BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Publishing Open Data using Open API

Exposure Draft

Applicable to:

1. Licensed bank
2. Licensed Islamic bank
3. Licensed insurer
4. Licensed takaful operator

Issued on: 5 September 2018

BNM/RH/ED 028-10

This Exposure Draft sets out the Bank's proposed guidance on the development and publication of Open Application Programming Interface (Open API) for open data by financial institutions.

The Bank invites written feedback on this Exposure Draft, particularly on the specific questions raised throughout the document. Responses may include suggestions on areas to be clarified or alternatives that the Bank should consider. The feedback should be supported with clear reasons, including accompanying evidence or illustrations where appropriate to facilitate an effective consultation process. Feedback could also be provided via Github [https://github.com/BankNegaraMY], particularly on the proposed Open Data API Specifications for selected product information. These Open Data API Specifications will be available on the following dates:

(a)	Motor insurance/takaful	: 14 September 2018
(b)	Credit card	: 14 September 2018
(c)	SME financing	: 17 September 2018

If comments are provided on Github, please indicate your contact details.

Responses must be submitted by 28 September 2018 to–
Pengarah
Jabatan Pembangunan Kewangan dan Inovasi
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
Email: openapi@bnm.gov.my

The Bank encourages electronic submission. Submissions received by the Bank may be made public unless confidentiality is specifically requested for the whole or part of the submission.

In preparing your feedback, you may direct any queries to the following officers:

(a) Khairul Fathi Ramli at kfathi@bnm.gov.my/03- 26988044 (ext. 7620)
(b) Azlan Zainal at azlanz@bnm.gov.my/03-91792888 (ext. 4336)
(c) Wan Nadira Hanim at wannadira@bnm.gov.my/03-26988044 (ext. 7818)
(d) Norariefah Mohd Iqbal at norariefah@bnm.gov.my/03- 91792158 (ext. 2556)

Issued on: 5 September 2018

TABLE OF CONTENTS

PART A OVERVIEW

1. Introduction

1.1. An Application Programming Interface (API) enables the interaction between different software applications via a specified set of protocols. This allows software applications to communicate with each other to exchange data directly or to access another software application's functionalities, through automated access.

1.2. Open APIs allow third party developers to access data without needing to establish a business relationship with the Open API publisher. Access to restricted or more sensitive data through Open APIs, such as customer account information, is usually supported by security, legal and governance frameworks necessary to protect customer's confidentiality and financial institutions' core systems.

1.3. The Bank recognizes the benefits of Open API standardisation initiatives to the industry at large, including improving third party experience in accessing Open APIs published by different providers. This would encourage greater usage and offerings of innovative solutions by third parties, which results in efficiency gains to both customers and businesses alike. Time-to-market can be reduced as third parties are able to rapidly build on existing systems by leveraging on standardised Open APIs. However, the identification of Open APIs to be standardised should take into consideration various factors, including the financial industry's level of readiness to adopt such APIs and the overall benefits arising from such standardisation.

1.4. The Bank has undertaken measures to encourage wider adoption of Open API in the payments arena. In March 2018, the Bank finalised the Interoperable Credit Transfer Framework, a move to encourage the approved operator of shared payment infrastructure and issuers of designated payment instruments to publish Open APIs to facilitate convenient credit transfers and the development of other value-added services.

Open API Implementation Groups: Pursuit of Open API standardisation

1.5. The initiative to identify use cases and further foster the adoption of Open API in the financial sector would be undertaken in close collaboration with the financial industry and other relevant stakeholders. The Bank has moved ahead in the first quarter of 2018 to establish Open API Implementation Groups at industry-level for both banking/Islamic banking and insurance/takaful industries, with representation from select financial technology (fintech) companies. The Open API Implementation Groups, in consultation with the Bank, will identify and develop standardised Open APIs for high-impact use cases.

1.6. In 2018, the focus of the Open API Implementation Groups is to pursue standardisation of Open APIs which would enhance third party developers' access to open data published by banks/Islamic banks and insurers/takaful operators, commencing with product information on SME financing, credit card and motor insurance/takaful products. These open data have been identified based on the following objectives:

(a) further enhance SMEs' access to financing products and services offered by financial institutions;

(b) promoting comparability of motor insurance/takaful products in line with the move towards liberalisation;

(c) facilitate development of fintech to allow consumers to compare a wide range of financial products and services matching their specific needs and circumstances, besides improving experience and providing choices to customers; and

(d) leverage on technology for the provision, distribution and consumption of financial services.

1.7. While open data is, by definition, publicly accessible, there is value in enabling seamless access *via* Open API. This will also be an important testbed to gauge industry reception and adoption in charting the future direction on Open API adoption.

1.8. This policy document outlines recommendations for financial institutions in developing and publishing Open Data API, accompanied with the Open Data API Specifications developed by the Open API Implementation Groups. Financial institutions are therefore encouraged to adopt these specifications to ensure industry-wide publication of standardised Open Data API.

Question 1:

(a) Does your institution plan on publishing Open Data API?

(i) If your answer is yes, what are these APIs?

(ii) If your answer is no, what are the reasons for not publishing Open Data APIs?

(b) What would be the recommended Open Data API Specifications to be developed by the Open API Implementation Groups, other than those on product information on SME financing, credit card and motor insurance/takaful products?

Phased approach towards Open API adoption

1.9. The Bank takes cognisance of the developments in other jurisdictions, where regulators and financial industries alike are considering the need to move towards Open Banking[1], which involves either read and/or write access to bank accounts. This forms part of regulatory effort to widen choices available to financial consumers in relation to satisfying their financial needs. Alongside empowered consumers, seamless access to data holds the potential to promote innovation and further enhance quality of financial services.

[1] For purposes of this Exposure Draft, Open Banking is defined as the use of Open APIs that enable third party developers to build applications and services around the financial institution; and allowing bank to share customers' financial/non-financial information with third parties, with customers' consent.

1.10. However, it is important to weigh these benefits against the associated risks and costs. In particular, careful consideration is necessary in developing the appropriate security controls and governance measures over greater data access and portability, which are part of the tenets of Open Banking. To this end, the Bank plans to issue a Discussion Paper on Open Banking implementation in Malaysia for feedback from the industry and public at large.

1.11. A collaborative partnership is pertinent to reap the benefits of data-driven innovation. Therefore, the Bank welcomes additional proposals from the financial industry players, fintech community as well as any interested parties on other potential use cases that would benefit from standardised Open APIs.

2. Applicability

2.1. This policy document is applicable to financial institutions intending to publish Open Data APIs.

2.2. For avoidance of doubt, the guidance under this Policy Document is not applicable to publication of private API[2] and partner API[3].

3. Legal provision

3.1. The guidance in this policy document is specified pursuant to –

(a) section 266(c) of the Financial Services Act 2013 (FSA); and

(b) section 277(c) of the Islamic Financial Services Act 2013 (IFSA).

[2] refers to APIs that facilitate information flow within an organisation by connecting different databases or systems.

[3] refers to APIs that support interfaces between a data provider and a third party which have entered into business relationships.

4. Effective date

4.1. This policy document comes into effect upon issuance of the final policy document.

5. Interpretation

5.1. The terms and expressions used in this policy document shall have the same meanings assigned to them in the FSA and IFSA, as the case may be, unless otherwise defined in this policy document.

5.2. For the purpose of this policy document:

“API” is a set of protocols that enables the communication between software applications;

“financial institution” refers to –

(a) licensed bank;
(b) licensed Islamic bank;
(c) licensed insurer; and
(d) licensed takaful operator;

“open API” means an API that allows third party access, which may be subject to certain controls by the Open API publisher;

“Open Data API Specifications” refer to the specifications developed by the Open API Implementation Groups, in consultation with the Bank, for industry adoption;

“Open Data API Standards” refer to the standards on Open Data APIs as recommended under this Policy Document for financial institutions;

“open data” refers to publicly available and usable data that is published by financial institutions, including financial product information (i.e. key information on a financial product, such as those provided in product disclosure sheets, which facilitates customers in making informed decisions);

“**Open Data API**” means a “read-only” Open API which allows access to open data; and

“**third party”** refers to any person who uses an Open API published by financial institution, whereby the user is not associated with the financial institution, and may include other financial institutions.

6. Related legal instruments and policy documents

6.1. This policy document must be read together with other relevant instruments and policy documents that have been issued by the Bank, including the following:

(a) Guidelines on the Provision of Electronic Banking (e-banking) Services by Financial Institutions;

(b) Guidelines on Internet Insurance;

(c) Circular on Internet Takaful;

(d) Managing Cyber Risks;

(e) Circular on Preparedness against Distributed Denial of Service (DDoS) Attack; and

(f) Guidelines on Management of IT Environment.

PART B POLICY RECOMMENDATIONS

7. Open Data API Standards

G 7.1 Open Data API Standards comprise of the following:

(a) API architecture standards, as provided under paragraphs 7.3 and 7.4, that outline the recommended design considerations to encourage interoperability across various Open APIs;

(b) recommendations under paragraphs 7.5 and 7.6 on considerations in determining the appropriate data standards; and

(c) security measures recommended under paragraph 7.7 that establish the baseline on security measures as protection against potential security threats, proportionate to the sensitivity of the Open Data API functions.

G 7.2 Financial institutions are encouraged to adhere to the Open Data API Standards in developing Open Data APIs.

API Architecture Standards

G 7.3 Financial institutions are encouraged to adopt the Representational State Transfer (REST) communication protocol/principles and JavaScript Object Notation (JSON) data format.

G 7.4 Financial institutions are encouraged to facilitate conversion from alternative protocols and data formats to REST and JSON respectively.

Data Standards

G 7.5 Financial institutions should consider the following factors in determining data standards to be adopted for publication of Open Data APIs:

(a) data standards recommended by the Implementation Groups which may include available industry standards e.g. Open Financial Exchange (OFX), ACORD or XML; and

(b) appropriateness in meeting the intended business function of the Open APIs.

G 7.6 The Bank recommends for financial institutions that use their own data definitions to publish these definitions online, with sufficient level of detail to facilitate third party understanding and adoption.

Question 2:
Are the recommendations under paragraphs 7.5 & 7.6 sufficient as guidance in determining the appropriate data standard?

Security Standards

G 7.7 Security measures installed by financial institutions in relation to Open Data API should be proportionate to the potential risks. At minimum, financial institutions should put in place the following measures to mitigate cybersecurity risks:

(a) restrict API to only perform interfacing functions and allow pass through of information only;

(b) restrict access to the API configurations to dedicated staff only;

(c) restrict APIs from storing sensitive data such as customer information;

(d) protect the API server with security layers such as firewall and intrusion prevention system (IPS) to mitigate risk of cyber attacks on the financial institutions' interfaced IT systems;

(e) ensure high availability of API service by designing APIs to support efficient processing of information and scalability of functionalities;

(f) undertake secure coding practices of the API such as restricting hard coding of ID and password;

(g) adopt the latest and robust authorisation and authentication protocols adequate for the risks presented by Open Data APIs;

(h) conduct periodic audit and penetration testing on the API infrastructure and configuration setup;

(i) conduct real time monitoring on any suspicious activities at the API;

(j) restrict use of unsecured communications protocols and encryption standards for the API system and communications infrastructure as well as the interfaces; and

(k) all sensitive credentials such as password must be encrypted using latest and most secured standards for example Transport Layer Security (TLS).

> Question 3:
>
> Are the above recommended security standards sufficient in the context of publication of Open Data APIs? Where additional measures are recommended, please provide justification, including identifying potential threats arising from absence of these security measures.

8. Third party governance process

G 8.1 Financial institutions are encouraged to establish basic registration process for third party. However, financial institutions may implement more advanced functionalities for its third-party governance processes, provided it does not create unnecessary barriers for the third party to access the Open Data API.

> Question 4:
>
> (a) Do you find the above recommendations sufficient? If no, why?
>
> (b) If your institution decides additional measures are necessary, please describe them and explain the rationale behind these additional measures.

9. Adoption of Open Data API Specifications and publication of Open Data APIs

G 9.1 Financial institutions are encouraged to adopt Open Data API Specifications recommended by the Open API Implementation Groups for selected open data. These specifications are provided at https://github.com/BankNegaraMY.

G 9.2 Where financial institutions have adopted standards or specifications on Open Data APIs which differ from those recommended by the Open API Implementation Groups, financial institutions are advised to assess potential impact to third party adoption and security arising from these differences, if any. Financial institutions are encouraged to take measures to resolve potential frictions or gaps that may impede implementation or adoption, as appropriate.

Question 5:

(a) If your institution has already adopted different specifications/standards in developing Open Data APIs, please provide details on these specifications/standards and elaborate on the rationale for adoption.

(b) Please indicate the potential issues in updating your institution's Open Data API using the recommended standards or Open Data API Specifications.

G 9.3 To facilitate third party adoption, financial institutions are strongly encouraged to publish detailed API documentation online to accompany the published Open Data APIs.

G 9.4 Financial institutions are encouraged to define and disclose key performance metrics of the published Open Data APIs, such as response time, API availability/uptime, performance throughput, invocation quota/ throttling limit.

G 9.5 Open Data API Specifications may be revised periodically to address issues or to enrich the Open API's functionalities. Financial institutions are encouraged to ensure the published Open Data APIs are consistent with the latest version of Open Data API Specifications, within 2 months of revision.