



Project FINI

API Workshop #1

Raymond Lee
Leo Ho

Innovation and Data Lab
Post-Trade Systems

23 June 2022

HKEX
香港交易所

Disclaimer

The information contained in this document is for general informational purposes only and does not constitute an offer, solicitation, invitation or recommendation to subscribe for or purchase any securities, or other products or to provide any investment advice or service of any kind. This document is solely intended for distribution to and use by professional investors. This document is not directed at, and is not intended for distribution to or use by, any person or entity in any jurisdiction or country where such distribution or use would be contrary to law or regulation or which would subject Hong Kong Exchanges and Clearing Limited ("HKEX") to any registration requirement within such jurisdiction or country.

This document contains forward-looking statements which are based on the current expectations, estimates, projections, beliefs and assumptions of HKEX about the businesses and the markets in which it and its subsidiaries operate. These forward-looking statements are not guarantees of future performance and are subject to market risk, uncertainties and factors beyond the control of HKEX. Therefore, actual outcomes and returns may differ materially from the assumptions made and the statements contained in this document.

Where this document refers to Shanghai-Hong Kong Stock Connect and/or Shenzhen-Hong Kong Stock Connect (together, the "Stock Connect" programs), please note that currently, access to northbound trading is only available to intermediaries licensed or regulated in Hong Kong; southbound trading is only available to intermediaries licensed or regulated in Mainland China. Direct access to the Stock Connect is not available outside Hong Kong and Mainland China.

Where this document refers to Bond Connect, please note that currently, access to northbound trading is only available to foreign investors that are able to trade onshore bonds on the China Foreign Exchange Trade System & National Interbank Funding Centre.

Although the information contained in this document is obtained or compiled from sources believed to be reliable, HKEX does not guarantee the accuracy, validity, timeliness or completeness of the information or data for any particular purpose, and shall not accept any responsibility for, or be liable for, errors, omissions or other inaccuracies in the information or for the consequences thereof. The information set out in this document is provided on an "as is" and "as available" basis and may be amended or changed. It is not a substitute for professional advice which takes account of your specific circumstances and nothing in this document constitutes legal advice. HKEX shall not be responsible or liable for any loss or damage, directly or indirectly, arising from the use of or reliance upon any information provided in this document.



Summary

HKEX plans to roll out FINI in **Q2 2023**, which will include an API Gateway for market participants to automate different types of IPO workflows.

This workshop serves as a **primer** for market participants on how to set up and use the **FINI API Gateway**.

01

Introduction

02

API Access Setup

03

End-to-end Encryption

04

API Requests / Responses

Introduction





FINI API Gateway

The **FINI API Gateway** offers a channel for market participants automate different types of IPO workflows using JSON endpoints.

**Enquire IPO
Reference
Data**

[illegible]

```
{
  "code": "0",
  "message": "",
  "data": [
    {
      "ipId": "1234",
      "stkCode": "9988",
      "isin": "KYG017191142",
      "status": "25",
      "ipId": "1235",
      "stkCode": "9633",
      "isin": "CNE10004272",
      "status": "30",
      "ipId": "1236",
      "stkCode": "9618",
      "isin": "KYG620881014",
      "status": "45",
      "ipId": "1237",
      "stkCode": "6618",
      "isin": "KYG5074A1004",
      "status": "60",
      "ipId": "1238",
      "stkCode": "1024",
      "isin": "KYG532631028",
      "status": "70",
      "totalSize": "5",
      "timeStamp": "2021-08-25 16:22:13",
      "nextCursor": "1239",
      "exception": {}
    }
  ]
}
```

Obtain 5 latest active IPOs

Manage EIPO Subscriptions

[illegible]

```
{
  "code": "0",
  "message": "",
  "data": {
    "requestID": "1",
    "recordID": "1234567890123456A",
    "exception": []
  },
  "totalSize": 1,
  "timestamp": "2021-08-26 09:13:22",
  "exception": []
}
```

Add 1 subscription to a specific IPO

**Confirm /
Reject EIPO
Funding**

[illegible]

```
{
  "code": "0",
  "message": "",
  "data": {
    "transactionRef": "6398340114921",
    "preFundingStatus": "20",
    "exception": [],
    "transactionRef": "6398340114936",
    "preFundingStatus": "20",
    "exception": [],
    "transactionRef": "6398340114947",
    "preFundingStatus": "20",
    "exception": [],
    "transactionRef": "6398340114959",
    "preFundingStatus": "20",
    "exception": [],
    "transactionRef": "6398340114972",
    "preFundingStatus": "30",
    "exception": [],
    "totalSize": 5,
    "timestamp": "2021-09-30 11:55:21",
    "exception": []
  }
}
```

Confirm the funding of 5 EIPO subscriptions lists



API Access Setup



API Access Setup

Pre-requisites

To access the API Gateway, agent and machine profiles must be set up with the following items:

<u>Item</u>	<u>Used in this demo</u>
A web browser to access the open internet	Google Chrome
An algorithm to generate JSON Web Keys (JWK)	[not within demo scope]
An algorithm to sign JSON Web Tokens (JWT)	Postman
An application to make REST API calls	Postman

 The applications used within this presentation are non-exhaustive. Users are recommended to implement applications based on their firms' technology stacks.



API Access Setup

Step 1: Generate two sets of public keys

Each public key should comprise of:

- a JSON Web Key (JWK) (**1**); and
- an expiration date, in epoch format, for the public key (**2**)

Public Key (example)

```
{
  "keys": [
    {
      "kty": "RSA",
      "e": "AQAB",
      "use": "sig",
      "kid": "ut6EVm95XKsYgZo_hot_bWorUi6hT1ihh8F15GxAo",
      "alg": "RS256",
      "n": "g-LeVFNY9jfrAVY8YW1ORvFjVgZcu8l48n2YzFXksxGvDIQY058RfSjBjRMDxYIEtN3HYHac-j03uydVrin9LnH_jQgCeRSWQswZlJ8_qfPfdkGxOMGDKJuWN3cdulUIZH5pBaQaqZ9Bn7xhgbeXCZn1VWvch6_t61fv36obnKR8tkZqglGphoeijf77rYZ9PcXsU_Owa4B7RJIA1clb6o2pj2YpGHBRIIOtRlhoaU73zsqK78j3ryNolf0XBIMDERDQrTKWyxT0LM254bgUhnGg9pPOIWQYn0uz7BSpaHNcEJWX3rYeqool0juwYXHupG_HC-nRq_mCQ",
      "exp": 1672491599
    }
  ]
}
```

The image shows two browser windows. The top window is 'mkjwk.org', which generates a JSON Web Key (JWK) from input parameters. The bottom window is 'epochconverter.com', which converts a date and time (2022-12-31 23:59:59 PM GMT) into an epoch timestamp (1672491599). Arrows indicate the flow of information from the tools to the example JWK.

Illustrative examples *

- 1 This JWK is generated from <https://mkjwk.org/>, based on the following parameters:

Key Type	RSA
Key Size	2048
Key Use	Signature
Algorithm	RS256
Key ID	SHA-256 hash value of JWK

- 2 This expiration date is set at **2022-12-31 23:59:59**, generated from <https://www.epochconverter.com/>.

Note: the expiration date must be less than a year away from the timestamp at which the agent / machine profiles are created.



* These are online tools are for illustrative purposes only. Users are strongly recommended that these steps should be implemented based on their firm's internal technology stacks

API Access Setup

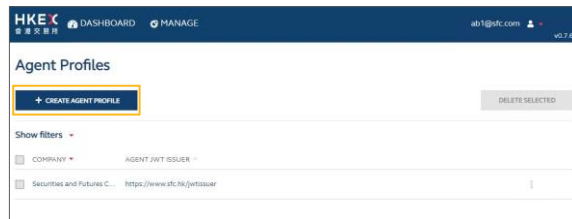
Step 2: Register public keys on Client Connect

Each set of keys can be used to register a machine and agent profile on the Access Management section of the HKEX Client Connect website (<https://connect.hkex.com.hk>)*:

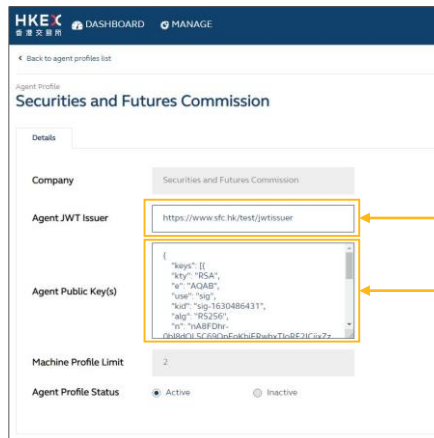
A | Access Management:



B | Agent / Machine Profile Management:



C | Agent / Machine Profile Creation:



Public Key (example)

```
{
  "keys": [
    {
      "alg": "RS-256",
      "e": "AQAB",
      "kty": "RSA",
      "n": "ySMspblxXSueMvtrx3NAhOWKrLYWAHEAfeHkyiRG2Hr4QJdlcJuQur9ax46LxeHemx30OmaEhKw2rqwy3sf3NRKwS9j4Wb2xWAoM2MVQ2AwhwOVsHLnkJzCfBgGtU1MG_gA4ZcZgzR0UB4GYlJNalDyEdCxmYeKSq4FagtvSiCIYTnL4L5oVfncpEQ4uh9Sq4jWjPhp5oVwFbpgXT57jlrU771vzmlT6oFUpBnXKtWfmcLpU2fgaxsTi4_2Tbm1rK3AVk3hGfmd11d_zDCOz61CJsRtHckAXcx8Z_3sykUqcuS7W3CyhnDOdxnY3nkyfHSLpP-TO3yJGHO0bpQ",
      "use": "sig",
      "exp": "1686660833",
      "kid": "9751bcffb73e559ca8cbd5347ce9d40f09562c56022035386383236eaa2c087"
    }
  ]
}
```

⚠ Separate sets of public keys must be used to register the agent and machine profiles on Client Connect.



* The manage machine and agent profile functions will be deployed on the HKEX Client Connect website during the market-wise testing phase. It is currently NOT accessible by public internet, please do not attempt accessing it.

Step 3: Obtain an access token through an API call

Access tokens may be obtained through a POST API call:

API call (example)

```
curl -X POST -k -d "grant_type=urn:ietf:params:oauth:grant-type:jwt-bearer"  
"assertion=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJhdWQiOiJodHRwczovL2NmNm5lY3QyQWUudTJjC5oa2V4LmNvbS5oazo0NDMvbm5BblhmFtL29hdXR0Mi9ldS9hY2NiZnlic3RpdG9rZW4ILCJpc3MiOiJodHRwciovL3NmYy5jb2UuaGVzdGVzdC9qd3Rpc3N1ZXliLClleHAiOjE2NTUyMTMwMzMslmN1Y1l6ImhrZUhhcGkifQ.pw5wXNAdxHGK37pGUKrhpuKLXJw4Ni9T78tNgwwWbGc"  
"client_assertion_type=urn:ietf:params:oauth:assertion-type:jwt-bearer"  
"client_assertion=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJhdWQiOiJodHRwciovL2NmNm5lY3QyQWUudTJjC5oa2V4LmNvbS5oazo0NDMvbm5BBlhS9hbS9vYXN0DlvcZUxvYWVjZWN1ZHNzX3Rva2VulmlwaXNzIjoiaHR0cHM6Ly9oc2JlLmNvbS5oay9icm9raW5nL2p3dGlzc3VicislmV4C6lMTY1NDg4MjU0MCwic3ViIljoiaGtleGFwaSJ9.e5oQWFP6NTxZuiy5ftb2Y1JTlw0MtT9-CwdEd8z78LBQ" https://connect-am.u2cp.hkex.com.hk:443/openam/oauth2/eu/access_token
```

Notes

- For **grant_type** and **client_assertion_type**, always use input “**urn:ietf:params:oauth:grant-type:jwt-bearer**”
- For **assertion**, it should be the RS256-signed value of the agent profile payload
- For **client_assertion**, it should be the RS256-signed value of the machine profile payload
- The URI used in the testing environment, a different address may be used for production

```
{  
  "aud": "https://connect-  
am.u2cp.hkex.com.hk:443/openam/oauth2/eu/access_token"  
  "iss": "https://www.sfc.com.hk/test/wissuer",  
  "exp": "1672531199",  
  "sub": "CP00010"  
}
```

RS256→

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJhdWQiOiJodHRwciovL2NmNm5lY3QyQWUudTJjC5oa2V4LmNvbS5oazo0NDMvbm5BblhmFtL29hdXR0Mi9ldS9hY2NiZnlic3RpdG9rZW4ILCJpc3MiOiJodHRwciovL3NmYy5jb2UuaGVzdGVzdC9qd3Rpc3N1ZXliLClleHAiOjE2NTUyMTMwMzMslmN1Y1l6ImhrZUhhcGkifQ.pw5wXNAdxHGK37pGUKrhpuKLXJw4Ni9T78tNgwwWbGc
```

Field	Note
aud	The URI used in the testing environment, a different address may be used for production
iss	Agent JWT Issuer value as registered in Agent Profile in Client Connect
exp	Specifies the expiration time. This is the Unix epoch time. Must be less than 30 minutes from current system time
sub	The user's Company ID in Client Connect

```
{  
  "aud": "https://connect-  
am.u2cp.hkex.com.hk:443/openam/oauth2/eu/access_token"  
  "iss": "ec1a3544-ac1a-4adf-9d7a-9d82a4a597ad",  
  "exp": "1672531199",  
  "sub": "ec1a3544-ac1a-4adf-9d7a-9d82a4a597ad"  
}
```

RS256→

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJhdWQiOiJodHRwciovL2NmNm5lY3QyQWUudTJjC5oa2V4LmNvbS5oazo0NDMvbm5BblhmFtL29hdXR0cHM6Ly9oc2JlLmNvbS5oay9icm9raW5nL2p3dGlzc3VicislmV4C6lMTY1NDg4MU0Mcwic3ViIljoiaGtleGFwaSJ9.e5oQWFP6NTxZuiy5ftb2Y1JTlw0MtT9-CwdEd8z78LBQ
```

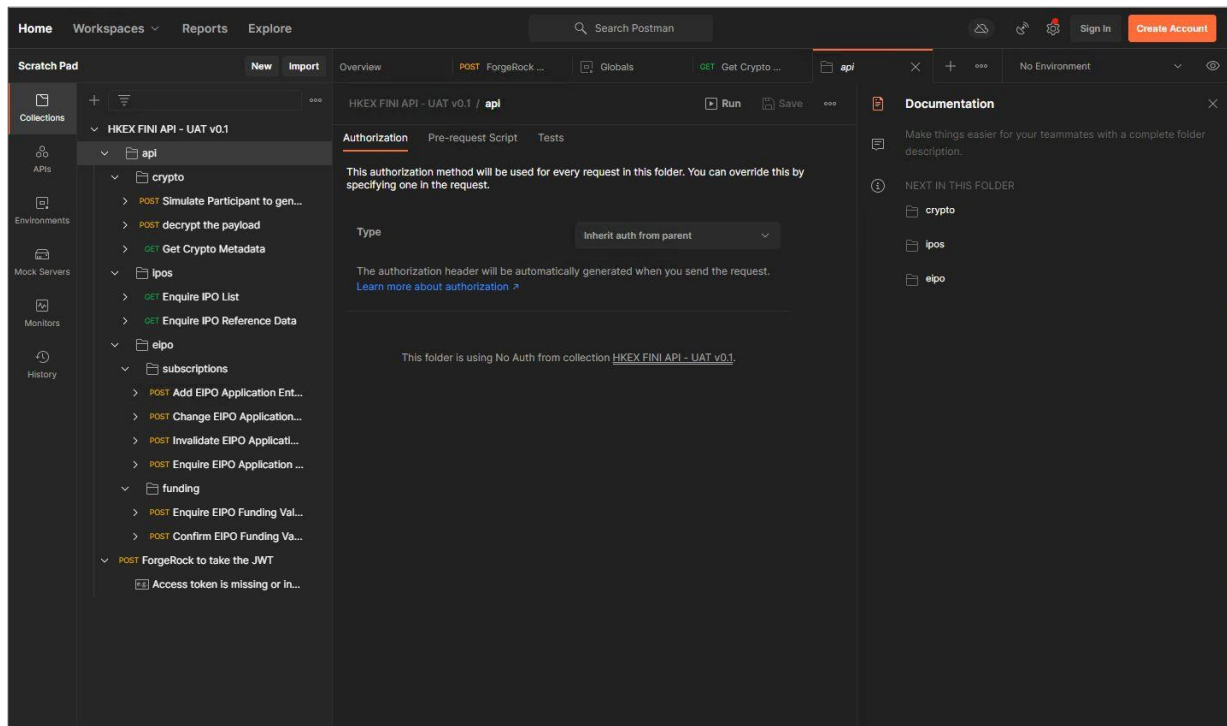
Field	Note
aud	The URI used in the testing environment, a different address may be used for production
iss	Machine Profile UUID. Machine Profile UUID is system generated ID of Machine profile.
exp	Specifies the expiration time. This is the Unix epoch time. Must be less than 30 minutes from current system time
sub	Machine Profile UUID. Machine Profile UUID is system generated ID of Machine profile.

 Access tokens expire every 30 seconds and must be refreshed to operate the FINI API endpoints.



API Access Setup

Illustrative demo



End-to-end Encryption



End-to-end Encryption

Pre-requisites

End-to-end encryption / decryption must be adopted for API requests / responses involving Personal Identifiable Information (PII). This applies to following data fields across EIPO subscription-related API endpoints:

- Type of identification held by the applicant (idType)
- Issuing authority of the applicant's identification document (idCountryJurisdiction)
- ID number of the applicant's identification document (idNum)
- Full English name of the applicant (fullNameEng)
- Full Chinese or non-English name of the applicant (fullNameChi)

Item

Used in this demo

An algorithm to generate random and pseudorandom numbers

Java (library: SecureRandom)

An algorithm for AES-256, RSA and HMACSHA256 encryption / decryption

Java (library: Crypto)

An application to make REST API calls

Postman

 **The applications used within this presentation are non-exhaustive. Users are recommended to implement applications based on their firms' technology stacks.**

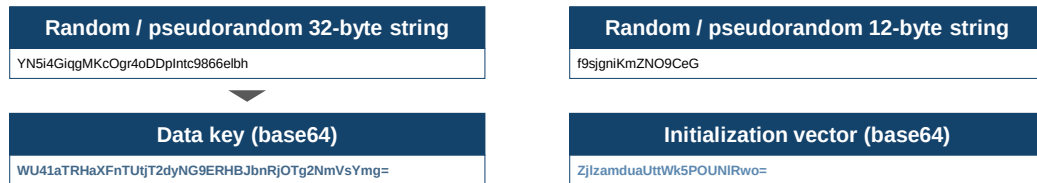




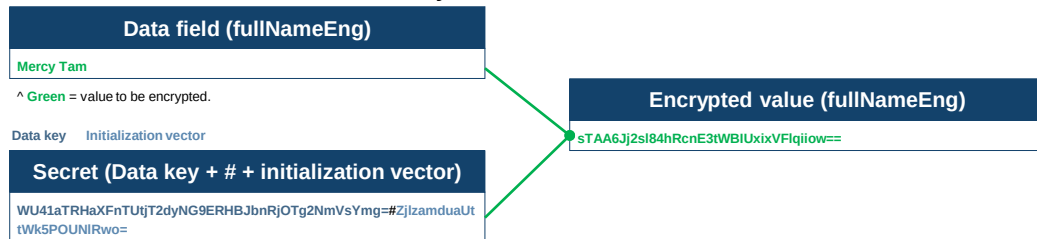
End-to-end Encryption

Step 2: Generate data key and initialization vector to encrypt data fields

Both fields should be generated using random or pseudorandom algorithm, then encoded in base64 format:



The concatenation of the data key and initialization vector should then be used as the secret key for encryption:



Configuration	Value
Algorithm	AES (256 recommended)
Mode	GCM
Padding	NoPadding

A "%enc_%" prefix should then be appended before the encrypted value:



Step 3: Submit the encrypted API request with HTTP headers

API request (example)

[illegible]

Notes

- For **Authorization**, it should be the JWT access token
- For **X-FINI-ENCRYPTED-KEY**, it should be the concatenation of the **data key** and **initialization vector** (delimited by #), encrypted using the publicKey from **Step 1**
- For **X-FINI-REQUEST-ID**, it should be a GUID with no hyphens
- For **X-FINI-TIMESTAMP**, it should be the system local timestamp + time difference from **Step 1**
- For **X-FINI-SIGNATURE**, it should be the concatenation of the encrypted fields, **X-FINI-REQUEST-ID** and **X-FINI-TIMESTAMP**, encrypted using the data key
- The URI used in the testing environment, a different address may be used for production

Data key

Initialization vector

WU41aTRHaXFnTUtjT2dyNG9ER
HBjbnRjOTg2NmVsYmg=#Zjizam
duaUttWk5POUNIRwo=

RSA/None/PKCS1Padding

Hajp922mwdB98nsit7g5e1actVFYfgeYieOQlaV1pCmXVJF
K8luWuHJ3ZfRt11N0c-waFqQwonylYrMnqUGnIEfmhx6
+rdQ5Vq2KjZ0rGPXewRntimOg1SckfmMQfZE9B8R0A6
vIbC0X515PFZjzPXCmF1fjGJeScCTxpcmV4yLaYrLnV
E6kpXl3GCec2suNSHJieJdXVJO86ZAsJ6hIRkOB+zn0
YfReX6g7KwfwrtLVj7Y1zYfMBAF8JuyFWA0lt6gNrmG
wO/oD0KA47gg0GXSDWNsOGd4Shnm72c7rFGoDTSvlMn
X9dN+rizr2K3KXdfUw74L Srdidm

— This is what a Globally Unique Identifier (GUID) without hyphens looks like. A new GUID should be generated for every new request.

cbbfb2afa2094b14a7c6b66a0a399
034

Encrypted payload

X FIN REQUEST IS

X-FINI-REQUEST-IL

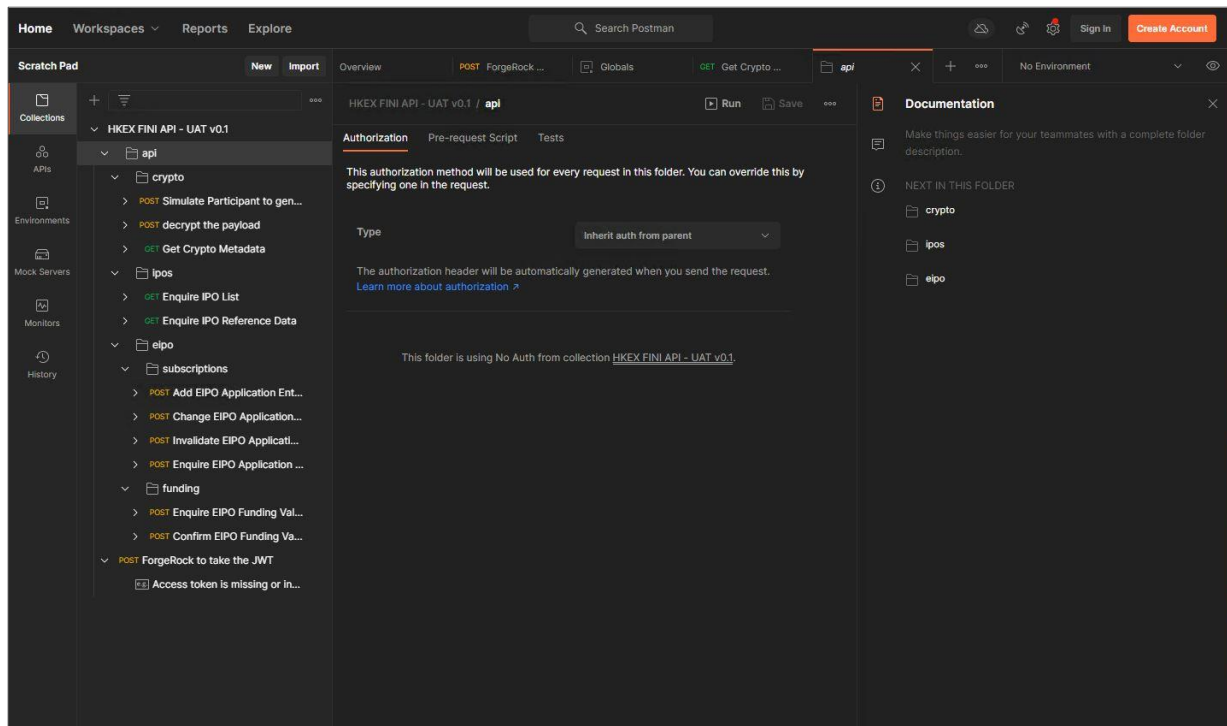
```
{
  "data": {
    "requestId": "1",
    "ipId": "1",
    "idList": [
      {
        "idType": "%cnc",
        "leafPkNon3z1DzDSEkiD9EQgs=",
        "idCountryJurisdiction": "CN",
        "ACvzoas5oJ0xiFScyNbrKxtUgWp==",
        "idNum": "%cnc",
        "BVeZ9H9Pwh7Ee5IE2Ump6bnm/QbkYIusbm%",
        "fullNameEng": "%cnc",
        "CQNGpKkFs1GrHOGOMgJRoJsmXZ+ekEXEz61HEcnPrn",
        "fullNameChi": "%cnc",
        "9r7CYlcb0QZks9K1QLpN3Cz4RjR2YazUwQ==",
        "appQuan": "1000",
        "firmId": "00000",
        "own": "1987-09-25",
        "id-16-4e57-8387-738b7aa757b",
        "id-17-cbbf2afa20a49b1417c6b66a0a399034167253119p"
      }
    ]
  }
}
```

HMACSHA256

1e53e99379e78f6c37b9f7a3803412c2a54dde050494e99
420d781f3ae8861d7

End-to-end Encryption

Illustrative demo



API Requests / Responses



API Requests / Responses

Pre-requisites

To start making API calls to the FINI API Gateway, the following items are required:

Item

An algorithm to format JSON payloads

An application to make REST API calls

Used in this demo

Java

Postman

 The applications used within this presentation are non-exhaustive. Users are recommended to implement applications based on their firms' technology stacks.



API Requests / Responses

Step 1: Select applicable URI

Each API endpoint will have its own applicable Uniform Resource Identifier (URI):

GET	<code>*/api/ipos/list/v1</code>	IPO Reference Data
GET	<code>*/api/ipos/refdata/v1</code>	
POST	<code>*/api/eipo/subscriptions/add/v1</code>	EIPO Subscription
POST	<code>*/api/eipo/subscriptions/change/v1</code>	
POST	<code>*/api/eipo/subscriptions/invalidate/v1</code>	
POST	<code>*/api/eipo/subscriptions/query/v1</code>	
POST	<code>*/api/eipo/funding/confirm/v1</code>	EIPO Funding
POST	<code>*/api/eipo/funding/query/v1</code>	



* The URL to the FINI API Gateway should be appended before the specific endpoint. For the purposes of this presentation and demo, the URL is <https://connect-am.u2cp.hkex.com.hk:443/> (**NOT** accessible by public internet, please do not attempt connecting to it).

Step 2 : Populate the required data fields

For **GET** endpoints, the data fields should be populated within the URI:

Worked example

URI:

GET

*api/ipos/list/v1

← The API endpoint for enquiring the list of IPOs on the system

Data fields:

#	Field	Type	Length	Req.?	Description
1	size	Integer	18	No	Expected page size of the API response. Must be between 1 and 1,000. If null or blank, default as 100.
2	nextCursor	String	20	Yes	Key reference (ipolD) from which the response message should start. "0" should be used to start from the first index.

Pseudo code:

```
curl -X GET -H "Authorization: Bearer  
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIIOiIxMjMONTY3ODkwiibmFtZSI6IkpvaG4gRG9lIiwiaWRtaW4iOiOnRydWUsImp0aSI6IjM5ZDg5MDc0LTl0NWQtNGQxNC04MzQ2LTl2MzQzYjdkIntC2YyIsImhhbmR0MTYxNDAAOTg1MSwiZXhwIjoxNjEOMDUxNDUxfQ.roqk6ISjCMdIQBBf4fd5CvTL1odneLj6LKSGhQxM8c" https://connect-am.u2cp.hkex.com.hk:443/api/ipos/list/v1?size=5&nextCursor=0
```

↑

Please give me the **five latest IPOs** recorded within the system

For **POST** endpoints, the data fields should be populated in a JSON payload:

Worked example

URI:

POST

/api/eipo/subscriptions/query/v1

← The API endpoint for enquiring own EIPO subscriptions

Data fields:

#	Field	Type	Length	Req.?	Description
1	data	Object		Yes	
1.1	ipoID	String	20	No	Must be a valid ipoID from the Enquire IPO List API endpoint. Mandatory if recordID [Field #1.2] = null or blank.
1.2	recordID	Array of String	1000 * 7	No	Must be a valid Record ID within own subscription list, under "Authorised" sub-flow status. Mandatory if ipoID [Field #1.1] = null or blank.
1.3	subFlowStatus	String	2	No	To filter response by a subscription's status, either by "Authorised" (active) or "Invalidated" (removed).
2	size	Integer	18	No	Expected page size of the API response. Must be between 1 and 1,000. If null or blank, default as 100.
3	nextCursor	String	20	Yes	Key reference (recordID) from which the response message should start. "0" should be used to start from the first index.

Pseudo code:

```
curl -X GET -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eYzdWlloilxMjMONTY3ODkwiibwbfZSI6IkpvaG4gRG9lIiwiYWRTaW4iOiYwYXUzIiwiaXNpdG9MDDc0LTIONWQnNGQxNC04MzQ2LTl2MzQyZjdlNTc2YyIsImh0cC" -d '{"data":{"ipoID":"1234"},"size":100,"nextCursor":"0"}' https://connect-am.u2cp.hkex.com.hk:443//api/eipo/subscriptions/query/v1
```

↑

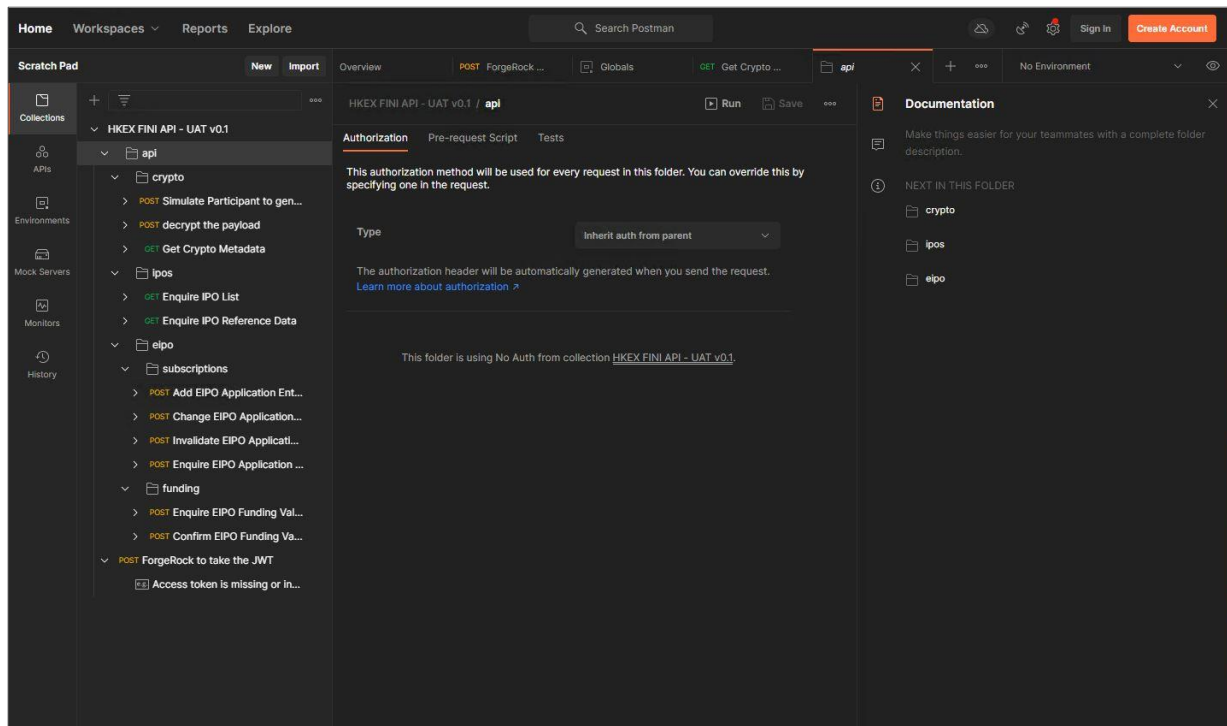
Please give me the **100 latest EIPO subscriptions** for **ipoID 1234**



* The URL to the FINI API Gateway should be appended before the specific endpoint. For the purposes of this presentation and demo, the URL is <https://connect-am.u2cp.hkex.com.hk:443/> (**NOT** accessible by public internet, please do not attempt connecting to it).

API Requests / Responses

Illustrative demo



Thank you.

For further information on HKEX, please go to
hkexgroup.com and **hkexnews.hk**

For further information on FINI, please go to
hkex.com.hk/fini

