I. Business Gateway

1. Vai trò

- Thực hiện routing các request từ các ứng dụng đầu cuối (client) đến các service nghiệp vụ trong hệ thống CoreFinance

- Thực hiện xác thực (Authentication) và ủy quyền (Authorization) cho các ứng dụng đầu cuối trước khi các request được routing

- Thêm các thông tin xác thực cần thiết vào các request của client trước khi routing

- Thực hiện cân bằng tải cho các instance của một service nghiệp vụ trong hệ thống CoreFinance

- Cho phép cấu hình dynamic routing, cung cấp các API để quản trị viên có thể cấu hình (thêm, sửa, xóa) các route ngay tại thời điểm runtime, không cần khởi động lại service Business Gateway. Do đó không gây downtime

- Thực hiện đẩy các dữ liệu log của các request lên các hệ thống lưu trữ log tập trung

- Thực hiện fallback request sang một service instance khác trong trường hợp request đến một service instance bị timeout

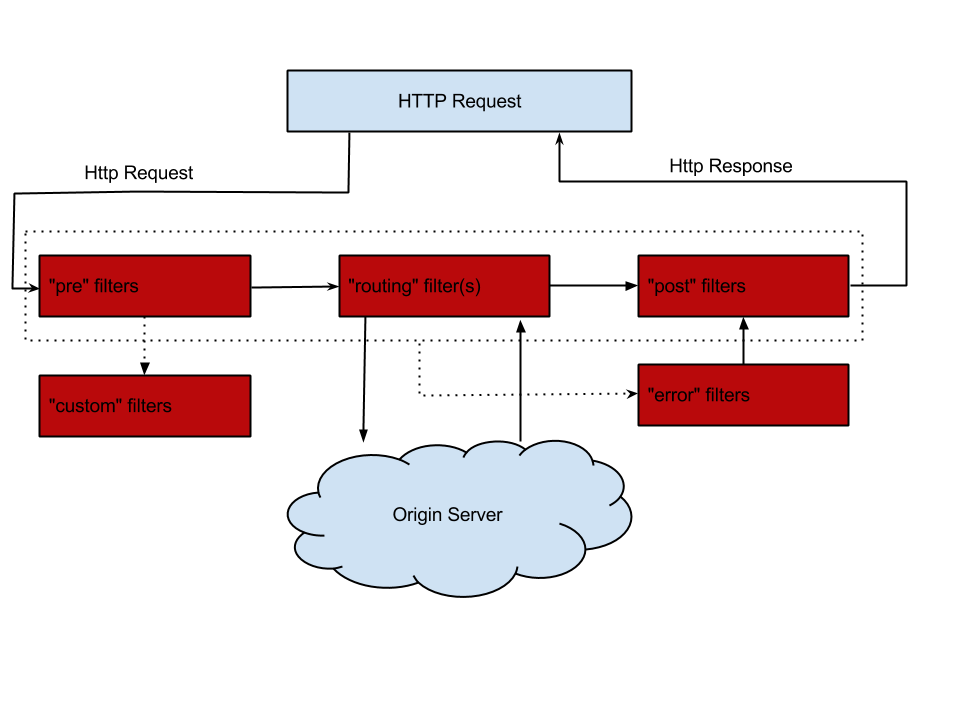
2. Công nghệ

Netflix Zuul 1.x + Spring Boot 2.0.4.RELEASE

Netflix Zuul là 1 open source edge service viết bằng ngôn ngữ java, được phát triển bởi Netflix với mục đích ban đầu là sử dụng như một api gateway cho tất cả các request từ các thiết bị và websites đến các service streaming của Netflix

(<https://github.com/Netflix/zuul>)

Phần trung tâm của Zuul là một tập của nhiều bộ lọc (filter). Các filter này thực hiện các hành động nào đó trước khi routing request hoặc response, các filter hoàn toàn có thể lập trình được theo ý muốn của người phát triển



Các thành phần của một filter:

**- Type:** định nghĩa giai đoạn mà filter được thực thi trong xuyên suốt flow của 1 request

**- Execution Order:** định nghĩa thứ tự thực thi của filter thuộc cùng một Type

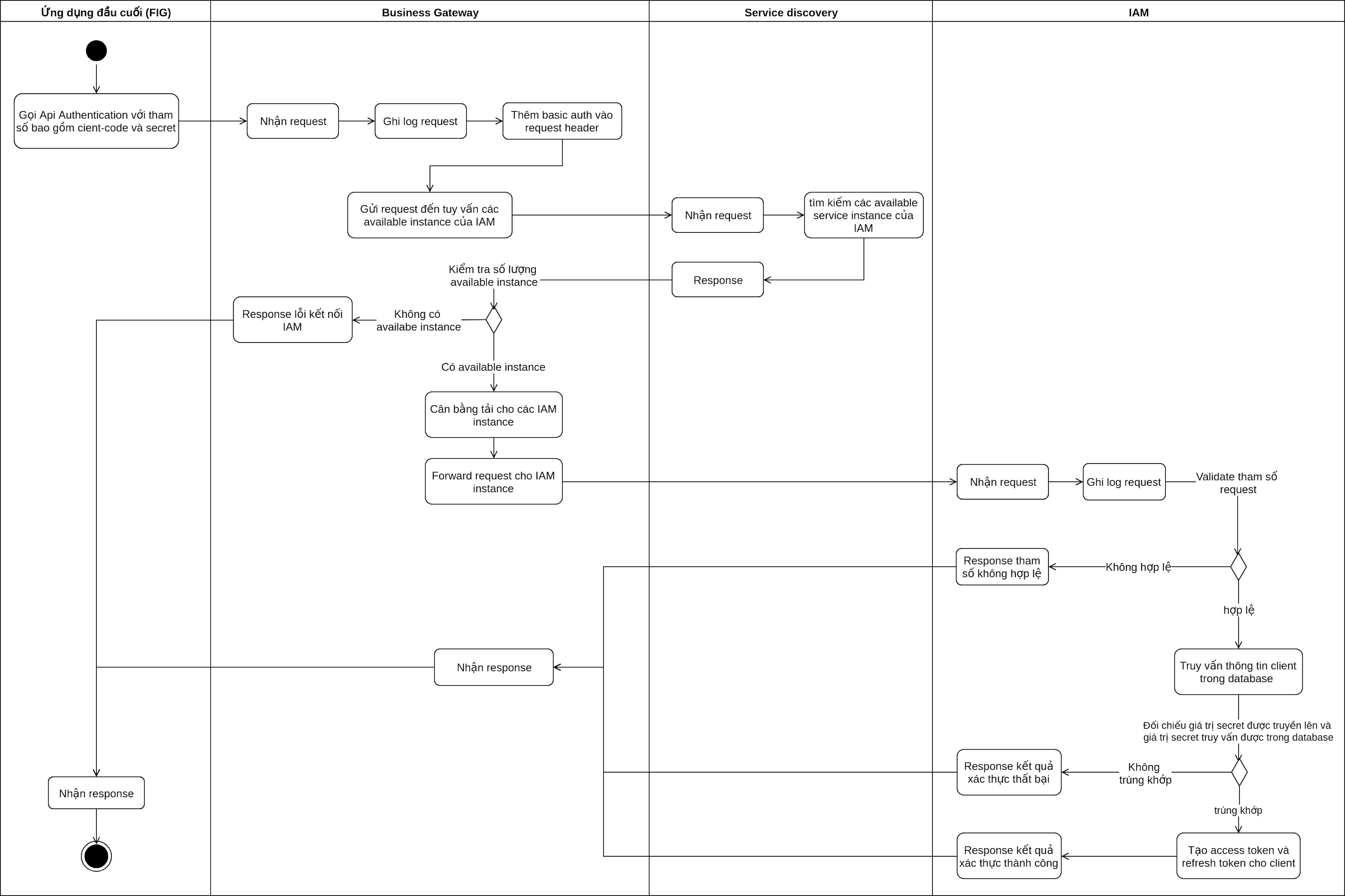
**- Criteria:** định nghĩa điều kiện để filter được thực thi

**- Action:** định nghĩa các hành động của filter khi được thực thi

3. API nghiệp vụ

3.1. Authentication các ứng dụng đầu cuối

*a. Activity diagram*



*b. Mô tả*

**API:** {host}/oauth/api/authentication/clientApplications/token

**Method:** POST

**Header:**

- Content-Type: application/json

**Body:**

|  |  |  |
| --- | --- | --- |
| Format | Mô tả | Ví dụ |
| {  "client\_code": [string],  "secret": [string]  } | **client\_code:** mã định danh được quản trị viên cấp cho ứng dụng đầu cuối  **secret:** mã bí mật được quản trị viên cấp cho ứng dụng đầu cuối | {  "client\_code": "fig",  "secret": "VGheBIBeNRwbWZMhOwUAgsbplSOA"  } |

**Response:**

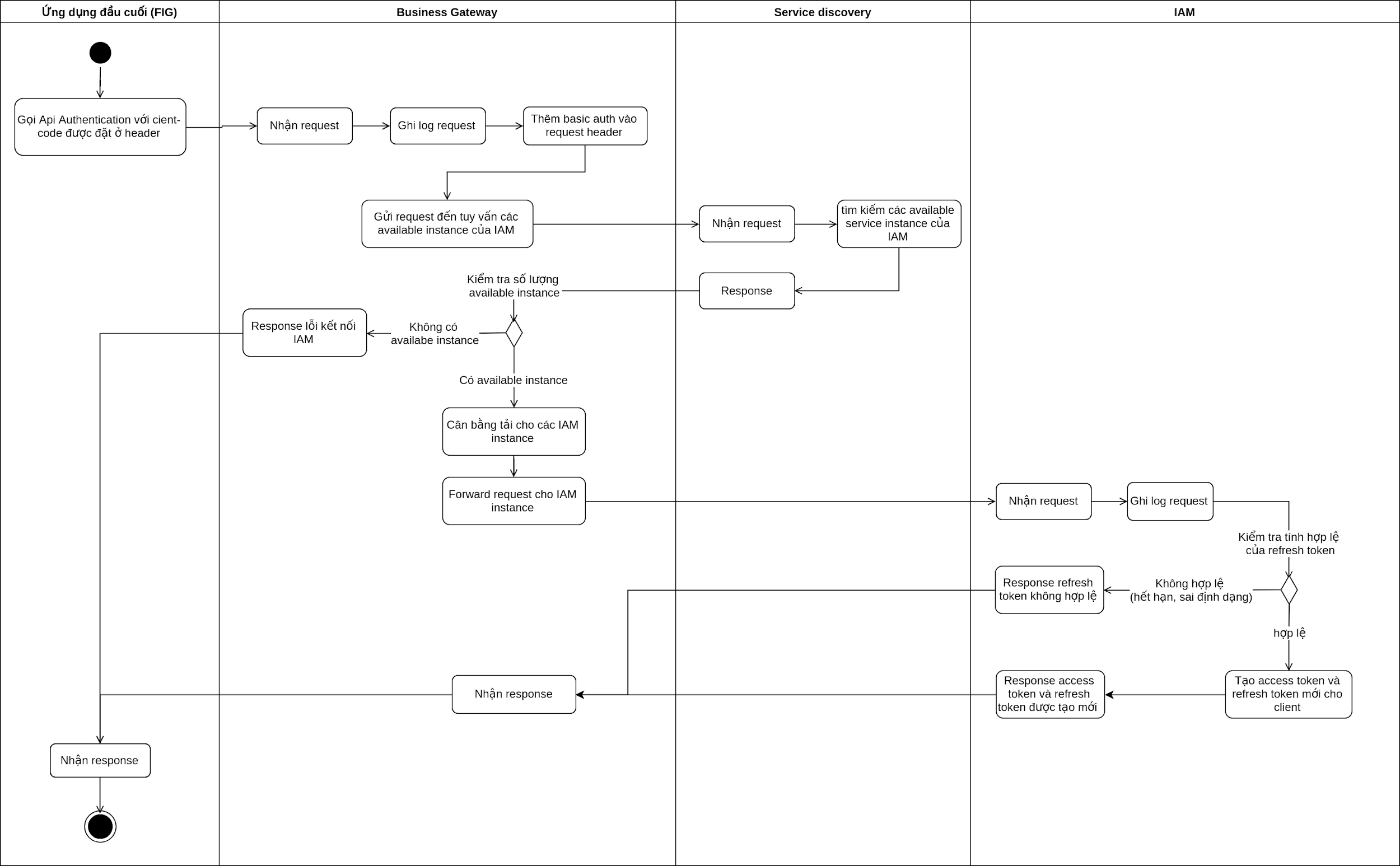
|  |  |  |
| --- | --- | --- |
| Format | Mô tả | Ví dụ |
| {  "response\_code": 200,  "message": "OK",  "data": {  "token\_type": [string],  "access\_token": [string],  "refresh\_token": [string],  "jti": [string],  "access\_token\_exp\_secs": [int],  "refresh\_token\_exp\_secs": [int]  }  } | **response\_code:** mã của response  **message:** thông điệp của response  **data:** dữ liệu trả về của response  **token\_type:** loại access token, sử dụng để authorization  **access\_token:** một chuỗi giá trị chứa thông tin về ứng dụng đầu cuối được mã hóa, dùng để authorization  **refresh\_token:** một chuỗi có cấu trúc tương đồng với access token, tuy nhiên có thời hạn sử dụng dài hơn và được sử dụng để làm mới access token khi nó hết hạn  **jti:** một chuỗi uuid định danh cho access token được sinh ra  **access\_token\_exp\_secs:** khoảng thời gian (giây) có hiệu lực của access token tính từ thời điểm response trả về  **refresh\_token\_exp\_secs:** khoảng thời gian (giây) có hiệu lực của refresh token tính từ thời điểm response trả về | {  "response\_code": 200,  "message": "OK",  "data": {  "token\_type": "bearer",  "access\_token": "eyh9.eyJd.sy21J",  "refresh\_token": "eyhb.GciiJ.IUzI1",  "jti": "18725-886d-4d4e-85a4-7e97ce3",  "access\_token\_exp\_secs": 86400,  "refresh\_token\_exp\_secs": 2592000  }  } |

*c. Các mã response*

|  |  |  |
| --- | --- | --- |
| response\_code | message | Mô tả |
| 200 | OK | Thành công |
| 4003 | invalid or missing request parameters | Tham số truyền lên thiếu hoặc không hợp lệ |
| 4011 | wrong client code or secret | Giá trị client code hoặc secret không hợp lệ |
| 4012 | auth type not permitted | Client không được phép authentication và authorization bằng access token |
| 4031 | wrong involker id or secret | Giá trị client id hoặc secret trong của API Gateway không đồng bộ với IAM |
| 500 | internet server error | Có lỗi xảy ra |

3.2. Làm mới access token

*a. Activity diagram*



*b. Mô tả*

**API:** {host}/oauth/api/authentication/clientApplications/token

**Method:** POST

**Header:**

- Content-Type: application/json

**Body:**

|  |  |  |
| --- | --- | --- |
| Format | Mô tả | Ví dụ |
| {  "refresh\_token": [string]  } | **refresh\_token:** refresh token của ứng dụng đầu cuối được cấp sau khi thực hiện authentication | {  "refresh\_token": "eyhb.GciiJ.IUzI1"  } |

**Response:**

|  |  |  |
| --- | --- | --- |
| Format | Mô tả | Ví dụ |
| {  "response\_code": 200,  "message": "OK",  "data": {  "token\_type": [string],  "access\_token": [string],  "refresh\_token": [string],  "jti": [string],  "access\_token\_exp\_secs": [int],  "refresh\_token\_exp\_secs": [int]  }  } | **response\_code:** mã của response  **message:** thông điệp của response  **data:** dữ liệu trả về của response  **token\_type:** loại access token, sử dụng để authorization  **access\_token:** một chuỗi giá trị chứa thông tin về ứng dụng đầu cuối được mã hóa, dùng để authorization  **refresh\_token:** một chuỗi có cấu trúc tương đồng với access token, tuy nhiên có thời hạn sử dụng dài hơn và được sử dụng để làm mới access token khi nó hết hạn  **jti:** một chuỗi uuid định danh cho access token được sinh ra  **access\_token\_exp\_secs:** khoảng thời gian (giây) có hiệu lực của access token tính từ thời điểm response trả về  **refresh\_token\_exp\_secs:** khoảng thời gian (giây) có hiệu lực của refresh token tính từ thời điểm response trả về | {  "response\_code": 200,  "message": "OK",  "data": {  "token\_type": "bearer",  "access\_token": "eyh9.eyJd.sy21J",  "refresh\_token": "edfb.HsiiJ.akizI1",  "jti": "b398cab5-72e1-4e60-8d10-c2fd",  "access\_token\_exp\_secs": 86400,  "refresh\_token\_exp\_secs": 2592000  }  } |

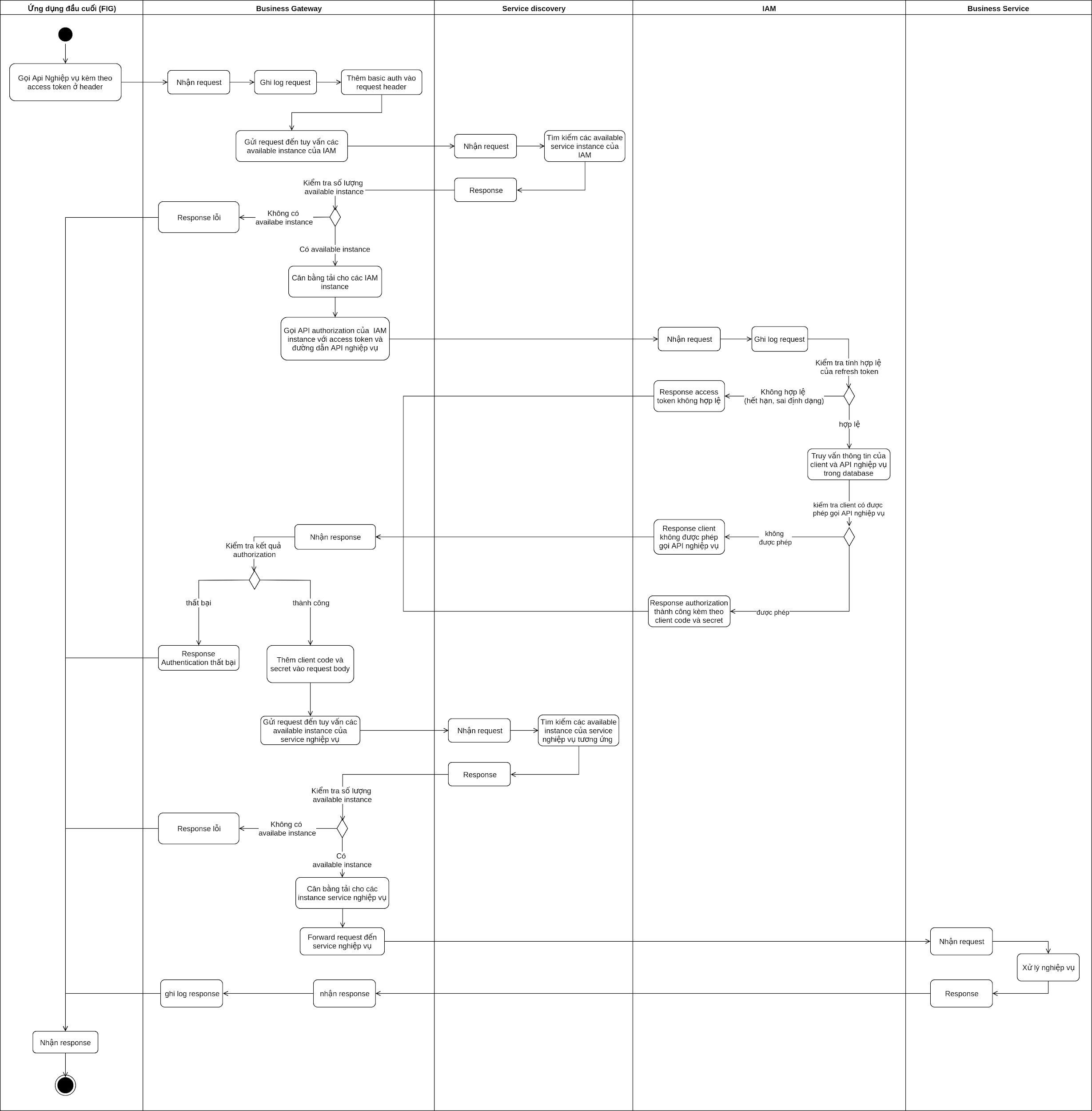
*c. Các mã response*

|  |  |  |
| --- | --- | --- |
| response\_code | message | Mô tả |
| 200 | OK | Thành công |
| 4003 | invalid or missing request parameters | Tham số truyền lên thiếu hoặc không hợp lệ |
| 4011 | wrong client code or secret | Giá trị client code hoặc secret không hợp lệ |
| 4012 | auth type not permitted | Client không được phép authentication và authorization bằng access token |
| 4031 | wrong involker id or secret | Giá trị client id hoặc secret trong của Business Gateway không đồng bộ với IAM |
| 500 | internet server error | Có lỗi xảy ra |

3.3. Gọi các API nghiệp vụ của hệ thống CoreFinance thông qua Business Gateway

3.3.1. Gọi các API nghiệp vụ sử dụng access token để authorization

*a. Activity Diagram*



*b. Mô tả*

**API:** {host}/{path của API nghiệp vụ}

**Method:** {Method của API nghiệp vụ}

**Header:**

- **Authorization**: {token\_type} {access token} (VD: **Authorization:** bearer eySFEfgh9.eysdfsdsfJd.sydfwefew1J)

- {Header của API nghiệp vụ, nếu có}

**Body:** {Body của API nghiệp vụ, nếu có}

**Các thông tin được thêm mới vào request body sau bước Authorization và trước khi forwading request:**

|  |  |  |
| --- | --- | --- |
| Format | Mô tả | Ví dụ |
| {  "client\_id": [string],  "jwt\_secret": [string],  ...  } | **client\_id:** giá trị client code của ứng dụng đầu cuối  **jwt\_secret:** giá trị secret của ứng dụng đầu cuối | {  "client\_id": "fig",  "jwt\_secret": "VGheBIBeNRwbWZMhOwUAgsbplSOA",  ...  } |

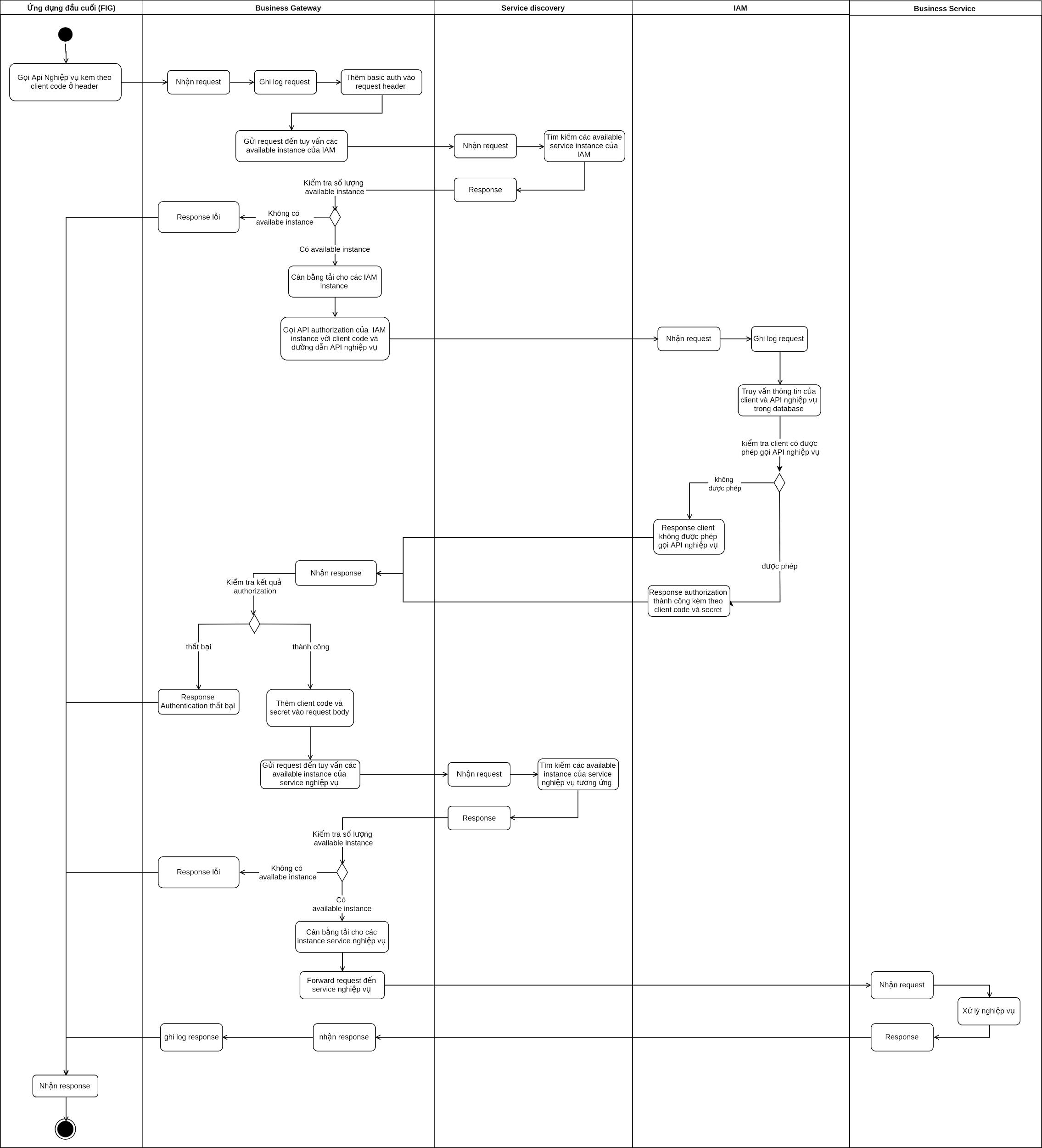
**Response:** {Là response của các API nghiệp vụ}

*c. Các mã response của Bussiness Gateway*

|  |  |  |
| --- | --- | --- |
| response\_code | message | Mô tả |
| 4012 | auth type not permitted | Client không được phép authentication và authorization bằng access token |
| 4013 | access token invalid | Access token không hợp lệ |
| 4014 | access token missing | Thiếu access token ở Authorization header |
| 4015 | access token expired | Access token hết thời hạn |
| 4032 | client application disabled | Ứng dụng đầu cuối đã tạm thời bị vô hiệu hóa |
| 4033 | route is not permitted for client application | Ứng dụng đầu cuối không được cho phép gọi API nghiệp vụ này |
| 4034 | missing authentication type | Request thiếu Authorization ở header |
| 4041 | client application not found | Không tìm thấy dữ liệu về ứng dụng đầu cuối, có thể dữ liệu đã bị xóa |
| 4042 | request path not found | Đường dẫn API không tồn tại |
| 4081 | IAM connection timeout | Kết nối đến IAM bị timeout (sau khi toàn bộ fallback thất bại) |
| 4082 | business service connection timeout | Kết nối đến các API nghiệp vụ bị timeout (sau khi toàn bộ fallback thất bại) |
| 500 | internet server error | Có lỗi xảy ra |

3.3.2. Gọi các API nghiệp vụ sử dụng client\_code để authorization

a. Activity Diagram



*b.Mô tả*

**API:** {host}/{path của API nghiệp vụ}

**Method:** {Method của API nghiệp vụ}

**Header:**

- **client\_code**: {token\_type} {access token} (VD: **client\_code:** {client\_code})

- {Header của API nghiệp vụ, nếu có}

**Body:** {Body của API nghiệp vụ, nếu có}

**Các thông tin được thêm mới vào request body sau bước Authorization và trước khi forwading request:**

|  |  |  |
| --- | --- | --- |
| Format | Mô tả | Ví dụ |
| {  "client\_id": [string],  "jwt\_secret": [string],  ...  } | **client\_id:** giá trị client code của ứng dụng đầu cuối  **jwt\_secret:** giá trị secret của ứng dụng đầu cuối | {  "client\_id": "fig",  "jwt\_secret": "VGheBIBeNRwbWZMhOwUAgsbplSOA",  ...  } |

**Response:** {Là response của các API nghiệp vụ}

*c. Các mã response của Bussiness Gateway*

|  |  |  |
| --- | --- | --- |
| response\_code | message | Mô tả |
| 4012 | auth type not permitted | Client không được phép authentication và authorization bằng access token |
| 4013 | access token invalid | Access token không hợp lệ |
| 4014 | access token missing | Thiếu access token ở Authorization header |
| 4015 | access token expired | Access token hết thời hạn |
| 4032 | client application disabled | Ứng dụng đầu cuối đã tạm thời bị vô hiệu hóa |
| 4033 | route is not permitted for client application | Ứng dụng đầu cuối không được cho phép gọi API nghiệp vụ này |
| 4034 | missing authentication type | Request thiếu Authorization ở header |
| 4041 | client application not found | Không tìm thấy dữ liệu về ứng dụng đầu cuối, có thể dữ liệu đã bị xóa |
| 4042 | request path not found | Đường dẫn API không tồn tại |
| 4081 | IAM connection timeout | Kết nối đến IAM bị timeout (sau khi toàn bộ fallback thất bại) |
| 4082 | business service connection timeout | Kết nối đến các API nghiệp vụ bị timeout (sau khi toàn bộ fallback thất bại) |
| 500 | internet server error | Có lỗi xảy ra |

4. API cấu hình, quản trị

4.1. API lấy danh sách các business route đang hoạt động

*a. Mô tả*

**API:** {host}/api/gateway/routes

**Method:** GET

**Body:** Không

**Response:**

|  |  |  |
| --- | --- | --- |
| Format | Mô tả | Ví dụ |
| {  "response\_code": 200,  "message": "OK",  "data": {  [id]: {  "id": [string],  "path": [string],  "serviceId": [string],  "url": [string],  "stripPrefix": [boolean],  "retryable": [boolean, nullable],  "sensitiveHeaders": [array<string>], "customSensitiveHeaders": [boolean],  "location": [string]  }  }  } | **response\_code:** mã của response  **message:** thông điệp của response  **data:** dữ liệu trả về của response  **id:** định danh của business route  **path:** Ant pattern của bussiness route  **serviceId:** tên của service được đăng ký trên Consul  **url:** đường dẫn tuyệt đối của service API trong trường hợp không sử dụng service discovery  **stripPrefix:** cho biết trước khi request được forward có tự động loại bỏ phần tiền tố trên đường dẫn hay không  **retryable:** có thiết lập cơ chế tự động retry lại khi forwad bị thất bại hay không  **sensitiveHeaders:** mảng danh sách chứa các giá trị của header được coi là nhạy cảm, các header nhạy cảm sẽ không được forward khi đi qua business gateway  **customSensitiveHeaders:** nhận giá trị false nếu **sensitiveHeaders** null và ngược lại  **location:** có cùng giá trị với **serviceId** | {  "response\_code": 200,  "message": "OK",  "data": {  "oauth": {  "id": "oauth",  "path": "/oauth/\*\*",  "serviceId": "iam",  "url": null,  "stripPrefix": true,  "retryable": null,  "sensitiveHeaders": [], "customSensitiveHeaders": true,  "location": “iam”  },  "foo": {  "id": "foo",  "path": "/foo/bar/\*\*",  "serviceId": null,  "url": “http://google.com,  "stripPrefix": true,  "retryable": true,  "sensitiveHeaders": null, "customSensitiveHeaders": false,  "location": null  },  "bar": {  "id": "bar",  "path": "/bar/foo",  "serviceId": “iam/actuator/health”,  "url": null,  "stripPrefix": true,  "retryable": false,  "sensitiveHeaders": [], "customSensitiveHeaders": true,  "location": “iam/actuator/health”  }  }  } |

4.2. Thêm mới/ cập nhật một business route

*a. Mô tả*

**API:** {host}/api/gateway/routes

**Method:** POST

**Body:**

|  |  |  |
| --- | --- | --- |
| Format | Mô tả | Ví dụ |
| {  "id": [string],  "path": [string],  "consul\_service\_name": [string],  “strip\_prefix”: [boolean],  “sensitive\_headers”: [array<string>]  } | **id:** định danh của bussiness route, nếu định danh chưa tồn tại thì sẽ thực hiện thêm mới, nếu đã tồn tại thì sẽ thực hiện cập nhật bussiness route  **path:** Ant pattern của bussiness route  **consul\_service\_name**: tên của service được đăng ký trên Consul  **strip\_prefix:** cho biết trước khi request được forward có tự động loại bỏ phần tiền tố trên đường dẫn hay không  **sensitive\_headers:** mảng danh sách chứa các giá trị của header được coi là nhạy cảm, các header nhạy cảm sẽ không được forward khi đi qua business gateway | {  "id": "foo-bar",  "path": "foo/bar/\*\*",  "consul\_service\_name": "foo-bar-service",  “strip\_prefix”: true,  “sensitive\_headers”: [“Authorization”]  } |

*\* Chú thích cách cấu hình bussiness route cho Business Gateway*

VD: cần cấu hình bussiness route trỏ đến API GET api/products và POST api/products/ratings của một service có tên đăng ký trên Consul là "Catalog-Service"

|  |  |
| --- | --- |
| Format | Kết quả |
| {  "id": "Catalog",  "**path**": "**/catalog/\*\***",  "consul\_service\_name":"Catalog-Service",  “**strip\_prefix**”: **true**,  “sensitive\_headers”: []  } | |  |  | | --- | --- | | **Business Gateway** | **Catalog-Service** | | GET catalog/api/products | => GET api/products | | POST catalog/api/products/ratings | => POST api/products/ratings | |
| {  "id": "Catalog",  "**path**": "**/api/products**",  "consul\_service\_name":"Catalog-Service",  “**strip\_prefix**”: **false**,  “sensitive\_headers”: []  } | |  |  | | --- | --- | | **Business Gateway** | **Catalog-Service** | | GET api/products | => GET api/products | |
| {  "id": "Catalog",  "**path**": "**/api/\*\***",  "consul\_service\_name":"Catalog-Service",  “**strip\_prefix**”: **false**,  “sensitive\_headers”: []  } | |  |  | | --- | --- | | **Business Gateway** | **Catalog-Service** | | GET api/products | => GET api/products | | POST api/products/ratings | => POST api/products/ratings | |
| {  "id": "Catalog",  "**path**": "**/catalog/items**",  "**consul\_service\_name**":  "**Catalog-Service/api/products**",  “**strip\_prefix**”: **true/false (không tác dụng)**,  “sensitive\_headers”: []  } | |  |  | | --- | --- | | **Business Gateway** | **Catalog-Service** | | GET catalog/items | => GET api/products | |
| {  "id": "Catalog",  "**path**": "**/catalog/\*\***",  "**consul\_service\_name**":  "**Catalog-Service/api/\*\***",  “**strip\_prefix**”: **true**,  “sensitive\_headers”: []  } | |  |  | | --- | --- | | **Business Gateway** | **Catalog-Service** | | GET catalog/products | => GET api/products | | POST catalog/products/ratings | => POST api/products/ratings | |
| {  "id": "Catalog",  "**path**": "**/products/\*\***",  "**consul\_service\_name**":  "**Catalog-Service/api/\*\***",  “**strip\_prefix**”: **false**,  “sensitive\_headers”: []  } | |  |  | | --- | --- | | **Business Gateway** | **Catalog-Service** | | POST products/ratings | => POST api/products/ratings | | GET products | => GET api/products | |

**Response:**

|  |  |  |
| --- | --- | --- |
| Format | Mô tả | Ví dụ |
| {  "response\_code": 200,  "message": "OK",  "data": null  } | **response\_code:** mã của response  **message:** thông điệp của response  **data:** dữ liệu trả về của response | {  "response\_code": 200,  "message": "OK",  "data": null  } |

*b. Các mã response của Bussiness Gateway*

|  |  |  |
| --- | --- | --- |
| response\_code | message | Mô tả |
| 200 | OK | Thê mới/ cập nhật bussiness route thành công |
| 500 | internet server error | Có lỗi xảy ra |

4.3. Xóa một business route

*a. Mô tả*

**API:** {host}/api/gateway/routes/{bussiness route id}

**Method:** DELETE

**Body:** Không

**Response:**

|  |  |  |
| --- | --- | --- |
| Format | Mô tả | Ví dụ |
| {  "response\_code": 200,  "message": "OK",  "data": null  } | **response\_code:** mã của response  **message:** thông điệp của response  **data:** dữ liệu trả về của response | {  "response\_code": 200,  "message": "OK",  "data": null  } |

*b. Các mã response của Bussiness Gateway*

|  |  |  |
| --- | --- | --- |
| response\_code | message | Mô tả |
| 200 | OK | Xóa bussiness route thành công |
| 404 | route id not found | Không tìm thấy business route |
| 500 | internet server error | Có lỗi xảy ra |

II. IAM

1. Vai trò

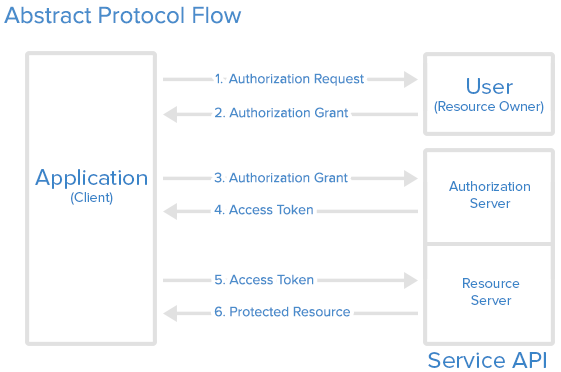
- Authentication cho các ứng dụng đầu cuối thông qua client code và secret

- Authorization cho các ứng dụng đầu cuối và kiểm tra tính hợp lệ của truy cập từ ứng dụng đó vào một API nghiệp vụ trong hệ thống CoreFinance

2. Công nghệ

OAuth2 + Spring Boot 2.0.4.RELEASE

2.1. Mô hình chuẩn của OAuth2



1. Client Application sẽ yêu cầu Resource Owner (User, một Application khác,...) để xin quyền được access đến các tài nguyên thuộc quyền sở hữu của Resource Owner ở Resource Server

2. Resource Owner nếu chấp nhận sẽ gửi lại cho Client Application một Authorization Grant (username password, authorization code, refresh token,...)

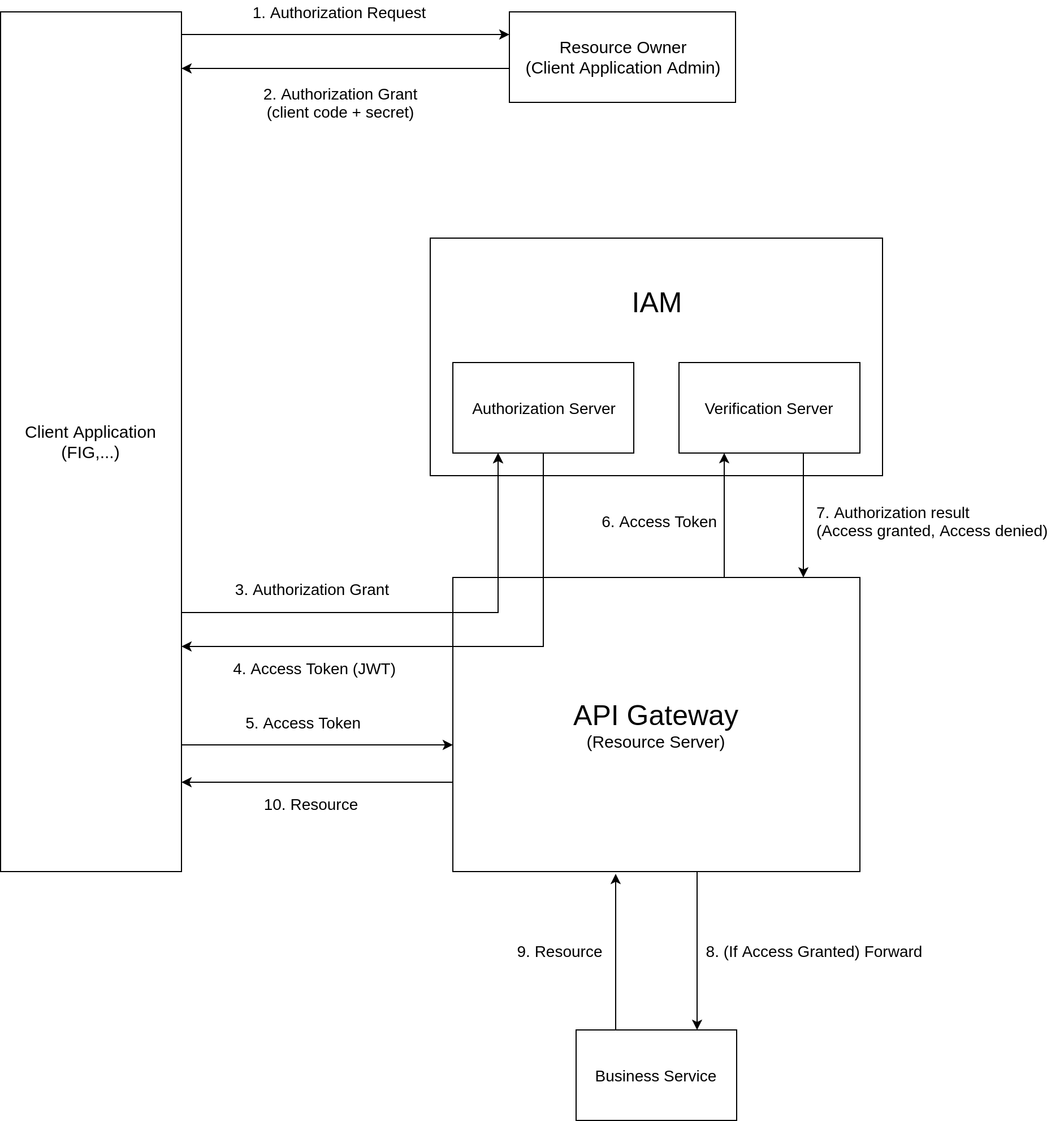
3. Client Application sẽ sử dụng Authorization Grant để request lên Authorization Server để yêu cầu được ủy quyền truy cập vào tài nguyên của Resource Owner trên Resource Server

4. Authorization Server tiến hành xác minh Authorization Grant do Client Application gửi lên, nếu hợp lệ sẽ trả về một access token cho Client Application

5. Client Application sử dụng access token cho mỗi lần truy cập đến các tài nguyên của Resource Owner trên Resource Server

6. Resource Server tiến hành xác minh access token do Client Application gửi lên tại mỗi lần truy cập, nếu hợp lệ sẽ trả về các tài nguyên được Client Application request

2.2. Mô hình OAuth2 của hệ thống CoreFinance



So với mô hình OAuth2 chuẩn:

- Quản trị viên quản lý dữ liệu các ứng dụng đầu cuối truy cập vào hệ thống CoreFinance đóng vai trò là Resource Owner

- Các ứng dụng đầu cuối (VD: FIG) đóng vai trò là các Client Application

- IAM có hai nhiệm vụ: là Authoriation Server và thực hiện xác minh access token (vốn là trách nhiệm của Resource Server trong mô hình OAuth2 chuẩn)

- Api Gateway đóng vai trò như một Resource Server

- Authentication các ứng dụng đầu cuối được thực hiện gián tiếp, Các ứng dụng đầu cuối sẽ thực hiện request authentication đến Api Gateway, Api Gateway thêm một số thông tin cần thiết sau đó sẽ chuyển hướng request đến IAM để tiến hành xác thực và trả kết quả về cho các ứng dụng đầu cuối