also known as Swagger).

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 - URLs to existing product application page(s) (if applicable)

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
- URLs to existing product application page(s) (if applicable)

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 - URLs to existing product application page(s) (if applicable)

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 - URLs to existing product application page(s) (if applicable)

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 - URLs to existing product application page(s) (if applicable)

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
- URLs to existing product application page(s) (if applicable)

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 - URLs to existing product application page(s) (if applicable)

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 - URLs to existing product application page(s) (if applicable)

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 - URLs to existing product application page(s) (if applicable)

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
- URLs to existing product application page(s) (if applicable)

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
- URLs to existing product application page(s) (if applicable)

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 - URLs to existing product application page(s) (if applicable)

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 - URLs to existing product application page(s) (if applicable)

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 - URLs to existing product application page(s) (if applicable)

Other banking services

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 - URLs to existing product application page(s) (if applicable)

Retrieve ATM information
Request - Range of geographic locations (optional, if specified, only ATM located within the range of locations will be returned)
Response

- Locations of ATM (e.g. geographic coordinates, full address or both) - Services offered by ATM (e.g. HKD cash withdrawal, foreign currency cash withdrawal, cash deposit, bill payment, cheque deposit) - Accessibility of ATM (e.g. wheelchair access, indoor facility) - Related enquiry hotline number

Retrieve branch information
Request - Range of geographic locations and services (optional, if specified, only the branches located within the range of locations and offering requested services will be returned)
Response - Location of branch (e.g. geographic coordinates, full address or both) - Services offered by branch (e.g. deposits services, investment services, retail or corporate banking services, fully automated or manned services) - Accessibility of branch (e.g. wheelchair access, outdoor mobile branch) - Opening hours of branch - URL of photo of branch - Related enquiry telephone number

Retrieve foreign currency exchange rate information
Request - Foreign currency requested (optional, if specified, only the exchange rate of the specified currency against HKD will be returned) - Amount of foreign currency requested (optional, if specified, only the exchange rate applicable to the specified amount will be returned)
Response - Foreign currency name and code - Bank's foreign currency telegraphic transfer and banknote buying rate and selling rate against HKD - Conditions for applying the foreign currency exchange rate returned (e.g. rates apply to existing customers of a certain tier of accounts) - Last update time of the quoted foreign currency exchange rate - Service fees payable by customers to execute the foreign currency exchange - Disclaimer or other relevant terms and conditions to use the quoted foreign currency exchange rate

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.