Open Application Programming Interface Framework for the Insurance Sector in Hong Kong

Insurance Authority

Publication Date: 18 September 2023

Table of Contents

I. INTRODUCTION

Background

1. The insurance industry is becoming increasingly reliant on digitalization to boost efficiency, streamline procedures and reduce operating expenditure. Against this backdrop, Open Application Programming Interface[1] ("API") has been cited as one of the most popular transformational tools[2].

2. The Insurance Authority ("IA") is promulgating the Open API Framework ("Framework") with a view to fostering a vibrant ecosystem and spurring the development of Insurtech in Hong Kong. The Framework aims at enhancing data exchange, data openness and data connectivity, leading ultimately to the availability of innovative and affordable products for the general public.

3. A working group comprising representatives drawn from authorized insurers, consulting firms, technology companies and Fintech communities was formed by the IA to guide its deliberations, whose feedback and suggestions have been incorporated into the Framework where appropriate.

Objectives

4. The objectives of the Framework are to:

   a) encourage sharing of information to speed up innovation, connectivity and efficiency in the insurance sector;

   b) provide guidance and facilitation for development and implementation of Open API applications;

[1] API is a programming approach to facilitate exchange of information and execute instructions between different computer systems. Open APIs in turn refer to APIs that allow an organization (e.g. authorized insurer) to open up its IT systems and internal data for access by third-party service providers or their counterparts in an open and documented manner. The third-party access is not without restrictions, and system owners are expected to put in place adequate controls in areas such as vetting, data security and protection of policyholders.

[2] Findings of an industry-wide survey jointly conducted by the Insurance Authority and the Hong Kong Federation of Insurers.

c) create an environment conducive to collaboration between authorized insurers, third-party service providers ("TSP")[3], other commercial entities and financial regulators;

d) capture emerging business opportunities (e.g. cross-boundary business) and pioneer open insurance[4]; and

e) elevate global competitiveness of the insurance sector and dovetail with international trends in the delivery of insurance services.

II. OPEN API FRAMEWORK

Applicability

5. This Framework should be observed by all authorized insurers when they deploy Open API for business operations or delivery of products and services. The same applies to licensed insurance intermediaries seeking collaboration with authorized insurers as TSPs.

6. The Framework should be read in conjunction with relevant provisions of the Insurance Ordinance (Cap. 41) and rules, codes, circulars and guidelines issued by the IA or other regulatory bodies, including the Guideline on the Use of Internet for Insurance Activities (GL8), Guideline on Outsourcing (GL14) and the Guideline on Cybersecurity (GL20).

Guiding Principles

7. The Framework has been developed based on the following guiding principles:

a) facilitating and encouraging adoption of Open API in the insurance sector before considering any mandatory measures;

[3] In this context, TSP refers to any persons, companies, or entities that perform paid or non-paid services for the authorized insurer. The TSP may be a unit of the same authorized insurer (e.g. head office or overseas branch), an affiliate of the authorized insurer or an independent third party located in Hong Kong or from overseas.

[4] Open insurance involves accessing and sharing of data through APIs to foster digital and open relationships between insurance practitioners and their counterparts.

b) taking advantage of Open API to enhance system interfaces and data exchange, creating an environment that fosters innovation and service improvement for the benefits of customers and financial institutions;

c) encouraging market participants to partner with TSPs to leverage on Open API to develop innovative insurance products and services;

d) affording authorized insurers with the flexibility to integrate Open API into their business strategies, while observing industry standards and regulatory instruments issued by the financial regulators; and

e) drawing reference to similar papers and guidelines issued by local[5], national and foreign financial regulators with feedback and suggestions from industry stakeholders incorporated as appropriate.

Possible Functions of Open API

8. To showcase practical examples of how Open API can be gainfully deployed, a list of use cases is at **Appendix 1**. Some possible functions in respect of the insurance sector are outlined below -

Categories	Possible functions
Products and services	• Retrieve product details (e.g. product IDs, names, features, coverage, premium, terms and conditions) • Product types include - (a) endowment, unit-linked, universal life, whole life, term life, accident & health, group life insurance; and (b) accident & health, motor vehicle, aircraft, ships, property damage, employees' compensation, travel, medical, home and other general liability insurance.

[5] Such as the Hong Kong Monetary Authority and its Open API Framework for the Hong Kong Banking Sector at https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2018/20180718e5a2.pdf

Categories	Possible functions
	• Retrieve information used for product underwriting purpose (e.g. medical history, age, gender and financial condition)
Customer acquisition, sales and distribution	• General marketing and URLs redirection • Process application requests • Tracking of policy application status • Suitability assessment
Policy administration and servicing	• Retrieve policy details • Process changes requests
Retrieval of historical data on performance of products	• Retrieve information on fulfillment ratios and historical crediting interest rates of universal life insurance products
Claims handling	• Process and management of claims
Others	• Retrieve information on customer loyalty and rewards programmes • Post-sale services and assistance • Retrieve information from other financial institutions (e.g. banks) for insurance services • Management of insurance intermediaries

Open API Standard

9. Standardization of Open APIs brings additional security for end-users, lesser duplication of functionalities and lower cost. Nonetheless, after consulting the working group and reviewing the experience of other jurisdictions, we prefer not to prescribe an industry-wide standard at this stage but to urge authorized insurers to draw reference from the "Sample Checklist of Risk Assessment and Risk Mitigation Controls" at **Appendix 2** when pursuing the adoption of Open API.

Architecture, API, Data and Security Standards

10. Architecture refers to how websites, digital platforms or applications of the partnering TSPs connect to an authorized insurer via Open API. The most frequently used communication protocols are Representational State Transfer

("REST") and Simple Object Access Protocol ("SOAP"). For REST-based APIs, JavaScript Object Notation ("JSON") is the more prevalent data format and extensible Markup Language ("XML") is used for SOAP-based APIs. We recommend the use of REST with JSON as data format.

11. For the API standard, reasonable versioning requirements supporting different releases, possessing sound backward compatibility for releases and allowing flexibility for functional errors should be applied.

12. Authorized insurers should publish data definitions, as well as technical and engagement details on how to plug into their Open API applications using common protocols like Open API Specification (i.e. Swagger). No restriction will be placed on own data descriptions, so long as they are made public.

13. Authorized insurers should have change management procedures and proper disclosure to enhance transparency and should install a mechanism for users to report issues, incidents or failures.

Security Standards

14. Security standards governing authentication, integrity, confidentiality and authorization should be established for Open API applications.

15. Safeguards on keys or access tokens[6] should be available to avoid the risk of unauthorized access, complemented by encryption and management oversight.

16. Authorized insurers should apply a risk-based authentication approach and grant access privilege to their partnering TSPs only by customer consent.

17. Some recommended security protection technologies are set out below:

[6] An access token is used to authorize access to API to exchange confidential data.

Protection Required	Recommended Technology
Authentication of websites managed by authorized insurers and partnering TSPs	X.509
Integrity and confidentiality of data	Transport Layer Security
Authentication of customers	Own methods
Authorization of customer	OAuth 2.0

18. Authorized insurers should adhere to requirements prescribed in regulatory instruments concerning secure use of technology and review the architecture, API, data and security standards from time to time.

TSP Governance and Risk Management

19. Authorized insurers should impose requirements on their partnering TSPs to address internal controls, due diligence, onboarding, monitoring, demarcation of roles and responsibilities, accountability, data protection, security, customer protection, operational/infrastructure resilience as well as incident reporting and handling. These requirements should be fair, reasonable and commensurate with the risks involved.

20. Authorized insurers should conduct risk assessment in line with the nature of engagement with their partnering TSPs that are appropriate, proportionate, adequate and comprehensive but not overly restrictive to other TSPs.

Contractual Arrangement

21. Authorized insurers and partnering TSPs should ratify bilateral agreements to clarify accountabilities, making clear about the rights and liabilities of data owners and users.

Due Diligence for a TSP

22. Authorized insurers should conduct due diligence on the partnering TSPs with reference to their business profile, qualifications and financial conditions.

Governance, Risk Management and Control

23. To cope with the risks arising from implementation of Open API, authorized insurers and partnering TSPs should have proper risk governance frameworks and processes, including policies and procedures for risk management and internal control systems.

24. Authorized insurers and partnering TSPs should conduct regular assessments and take appropriate risk mitigating measures spanning across areas that include cybersecurity, system resilience, data breach or privacy, data misuse, liability and financial crime.

Technology Risk Management and Cyber Security

25. Authorized insurers should ensure that the partnering TSPs have in place risk management policies and procedures commensurate with the scale and complexity of their business profile. These policies and procedures should cover at least IT controls, system availability and stability, system testing, system and data encryption, system change, system monitoring and security, cyber security controls as well as incident response and management.

Data Protection

26. Customer data on insurance policies and services inevitably contain sensitive personal information such as medical history, age, gender, religion and financial condition. It is therefore important for authorized insurers to impose restrictions on the collection, use, retention and disposal of such information by their partnering TSPs.

27. The partnering TSPs must state explicitly that the collection of customer data is not conducted by the authorized insurer and reveal the related purpose. Access by third parties to the data so collected should be done with explicit and informed consent by the customers. Authorized insurers and partnering TSPs should abide by applicable laws and guidelines on protection of personal data and customer confidentiality (e.g. the Personal Data (Privacy) Ordinance, Cap. 486).

Fair Treatment of Customers and Consumer Protection

28. Authorized insurers should uphold the principle of "treating customers fairly" and ascertain that their partnering TSPs have effective policies to safeguard customers against mishaps associated with products and services provided through Open API.

29. Authorized insurers and partnering TSPs should assess and reduce risks and liabilities posed to their customers by Open API. Some typical examples include cybersecurity threats, fraudulent websites and misuse of personal data. Equitable settlement arrangements should be conveyed to customers in the events of losses or disputes, supported by a fair and responsive mechanism for handling complaints and redressing grievances.

System Resilience and Contingency Management

30. System resilience induces trust and confidence. Authorized insurers should design their IT configurations with due care on availability and recoverability by taking reasonable, appropriate, timely and sufficient steps to maintain the resilience of systems run by their partnering TSPs.

31. Authorized insurers and partnering TSPs should draw up viable Business Continuity Plans for their Open API applications to strengthen the ability of ongoing operation and limit losses in the event of severe disruption.

Ongoing Monitoring of Partnering TSPs

32. Authorized insurers should continuously monitor their partnering TSPs to ensure compliance with this Framework and other regulatory instruments. Significant incidents (e.g. data leakage) should be reported promptly by the partnering TSPs.

Open API Repositories

33. To improve transparency and consumer protection, authorized insurers should provide information about their Open API applications, partnering TSPs, relevant Open API-facilitated products and services that are accessible by TSPs and other interested parties on their own websites and/or other online repositories or central registers.

34. Authorized insurers and partnering TSPs should remind their customers to perform prior checking to avoid accessing fraudulent websites or falling victim to scams. Authorized insurers should actively detect fraudulent websites or scams where an entity claims to be a partnering TSP, pretends to be associated with a partnering TSP or authorized insurers and issue prompt notifications when such discoveries are made.

Future Development

35. Since successful use cases are important in showcasing the potential scope of Open API adoption, the IA will engage in close dialogue with the industry to enrich the range of use cases and partner with other financial regulators to nurture cross-sector and cross-boundary applications.

36. The IA will work together with industry stakeholders to pan out a healthy and sustainable development of Open API in the insurance sector. The IA will also keep track with evolving market dynamics and capture opportunities such as data connectivity in the Guangdong-Hong Kong-Macao Greater Bay Area.

37. The IA will review this Framework every two years and may, at an appropriate juncture, issue a new guideline on the use of Open API to achieve uniformed compliance with baseline requirements prevailing at the time.

Commencement

38. This Framework shall take effect from 18 September 2023.

Appendix 1

Open API Use Cases

A. iAM Smart

1. "iAM Smart" was launched by Office of the Government Chief Information Officer ("OGCIO") in 2020 to provide local residents with a digital identity and authentication to conduct on-line transactions as well as receive updates from the Government using their mobile devices. Over 1 million registered users could access more than 160 online services through this platform.

2. The Pilot Sandbox Programme for iAM Smart was subsequently rolled out by the OGCIO in 2020 for financial institutions to test their API applications under a production-setting environment. Up to now, 46 authorized insurers and licensed insurance intermediaries have taken part in this initiative.

B. Customer Experience

1. Favourable customer experience is essential for persistence and brand loyalty. Instead of focusing on frontline interaction, some authorized insurers have gone one step further to foster financial inclusiveness and a vibrant ecosystem. Meanwhile, Phase III of the HKMA Open API Framework[7] opens up bank account information such as account balance, credit card balance, transaction records and credit limit change for real-time access.

2. At present, when one purchases a policy and pay premiums to the insurer via a bank, it may take several days for the insurer to issue acknowledgement causing delay in provision of coverage to the policyholders. An authorized insurer took advantage of Open API to obtain account balance from the bank in real time to expedite the issuance of new policies.

[7] HKMA - Open Application Programming Interface for the Banking Sector at https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/open-application-programming-interface-api-for-the-banking-sector/

C. Commercial Data Interchange ("CDI")

1. The CDI went live in October 2022 for financial institutions to retrieve data from commercial entities, particularly small and medium-sized enterprises, with the help of API to refine processes like Know-Your-Customer, product design, customer acquisition and risk management. As providers and users of data, authorized insurers could derive enormous benefits from synergizing with participants of the CDI ecosystem.

D. Product Innovation

1. The onset of COVID-19 has severely affected the mortgage repayment ability of property owners and credit quality of loan portfolios held by the lenders. An authorized insurer adopted Open API to gain real-time access of personal data from the partnering banks to spearhead a marketing drive on innovative health and accident products, shielding mortgagors from possible financial strains posed by unemployment, sickness and death.

Appendix 2

Sample Checklist of Risk Assessment and Mitigation Controls

The IA has prepared a checklist of risk assessment and mitigation controls in relation to Open API adoption for reference by the authorized insurers and partnering TSPs as follows -

A. Governance and Risk Management	
1.	**Bilateral Agreement** Bilateral agreement ratified between authorized insurer and partnering TSPs.
2.	**Due Diligence** A summary of due diligence records on the partnering TSPs, including detailed assessment of their business profiles, qualifications and financial conditions. The summary should also cover onboarding checks and risk-based reviews of the partnering TSPs.
3.	**Internal Controls** Internal controls put into place by the authorized insurer and partnering TSPs that include due diligence, onboarding, monitoring, demarcation of roles and responsibilities, accountability, data protection, security, customer protection, operational/infrastructure resilience as well as incident reporting and handling.
4.	**Technology Risk Management and Cyber Security** Policies and procedures on technology risk management of the authorized insurer and partnering TSPs that include IT controls, system availability and stability, system resilience, system testing, system and data encryption, system change, system monitoring and security, cyber security controls as well as incident response and management.
5.	**Data Protection** Guidelines of the authorized insurer and partnering TSPs on collection, use, retention and disposal of customer data and information.

A. Governance and Risk Management	
6.	**Business Continuity** Business Continuity Plan of the authorized insurer and partnering TSPs may contain a crisis management process, call-out trees, a business resumption plan, a technology recovery plan and an alternate site plan.
7.	**Ongoing Monitoring** Documentation on assessment, monitoring and control on the partnering TSPs to ensure their compliance with this Framework and other relevant guidelines.
B. Sound Consumer Protection Practices by Authorized Insurers	
1.	**Fair Treatment of Customers** A copy of policies and procedures put into place by the authorized insurer and partnering TSPs on fair treatment of customers.
2.	**Partnering TSPs** A list of the partnering TSPs and corresponding in-scope products/services uploaded onto the website of the authorized insurer and/or online repositories.
3.	**Fraudulent Claims** A summary of procedures laid down by the authorized insurer and the records of monitoring websites purporting to be operated by the partnering TSPs or false claims of collaboration made by other TSPs.
4.	**Complaint Handling** A copy of policies and procedures on handling and resolution of complaints by the authorized insurer that should include a proper channel for customers to redress their grievances in a timely, fair and efficient manner.