NGÂN HÀNG NHÀ NƯỚC VIỆT NAM	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 64/2024/TT-NHNN	*Hà Nội, ngày 31 tháng 12 năm 2024*

THÔNG TƯ

Quy định về triển khai giao diện lập trình ứng dụng mở trong ngành Ngân hàng

Căn cứ Luật Ngân hàng Nhà nước Việt Nam ngày 16 tháng 6 năm 2010;

Căn cứ Luật Các tổ chức tín dụng ngày 18 tháng 01 năm 2024;

Căn cứ Luật Giao dịch điện tử ngày 22 tháng 6 năm 2023;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 52/2024/NĐ-CP ngày 15 tháng 5 năm 2024 của Chính phủ quy định về thanh toán không dùng tiền mặt;

Căn cứ Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ quy định về bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 102/2022/NĐ-CP ngày 12 tháng 12 năm 2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ngân hàng Nhà nước Việt Nam;

Theo đề nghị của Cục trưởng Cục Công nghệ thông tin;

Thống đốc Ngân hàng Nhà nước Việt Nam ban hành Thông tư quy định về triển khai giao diện lập trình ứng dụng mở trong ngành Ngân hàng.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

1. Thông tư này quy định về việc triển khai giao diện lập trình ứng dụng mở trong ngành Ngân hàng.

2. Thông tư này không điều chỉnh việc kết nối, xử lý dữ liệu chứa thông tin thuộc phạm vi bí mật nhà nước. Việc xử lý dữ liệu chứa thông tin thuộc

phạm vi bí mật nhà nước được thực hiện theo quy định của pháp luật hiện hành.

3. Thông tư này không điều chỉnh việc kết nối, xử lý dữ liệu trực tiếp giữa:

a) Hệ thống thông tin của Ngân hàng và hệ thống thông tin của tổ chức qua giao diện lập trình ứng dụng để phục vụ nghiệp vụ nội bộ của chính tổ chức đó;

b) Hệ thống thông tin của Ngân hàng và hệ thống thông tin của Tổ chức chủ trì hệ thống bù trừ điện tử. Tổ chức chủ trì hệ thống bù trừ điện tử được xác định theo quy định của Ngân hàng Nhà nước Việt Nam về hoạt động cung ứng dịch vụ trung gian thanh toán.

Điều 2. Đối tượng áp dụng

1. Ngân hàng thương mại, ngân hàng hợp tác xã, chi nhánh ngân hàng nước ngoài (sau đây gọi chung là Ngân hàng).

2. Tổ chức, cá nhân có liên quan trong việc triển khai dịch vụ qua giao diện lập trình ứng dụng mở trong ngành ngân hàng.

Điều 3. Giải thích từ ngữ

Trong Thông tư này, các thuật ngữ dưới đây được hiểu như sau:

1. Giao diện lập trình ứng dụng (tên tiếng anh là: Application Programming Interface, sau đây viết tắt là API) là giao diện cho phép giao tiếp giữa các ứng dụng phần mềm trong một tổ chức hoặc giữa các tổ chức với nhau.

2. Giao diện lập trình ứng dụng mở trong ngành Ngân hàng (Open API) là tập hợp các API được Ngân hàng cung cấp cho bên thứ ba trực tiếp kết nối, xử lý dữ liệu để cung ứng dịch vụ cho khách hàng. Open API gồm: Open API cơ bản và Open API khác.

3. Hệ thống thử nghiệm Open API là hệ thống thông tin của Ngân hàng cung cấp cho bên thứ ba để thử nghiệm các Open API trước khi triển khai chính thức.

4. Khách hàng là cá nhân sử dụng dịch vụ của Ngân hàng.

5. Bên thứ ba là tổ chức hoặc Ngân hàng khác có thỏa thuận bằng hợp đồng với Ngân hàng trong việc kết nối, xử lý dữ liệu qua Open API để cung ứng dịch vụ cho khách hàng.

6. Sự đồng ý của khách hàng là việc thể hiện rõ ràng, tự nguyện, khẳng định việc cho phép xử lý dữ liệu cá nhân của khách hàng.

Điều 4. Nguyên tắc chung

Ngân hàng, khách hàng và bên thứ ba (sau đây gọi là các bên) khi triển khai Open API phải tuân thủ các yêu cầu sau:

1. Tuân thủ các quy định của pháp luật về giữ bí mật, cung cấp thông tin khách hàng và bảo vệ dữ liệu cá nhân. Việc xử lý dữ liệu cá nhân của khách hàng chỉ phục vụ cho chính khách hàng đó, trừ trường hợp theo quy định của pháp luật.

2. Dữ liệu trong quá trình xử lý phải được quản lý, lưu trữ, khai thác, sử dụng đúng mục đích tại hợp đồng giữa các bên và phù hợp với quy định của pháp luật.

3. Dữ liệu trong quá trình xử lý phải bảo đảm tính cập nhật và chính xác. Trường hợp có sai lệch phải thực hiện đính chính, hiệu chỉnh kịp thời theo thỏa thuận giữa các bên.

Chương II
QUY ĐỊNH CỤ THỂ VỀ TRIỂN KHAI OPEN API

Mục 1

QUY ĐỊNH TRIỂN KHAI OPEN API

Điều 5. Nguyên tắc triển khai Open API

1. Khi triển khai Open API cơ bản quy định tại Điều 6 Thông tư này, Ngân hàng phải tuân thủ quy định tại Phụ lục 01, Phụ lục 02 ban hành kèm theo Thông tư này.

2. Khi triển khai Open API khác theo nhu cầu thực tế và phù hợp quy định của pháp luật ngoài danh mục Open API quy định tại Điều 6 Thông tư này, Ngân hàng phải tuân thủ quy định tại Phụ lục 02 ban hành kèm theo Thông tư này.

3. Ngân hàng chỉ được phép triển khai Open API quy định tại điểm c khoản 1 Điều 6 cho bên thứ ba là Ngân hàng, tổ chức cung ứng dịch vụ trung gian thanh toán.

Điều 6. Danh mục Open API

1. Danh mục Open API cơ bản được tổ chức thành các nhóm sau:

a) Open API truy vấn thông tin tỷ giá, lãi suất của Ngân hàng gồm: API Lấy thông tin lãi suất, API Lấy thông tin tỷ giá;

b) Open API truy vấn thông tin của khách hàng gồm: API Xác nhận và lấy sự đồng ý của khách hàng, API Lấy mã truy cập, API Làm mới mã truy cập, API Thu hồi mã truy cập, API Lấy danh sách tài khoản, API Lấy thông tin tài khoản, API Lấy lịch sử giao dịch;

c) Open API khởi tạo thanh toán, nạp tiền vào ví điện tử, rút tiền ra khỏi ví điện tử gồm:

(i) Open API khởi tạo thanh toán gồm: API Khởi tạo thanh toán, API Xác nhận khách hàng Luồng Redirect, API Lấy mã truy cập luồng Redirect, API Cập nhật trạng thái xác nhận thanh toán của khách hàng luồng Decoupled, API Xác nhận thanh toán, API Lấy trạng thái giao dịch, API Lấy trạng thái xác nhận thanh toán của khách hàng luồng Decoupled;

(ii) Open API Nạp tiền vào ví điện tử gồm: API Nạp ví điện tử, API Xác nhận OTP, API Cập nhật trạng thái xác nhận nạp ví điện tử của khách hàng luồng Decoupled, API Lấy trạng thái xác nhận nạp ví điện tử của khách hàng luồng Decoupled, API Xác nhận nạp ví điện tử, API Lấy trạng thái giao dịch;

(iii) Open API Rút tiền ra khỏi ví điện tử.

2. Chi tiết đặc tả danh mục Open API tại khoản 1 Điều này được quy định cụ thể tại Phụ lục 01 ban hành kèm theo Thông tư này.

Điều 7. Danh mục tiêu chuẩn kỹ thuật

1. Các tiêu chuẩn kỹ thuật triển khai Open API gồm tiêu chuẩn kiến trúc, tiêu chuẩn dữ liệu và tiêu chuẩn an toàn thông tin.

2. Tiêu chuẩn kỹ thuật triển khai Open API trong ngành Ngân hàng quy định cụ thể tại Phụ lục 02 ban hành kèm theo Thông tư này.

Điều 8. Hợp đồng giữa Ngân hàng với bên thứ ba

Ngân hàng phải ký kết hợp đồng với bên thứ ba về việc triển khai Open API, bao gồm tối thiểu các nội dung sau:

1. Cam kết bảo mật thông tin, trong đó có thỏa thuận về việc bảo đảm an toàn, bảo mật thông tin khi thực hiện xử lý dữ liệu qua Open API do Ngân hàng cung cấp.

2. Cam kết sử dụng dữ liệu do Ngân hàng cung cấp đúng phạm vi, mục đích.

3. Bên thứ ba phải thông báo cho Ngân hàng khi phát hiện nhân sự vi phạm quy định về an toàn thông tin mạng khi triển khai Open API.

4. Thông tin về dịch vụ cung cấp cho khách hàng được triển khai qua Open API.

5. Thông tin về phí dịch vụ cung cấp cho khách hàng được triển khai qua Open API (nếu có).

6. Điều khoản về hệ thống thông tin của bên thứ ba kết nối, xử lý dữ liệu qua Open API phải được đánh giá, xác định cấp độ theo quy định của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

7. Quyền truy cập dữ liệu của bên thứ ba khi triển khai Open API.

8. Điều khoản chấm dứt hợp đồng.

Điều 9. Công khai thông tin Open API

Trước khi chính thức kết nối, xử lý dữ liệu với bên thứ ba, Ngân hàng phải công khai thông tin Open API trên trang thông tin điện tử chính thức của Ngân hàng bao gồm tối thiểu các nội dung sau:

1. Thông tin về Hệ thống thử nghiệm Open API.

2. Danh mục các Open API Ngân hàng triển khai.

Mục 2

QUYỀN VÀ TRÁCH NHIỆM CỦA NGÂN HÀNG VÀ BÊN THỨ BA

Điều 10. Quyền của Ngân hàng

1. Yêu cầu bên thứ ba cung cấp các thông tin cần thiết liên quan đến quá trình kết nối, xử lý dữ liệu qua Open API.

2. Các quyền khác quy định trong hợp đồng với bên thứ ba.

Điều 11. Trách nhiệm của Ngân hàng

1. Hoàn thiện cơ sở hạ tầng hệ thống thông tin phục vụ triển khai Open API để sẵn sàng kết nối, xử lý dữ liệu.

2. Xây dựng và hoàn thiện các tài liệu hướng dẫn kết nối, xử lý dữ liệu.

3. Bảo đảm chất lượng dữ liệu trong quá trình triển khai Open API. Thông báo kịp thời cho bên thứ ba khi có sai lệch dữ liệu và phối hợp với bên thứ ba đính chính, hiệu chỉnh kịp thời.

4. Bảo đảm an toàn, an ninh mạng cho hệ thống thông tin triển khai Open API, đáp ứng tối thiểu cấp độ 3 theo quy định của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và tuân thủ quy định của Ngân hàng Nhà nước Việt Nam về an toàn hệ thống thông tin trong hoạt động ngân hàng.

5. Cung cấp công cụ hoặc chức năng cho phép khách hàng thực hiện:

a) Tra cứu các dữ liệu mà khách hàng đồng ý cho bên thứ ba xử lý;

b) Rút lại sự đồng ý của khách hàng theo quy định của pháp luật.

6. Thiết lập thời hạn được thực hiện truy vấn thông tin của khách hàng sau khi được khách hàng đồng ý không quá 180 ngày, trừ trường hợp có thỏa thuận khác giữa khách hàng với Ngân hàng.

7. Cung cấp thông tin tình hình triển khai Open API cho Ngân hàng Nhà nước Việt Nam (thông qua Cục Công nghệ thông tin) khi được yêu cầu.

8. Phối hợp với bên thứ ba theo thỏa thuận và với cơ quan có thẩm quyền để giải quyết vướng mắc, tranh chấp trong quá trình triển khai Open API.

9. Có giải pháp công nghệ giới hạn số lần truy vấn tự động thông tin của khách hàng từ bên thứ ba.

10. Chịu trách nhiệm lựa chọn, thẩm định, giám sát và quản lý bên thứ ba.

11. Thực hiện cập nhật hoặc thu hồi quyền truy cập dữ liệu của bên thứ ba khi có thay đổi theo hợp đồng.

12. Giám sát hoạt động truy cập:

a) Có hệ thống giám sát để phát hiện và ngăn chặn các hành vi truy cập bất thường hoặc trái phép từ bên thứ ba;

b) Ghi nhật ký toàn bộ việc sử dụng Open API từ bên thứ ba tối thiểu trong vòng 03 tháng và sao lưu tối thiểu 01 năm để phục vụ kiểm tra khi cần thiết.

Điều 12. Quyền và trách nhiệm của bên thứ ba

1. Bên thứ ba có các quyền theo hợp đồng hoặc thỏa thuận với Ngân hàng, khách hàng.

2. Trách nhiệm của bên thứ ba:

a) Cung cấp công cụ hoặc chức năng cho phép khách hàng thực hiện trực tuyến:

(i) Tra cứu các dữ liệu mà khách hàng đồng ý cho bên thứ ba xử lý;

(ii) Rút lại sự đồng ý của khách hàng theo quy định của pháp luật.

b) Thông báo cho khách hàng các điều khoản, điều kiện về việc sử dụng dịch vụ và hướng dẫn khách hàng cách thức sử dụng dịch vụ.

c) Ban hành quy trình quản lý rủi ro; quy trình chăm sóc khách hàng; quy trình xử lý khiếu nại; quy trình giải quyết tranh chấp; quy trình bảo đảm hoạt động liên tục và quy trình sử dụng dịch vụ khi cung cấp dịch vụ cho khách hàng.

d) Khai thác và sử dụng dữ liệu đúng phạm vi theo thỏa thuận giữa các bên và theo quy định của pháp luật.

đ) Thông báo kịp thời cho Ngân hàng khi xảy ra sự cố về công nghệ thông tin, an toàn thông tin khi triển khai Open API. Hình thức và thời gian thông báo theo thỏa thuận giữa Ngân hàng và bên thứ ba.

e) Thông báo kịp thời cho Ngân hàng khi có sai lệch dữ liệu và phối hợp với Ngân hàng đính chính, hiệu chỉnh kịp thời. Hình thức và thời gian thông báo theo thỏa thuận giữa Ngân hàng và bên thứ ba.

Chương III
ĐIỀU KHOẢN THI HÀNH

Điều 13. Trách nhiệm của Cục Công nghệ thông tin

1. Chủ trì, phối hợp với các đơn vị liên quan thuộc Ngân hàng Nhà nước Việt Nam xử lý các vướng mắc phát sinh trong quá trình thực hiện Thông tư này.

2. Theo dõi, tổng hợp, báo cáo Thống đốc Ngân hàng Nhà nước tình hình thực hiện của các Ngân hàng theo quy định tại Thông tư này.

3. Kiểm tra Ngân hàng trong việc thực hiện Thông tư này.

Điều 14. Hiệu lực thi hành

Thông tư này có hiệu lực thi hành kể từ ngày 01 tháng 3 năm 2025.

Điều 15. Điều khoản chuyển tiếp

Các Ngân hàng đã kết nối, xử lý dữ liệu trực tiếp với bên thứ ba qua API hoặc Open API để cung cấp dịch vụ cho khách hàng cá nhân trước thời điểm Thông tư này có hiệu lực thi hành phải thực hiện:

1. Lập danh mục API, Open API đang triển khai và kế hoạch thực hiện chi tiết bảo đảm tuân thủ quy định Thông tư này gửi Ngân hàng Nhà nước Việt Nam (thông qua Cục Công nghệ thông tin), hoàn thành trước ngày 01 tháng 07 năm 2025.

2. Tuân thủ các quy định tại Thông tư này, hoàn thành trước ngày 01 tháng 3 năm 2027.

Điều 16. Tổ chức thực hiện

Thủ trưởng các đơn vị thuộc Ngân hàng Nhà nước Việt Nam, ngân hàng thương mại, ngân hàng hợp tác xã, chi nhánh ngân hàng nước ngoài chịu trách nhiệm tổ chức thực hiện Thông tư này./.

Nơi nhận:
- Như Điều 16;
- Ban Lãnh đạo NHNN;
- Văn phòng Chính phủ;
- Bộ Tư pháp (để kiểm tra);
- Công báo;
- Cổng TTĐT của NHNN;
- Lưu: VP, PC, CNTT (03 bản).

KT. THỐNG ĐỐC
PHÓ THỐNG ĐỐC

Phạm Tiến Dũng

PHỤ LỤC 01

ĐẶC TẢ TIÊU CHUẨN KỸ THUẬT CÁC OPEN API TRONG NGÀNH NGÂN HÀNG

(Ban hành kèm theo Thông tư số 64/2024/TT-NHNN ngày 31 tháng 12 năm 2024 của Thống đốc Ngân hàng Nhà nước Việt Nam)

Bảng Thuật ngữ

STT	Thuật ngữ	Mô tả
1.	PSU (Payment Service User)	Khách hàng
2.	TPP (Third Party Provider)	Bên thứ ba
3.	Bank Auth Server	Hệ thống xác nhận của Ngân hàng
4.	Bank Open API	Hệ thống của Ngân hàng
5.	access_token	Mã truy cập
6.	refresh_token	Mã làm mới
7.	UUID (Universally Unique Identifier)	Mã định danh duy nhất
8.	INF (INFormation)	Các Open API truy vấn thông tin tỷ giá, lãi suất của Ngân hàng
9.	AIS (Account Information Service)	Các Open API truy vấn thông tin của khách hàng
10.	PIS (Payment Initiation Service)	Các Open API khởi tạo thanh toán
11.	EWLTS (Ewallet Service)	Các Open API nạp tiền vào ví điện tử, rút tiền ra khỏi ví điện tử

Bảng Danh mục các Open API chia theo các nhóm quy định tại Điều 6

STT	Danh sách Open API
I	**Open API truy vấn thông tin tỷ giá, lãi suất của Ngân hàng (điểm a khoản 1)**
1.	API Lấy thông tin lãi suất
2.	API Lấy thông tin tỷ giá
II	**Open API truy vấn thông tin của khách hàng (điểm b khoản 1)**
1.	API Xác nhận và lấy sự đồng ý của khách hàng
2.	API Lấy mã truy cập
3.	API Làm mới mã truy cập
4.	API Thu hồi mã truy cập
5.	API Lấy danh sách tài khoản
6.	API Lấy thông tin tài khoản
7.	API Lấy lịch sử giao dịch
III	**Open API khởi tạo thanh toán, nạp tiền vào ví điện tử, rút tiền ra khỏi ví điện tử (điểm c khoản 1)**
A	**Open API khởi tạo thanh toán**
1.	API Khởi tạo thanh toán

2.	API Xác nhận khách hàng luồng Redirect
3.	API Lấy mã truy cập luồng Redirect
4.	API Cập nhật trạng thái xác nhận thanh toán của khách hàng luồng Decoupled
5.	API Xác nhận thanh toán
6.	API Lấy trạng thái giao dịch
7.	API Lấy trạng thái xác nhận thanh toán của khách hàng luồng Decoupled
B	**Open API Nạp tiền vào ví điện tử**
1.	API Nạp ví điện tử
2.	API Xác nhận OTP
3.	API Cập nhật trạng thái xác nhận nạp ví điện tử của khách hàng luồng Decoupled
4.	API Lấy trạng thái xác nhận nạp ví điện tử của khách hàng luồng Decoupled
5.	API Xác nhận nạp ví điện tử
6.	API Lấy trạng thái giao dịch
C	**Open API Rút tiền ra khỏi ví điện tử**

1. Nguyên tắc và quy định kỹ thuật chung

- Đường dẫn của các Open API quy định tại Phụ lục này được đặt tên theo nguyên tắc thống nhất như sau: "https://<domain>/api/v1/...."

- Tham số trong các Open API quy định tại Phụ lục này là tối thiểu.

- Bên thứ ba (TPP) sử dụng mã số thuế hợp lệ còn hoạt động tại Việt Nam (TPP-ID) làm mã định danh.

- Ngân hàng sử dụng mã ngân hàng dùng trong hoạt động nghiệp vụ ngân hàng do Ngân hàng Nhà nước Việt Nam cấp cho các ngân hàng (Provider-ID) làm mã định danh.

- Sau khi kết nối và bảo đảm an toàn truyền thông giữa Ngân hàng và TPP theo tiêu chuẩn quy định tại Phụ lục 02, TPP phải đăng ký mã định danh của ứng dụng (client_id) và mã xác nhận định danh (client_secret) với Ngân hàng.

- Ngân hàng quản lý kết nối và quyền truy cập Open API với các TPP theo chuẩn OAuth 2.0 Authorization Framework trong RFC 6749. Tùy theo các nhóm API, các Ngân hàng sử dụng các luồng lấy mã truy cập trong RFC 6749 như sau:

+ Client credentials grant flow (mục 4.4 trong RFC 6749).

+ Authorization code grant flow (mục 4.1 trong RFC 6749) và kết hợp kỹ thuật PKCE trong RFC 7636 đối với một số API lấy mã truy cập.

- Căn cứ vào quy định tại Thông tư, phạm vi cung cấp Open API của các Ngân hàng chia thành các nhóm sau: INF, AIS, PIS và EWLTS.

- Thời gian hiệu lực của token cho từng nhóm nêu trên được quy định như sau:

+ Authorization Code (GET /authorize): loại token sử dụng một lần, thời gian hiệu lực 180 giây.

+ Access Token với grant_type là *client_credentials* (POST /token): thời gian hiệu lực tối đa 3600 giây.

+ Access Token với grant_type là *authorization_code* (POST /token): đối với nhóm AIS thời gian hiệu lực tối đa 3600 giây; đối với nhóm PIS token sử dụng một lần và có thời gian hiệu lực tối đa 300 giây.

+ Refresh token với grant_type là *refresh_token* (POST /token): chỉ áp dụng cho nhóm AIS, thời gian hiệu lực theo quy định đồng ý chia sẻ dữ liệu khách hàng tại khoản 6 Điều 11. Trong khoảng thời gian refresh_token đang còn hiệu lực, TPP có thể sử dụng refresh_token để lấy access_token mới từ hệ thống xác nhận của Ngân hàng mà không cần yêu cầu khách hàng phải thực hiện lại luồng lấy mã truy cập tại mục 3 phụ lục này.

- Thời gian hiệu lực của consentId (giá trị được sinh ra sau khi xác thực thành công khách hàng theo luồng Decoupled trong các nhóm PIS; EWLTS và luồng OTP nhóm EWLTS) là 300 giây.

- Giá trị của cột "Bắt buộc" trong các bảng mô tả các Open API phía dưới được quy định như sau:

+ M: bắt buộc.

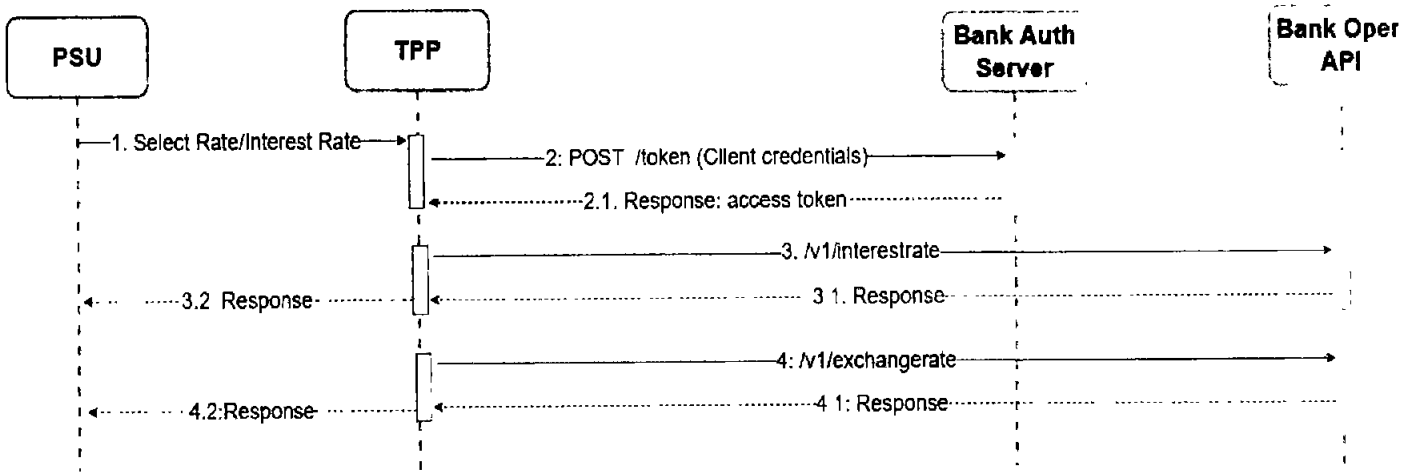
+ O: tùy chọn.

+ C: điều kiện.

- Các Open API có tham số trong Body được ký theo tiêu chuẩn RFC 7515 dạng Detached JWS.

- Các thành phần trong các hình vẽ luồng thực hiện trong Phụ lục này được thể hiện ở mức logic.

2. Các Open API truy vấn thông tin tỷ giá, lãi suất của Ngân hàng (điểm a khoản 1 Điều 6)



Hình 1. Luồng truy vấn thông tin tỷ giá, lãi suất của Ngân hàng (INF)

- Mô tả chi tiết luồng:

+ Bước 1: Trên ứng dụng của TPP, khách hàng thực hiện yêu cầu truy vấn thông tin tỷ giá hoặc lãi suất của một ngân hàng.

+ Bước 2: TPP thực hiện yêu cầu lấy **access_token** theo tiêu chuẩn **OAuth2.0** với **grant_type** là **client_credentials** (Chi tiết được mô tả tại mục 4.4 trong RFC 6749).

+ Bước 2.1. Hệ thống xác nhận của Ngân hàng kiểm tra thông tin trong yêu cầu và phản hồi cho TPP **access_token**.

Nếu khách hàng yêu cầu truy vấn thông tin lãi suất thì thực hiện tiếp bước 3:

+ Bước 3: TPP thực hiện gửi yêu cầu truy vấn lãi suất tới hệ thống của Ngân hàng thông qua API ***"API Lấy thông tin lãi suất"*** tại **mục 2.1**

+ Bước 3.1. Hệ thống của Ngân hàng phản hồi kết quả cho TPP.

+ Bước 3.2. Ứng dụng của TPP hiển thị kết quả trên giao diện cho khách hàng.

Nếu khách hàng yêu cầu truy vấn thông tin tỷ giá thì thực hiện tiếp bước 4:

+ Bước 4: TPP thực hiện gửi yêu cầu truy vấn tỷ giá tới hệ thống của Ngân hàng thông qua API ***"API Lấy thông tin tỷ giá"*** tại **mục 2.2**

+ Bước 4.1. Hệ thống của Ngân hàng phản hồi kết quả cho TPP.

+ Bước 4.2. Ứng dụng của TPP hiển thị kết quả trên giao diện cho khách hàng

2.1. API Lấy thông tin lãi suất

Endpoint	/v1/interestrate?currency={currency}
Method	GET
Scope	INF

- Request Header:

Content-Type	String	M	Mặc định "application/json"
Authorization	String	M	- Authorization định dạng: "Bearer + {access_token}": theo tiêu chuẩn RFC 6750. - Mã access_token được cấp theo quy định tại mục 4.4 trong RFC 6749 (với grant_type là client_credentials).
Request-DateTime	DateTime	M	- Ngày giờ thực hiện. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
Request-ID	String [60]	M	Mã định danh duy nhất cho request, thường ở định dạng UUID.
PSU-IP-Address	String [50]	O	Địa chỉ IP của khách hàng. Giá trị này phải ở dạng Ipv4 hoặc Ipv6.
PSU-User-Agent	String [200]	O	Thông tin trình duyệt trong trường hợp khách hàng sử dụng ứng dụng web của TPP hoặc các thông tin khác trong trường hợp khách hàng sử dụng ứng dụng khác của TPP.
PSU-Device-OS	String [100]	O	Hệ điều hành trên thiết bị (máy tính/di động,...) của khách hàng.
Provider-ID	String [8]	M	Mã định danh của Ngân hàng được quy định tại Mục 1.
TPP-ID	String [15]	M	Mã định danh của TPP được quy định tại Mục 1.

[illegible]	[illegible]	[illegible]	Mô tả
Client-ID	String [50]	O	Giá trị client_id được nêu tại Mục 1.

- Query parameter:

[illegible]			
currency	String [3]	M	Loại tiền tệ quy định theo mã của bộ ISO 4217 với 3 ký tự viết hoa.

- Response Header:

[illegible]			
Content-Type	String	M	Mặc định "application/json"
Request-ID	String	M	Giá trị được lấy từ request header trong API của TPP
Request-DateTime	String	M	Giá trị được lấy từ request header trong API của TPP
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Response Body:

+ HTTP STATUS CODE **200 OK:**

[illegible]				
interests		Array	M	Danh sách lãi suất
	currency	String [3]	M	Loại tiền tệ quy định theo mã của bộ ISO 4217 với 3 ký tự viết hoa.
	productCode	String [100]	O	Mã loại sản phẩm tiền gửi
	productDesc	String [300]	M	Mô tả loại sản phẩm tiền gửi
	termCode	String [100]	M	Kỳ hạn gửi
	minAmount	Number	M	Số tiền gửi tối thiểu
	customerType	String [4]	M	Loại khách hàng theo ISO 20022. Giá trị mặc định: "PRVT" (Khách hàng cá nhân)
	interestRate	String [5]	M	Lãi suất
	effectiveDate	Datetime	M	- Ngày hiệu lực. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
	additionalInfo	Object	O	Thông tin bổ sung (nếu có)

+ Error Code: Tham chiếu tại mục 7.2.1. Định dạng phản hồi lỗi và 7.2.2 Bảng mã lỗi chung.

2.2. API Lấy thông tin tỷ giá

Endpoint	/v1/exchangerate?currency={currency}
Method	GET
Scope	INF

- Request Header:

Content-Type	String	M	Mặc định "application/json"
Authorization	String	M	- Authorization định dạng: "Bearer + {access_token}": theo tiêu chuẩn RFC 6750. - Mã access_token được cấp theo quy định tại mục 4.4 trong RFC 6749 (với grant_type là client_credentials).
Request-DateTime	DateTime	M	- Ngày giờ thực hiện. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
Request-ID	String [60]	M	Mã định danh duy nhất cho request, thường ở định dạng UUID
PSU-IP-Address	String [50]	O	Địa chỉ IP của khách hàng. Giá trị này phải ở dạng Ipv4 hoặc Ipv6.
PSU-User-Agent	String [200]	O	Thông tin trình duyệt trong trường hợp khách hàng sử dụng ứng dụng web của TPP hoặc các thông tin khác trong trường hợp khách hàng sử dung ứng dụng khác của TPP.
PSU-Device-OS	String [100]	O	Hệ điều hành trên thiết bị (máy tính/di động,...) của khách hàng.
Provider-ID	String [8]	M	Mã định danh của Ngân hàng được quy định tại Mục 1.
TPP-ID	String [15]	M	Mã định danh của TPP được quy định tại Mục 1.
Client-ID	String [50]	O	Giá trị client_id được nêu tại Mục 1.

- Query parameter:

currency	String [3]	O	Loại tiền tệ quy định theo mã của bộ ISO 4217 với 3 ký tự viết hoa.

- Response Header:

Content-Type	String	M	Mặc định "application/json"

Request-ID	String	M	Giá trị được lấy từ request header trong API của TPP
Request-DateTime	String	M	Giá trị được lấy từ request header trong API của TPP
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Response Body:

+ HTTP STATUS CODE **200 OK:**

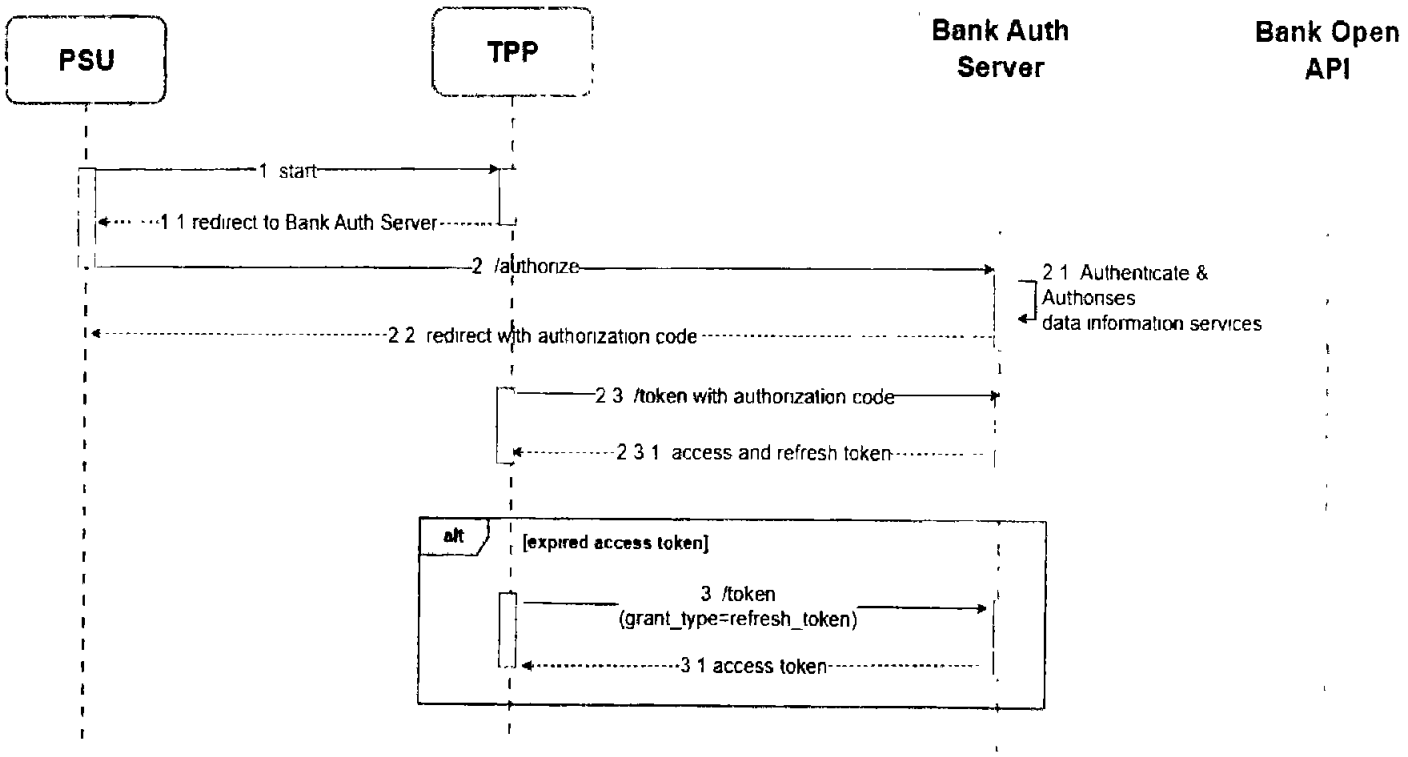
rates		Array	M	Danh sách tỷ giá
	currency	String [3]	M	Loại tiền tệ quy định theo mã của bộ ISO 4217 với 3 ký tự viết hoa
	buyCashRate	Number	M	Tỉ giá mua vào bằng tiền mặt
	buyTransferRate	Number	M	Tỉ giá mua vào bằng chuyển khoản
	sellCashRate	Number	M	Tỉ giá bán ra bằng tiền mặt
	sellTransferRate	Number	M	Tỉ giá bán ra bằng chuyển khoản
	additionalInfo	Object	O	Thông tin bổ sung (nếu có)
applyDate		DateTime	M	- Thời điểm áp dụng tỉ giá trên hệ thống của Ngân hàng. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.

+ **Error Code:** Tham chiếu tại mục 7.2.1. Định dạng phản hồi lỗi và 7.2.2 Bảng mã lỗi chung.

3. Các Open API truy vấn thông tin của khách hàng (điểm b khoản 1 Điều 6)

Chỉ áp dụng với các truy vấn mà khách hàng chủ động thực hiện trên ứng dụng của TPP.

- Luồng lấy mã truy cập của khách hàng được thực hiện khi lấy sự đồng ý chia sẻ dữ liệu của khách hàng được khởi tạo trên ứng dụng của TPP được mô tả như sau:



Hình 2 Luồng lấy mã truy cập

+ Bước 1: Khách hàng đăng nhập vào ứng dụng của TPP và thực hiện dịch vụ liên quan tới sự đồng ý chia sẻ dữ liệu của khách hàng do TPP cung cấp.

• Nếu khách hàng chưa thực hiện đồng ý chia sẻ dữ liệu hoặc đã hết thời gian đồng ý được quy định tại **khoản 6 Điều 11** thì tiếp tục thực hiện các **Bước từ 1.1 đến Bước 2.4**.

• Nếu thời gian đồng ý còn hiệu lực và **access_token** hết hiệu lực thì thực hiện tiếp từ **Bước 3.**

+ Bước 1.1. Hệ thống của TPP sẽ điều hướng khách hàng tới trang xác nhận của Ngân hàng.

+ Bước 2: Khách hàng được điều hướng tới trang xác nhận của Ngân hàng để lấy sự đồng ý chia sẻ dữ liệu của khách hàng thông qua API "***Xác nhận và lấy sự đồng ý của khách hàng***" tại **mục 3.1**. Tại đây, khách hàng thực hiện đăng nhập vào hệ thống xác nhận của Ngân hàng.

+ Bước 2.1. Hệ thống xác nhận của Ngân hàng xác nhận khách hàng. Sau khi xác nhận thành công, khách hàng xác nhận đồng ý chia sẻ dữ liệu thông qua giao diện của Ngân hàng.

+ Bước 2.2: Hệ thống xác nhận của Ngân hàng chuyển hướng khách hàng về ứng dụng của TPP kèm mã đồng ý **(authorization code)**. Chi tiết được mô ta tại **mục 3.1**

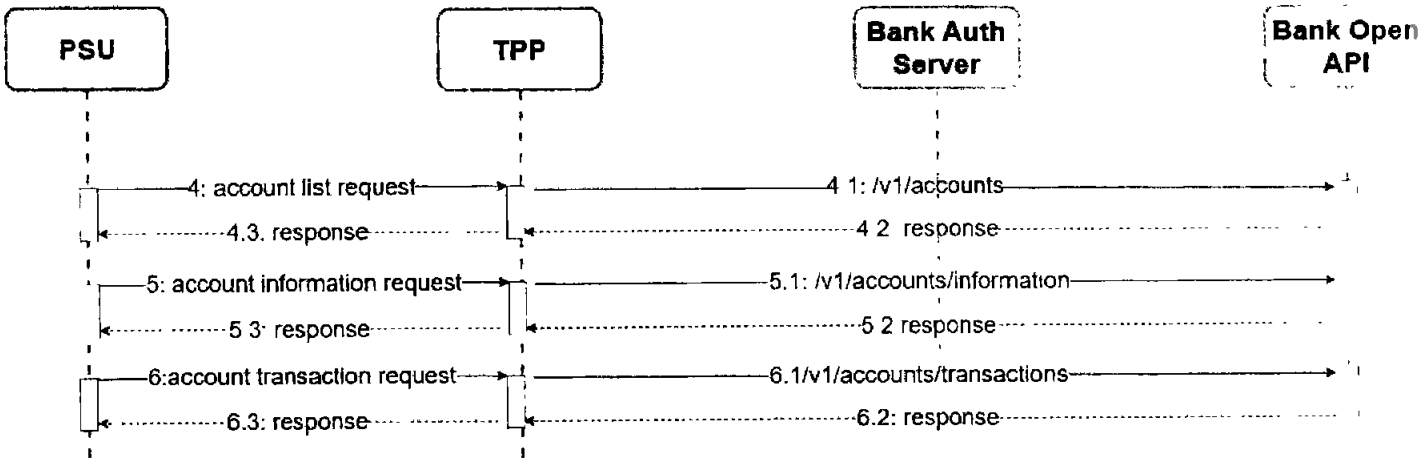
+ Bước 2.3: TPP gửi yêu cầu lấy **access_token** và **refresh_token** tới hệ thống xác nhận của Ngân hàng. Chi tiết được mô tả tại API "***Lấy mã truy cập***" tại **mục 3.2**.

+ Bước 2.3.1: Hệ thống xác nhận của Ngân hàng thực hiện phản hồi kết qua cho TPP. TPP sử dụng **access_token** để thực hiện các truy vấn liên quan về AIS. TPP sử dụng **refresh_token** để thực hiện làm mới **access_token** khi **access_token** hết hạn thực hiện tại Bước 3.

+ Bước 3: Trường hợp **access_token** hết hạn, TPP thực hiện gọi yêu cầu làm mới **access_token** dựa trên **refresh_token**. Chi tiết được mô tả tại API ***"Làm mới mã truy cập"*** tại **mục 3.3.**

+ Bước 3.1: Hệ thống xác nhận của Ngân hàng thực hiện phản hồi kết quả cho TPP.

- **Luồng truy vấn thông tin tài khoản** với **access_token** được lấy ở luồng lấy mã truy cập (hình 2) được mô tả như sau:



Hình 3· Luồng truy vấn thông tin tài khoản

+ Bước 4: Khách hàng gửi yêu cầu lấy danh sách tài khoản trên ứng dụng của TPP.

+ Bước 4.1: TPP gửi yêu cầu lấy danh sách tài khoản tới hệ thống của Ngân hàng thông qua API ***"Lấy danh sách tài khoản"*** tại **mục 3.5.**

+ Bước 4.2: Hệ thống của Ngân hàng phản hồi kết quả cho TPP.

+ Bước 4.3: Ứng dụng TPP hiển thị kết quả danh sách tài khoản trên giao diện cho khách hàng.

Nếu khách hàng yêu cầu lấy thông tin một tài khoản thì thực hiện tiếp bước 5:

+ Bước 5: Khách hàng gửi yêu cầu lấy thông tin một tài khoản trên ứng dụng cua TPP.

+ Bước 5.1: TPP gửi yêu cầu lấy thông tin một tài khoản tới hệ thống của Ngân hàng thông qua API ***"Lấy thông tin tài khoản"*** tại **mục 3.6**.

+ Bước 5.2: Hệ thống của Ngân hàng phản hồi kết quả cho TPP.

+ Bước 5.3: Ứng dụng TPP hiển thị kết quả thông tin tài khoản trên giao diện cho khách hàng.

Nếu khách hàng yêu cầu lấy lịch sử giao dịch thì thực hiện tiếp bước 6:

+ Bước 6: Khách hàng gửi yêu cầu lấy lịch sử giao dịch trên ứng dụng của TPP.

+ Bước 6.1: TPP gửi yêu cầu lấy lịch sử giao dịch tới hệ thống của Ngân hàng thông qua API ***"Lấy lịch sử giao dịch"*** tại **mục 3.7**.

+ Bước 6.2: Hệ thống của Ngân hàng phản hồi kết qua cho TPP

+ Bước 6.3: Ứng dụng TPP hiển thị kết quả thông tin lịch sử giao dịch trên giao diện cho khách hàng.

3.1. API Xác nhận và lấy sự đồng ý của khách hàng

Endpoint	/authorize
Method	GET

- Request Header:

Content-Type	String	M	application/x-www-form-urlencoded
Host	String	O	Xác định tên miền của máy chủ mà request đang gửi đến

- Query Parameter:

response_type	String	M	Mặc định "code"
client_id	String	M	Giá trị client_id được nêu tại Mục 1.
scope	String	M	Phạm vi truy cập: AIS
redirect_uri	String	M	Đường dẫn dùng để điều hướng khách hàng về ứng dụng của TPP sau khi hệ thống xác nhận của Ngân hàng hoàn thành xác nhận khách hàng.
state	String	M	Giá trị này được TPP tạo ra để duy trì trạng thái giữa request và respone, được sử dụng để ngăn chặn các cuộc tấn công trong lĩnh vực bảo mật web (Cross-site request forgery)
code_challenge	String	M	code_challenge = BASE64URL-ENCODE(SHA256(ASCII(code_verifier))) Chi tiết tham khảo thêm tại RFC 7636
code_challenge_method	String	O	Thuật toán được sử dụng để tạo ra code_challenge. Mặc định "S256"

- Response:

+ Hệ thống xác nhận của Ngân hàng điều hướng khách hàng về ứng dụng của TPP thông qua redirect_uri kèm với tham số trên đường dẫn được mô ta ở bảng dưới đây:

code	String	M	Mã đồng ý

state	String	M	Giá trị state từ request cua TPP.

+ **Error Code:** Tham chiếu tại mục 7.1.2. Mã lỗi API xác nhận và lấy sự đồng ý của khách hàng.

3.2. API Lấy mã truy cập

Endpoint	/token
Method	POST

- Request Header:

Content-Type	String	M	application/x-www-form-urlencoded
Authorization	String	M	Basic BASE64(client_id + ":" + client_secret)
Host	String	O	Xác định tên miền của máy chủ mà request đang gửi đến

- Request body:

grant_type	String	M	Mặc định "authorization_code"
code	String	M	Mã đồng ý mà Ngân hàng đã cấp cho TPP thông qua luồng lấy mã truy cập.
redirect_uri	String	M	Đường dẫn dùng để điều hướng khách hàng trở lại ứng dụng của TPP. Giá trị này phải khớp với giá trị redirect_uri đã truyền tại API Xác nhận và lấy sự đồng ý của khách hàng mục 3.1.
code_verifier	String	M	Giá trị code_verifier được sử dụng để tạo ra code_challenge mà TPP đã truyền tại API Xác nhận và lấy sự đồng ý của khách hàng mục 3.1. Chi tiết tham khảo thêm RFC 7636.

- Response Header:

Content-Type	String	M	Mặc định "application/json"

- Response body:

+ HTTP STATUS CODE **200 OK:**

access_token	String	M	Mã truy cập.
refresh_token	String	M	Mã làm mới.
token_type	String	M	Mặc định "Bearer"
expires_in	Number	M	Giá trị hiệu lực của access_token đã được mô tả tại Mục 1 đối với nhóm AIS

scope	String	M	Phạm vi của access_token. Giá trị này khớp với scope tại API Xác nhận và lấy sự đồng ý của khách hàng mục 3.1

+ Error Code: Tham chiếu tại mục 7.1.2. Mã lỗi API Lấy mã truy cập.

3.3. API Làm mới mã truy cập

Endpoint	/token
Method	POST

- Request Header:

Content-Type	String	M	application/x-www-form-urlencoded
Authorization	String	M	Basic BASE64(client_id + ":" + client_secret)
Host	String	O	Xác định tên miền của máy chủ mà request đang gửi đến

- Request body:

grant_type	String	M	Mặc định "refresh_token"
refresh_token	String	M	Giá trị refresh_token được trả về tại mục API Lấy mã truy cập
scope	String	O	Phạm vi (scope) không được vượt quá phạm vi (scope) tại API Xác nhận và lấy sự đồng ý của khách hàng mục 3.1.

- Response Header:

Content-Type	String	M	Mặc định "application/json"

- Response body:

+ HTTP STATUS CODE **200 OK:**

access_token	String	M	Mã truy cập.
refresh_token	String	O	Mã làm mới (Mã này có thể khác giá trị mã làm mới được sinh ra từ luồng lấy mã truy cập với grant_type authorization_code)
token_type	String	M	Mặc định "Bearer"
expires_in	Number	M	Giá trị hiệu lực của access_token đã được mô tả tại Mục 1 đối với nhóm AIS

+ Error code: Tham chiếu tại mục 7.1.2. Mã lỗi API Lấy mã truy cập.

3.4. API Thu hồi mã truy cập

TPP thực hiện gọi API này khi khách hàng thực hiện rút lại sự đồng ý trên ứng dụng của TPP.

Endpoint	/revoke
Method	POST

- Request Header:

Content-Type	String	M	application/x-www-form-urlencoded
Authorization	String	M	Basic BASE64(client_id + ":" + client_secret)
Host	String	O	Xác định tên miền của máy chủ mà request đang gửi đến

- Request body:

token	String	M	Giá trị của access_token hoặc refresh_token cần thu hồi
token_type_hint	String	O	Loại token cần thu hồi "access_token" hoặc "refresh_token"

- Response:

+ HTTP STATUS CODE **200 OK** và không có dữ liệu trả về. Tham khảo chi tiết RFC 7009.

+ Error code: Tham chiếu tại mục 7.1.2. Mã lỗi API Lấy mã truy cập.

3.5. API Lấy danh sách tài khoản

Endpoint	/v1/accounts
Method	GET
Scope	AIS

- Request Header:

Content-Type	String	M	Mặc định "application/json"
Authorization	String	M	- Authorization định dạng: "Bearer + {access_token}": theo tiêu chuẩn RFC 6750. - Mã access_token được cấp theo quy định tại mục 4.1 trong RFC 6749 (Authorization Code Grant).
Request-DateTime	DateTime	M	- Ngày giờ thực hiện. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339

Request-ID	String [60]	M	Mã định danh duy nhất cho request, thường ở định dạng UUID
PSU-IP-Address	String [50]	O	Địa chỉ IP của khách hàng. Giá trị này phải ở dạng IPv4 hoặc IPv6.
PSU-User-Agent	String [200]	O	Thông tin trình duyệt trong trường hợp khách hàng sử dụng ứng dụng web của TPP hoặc các thông tin khác trong trường hợp khách hàng sử dụng ứng dụng khác của TPP.
PSU-Device-OS	String [100]	O	Hệ điều hành trên thiết bị (máy tính/di động,...) của khách hàng.
Provider-ID	String [8]	M	Mã định danh của Ngân hàng được quy định tại Mục 1.
TPP-ID	String [15]	M	Mã định danh của TPP được quy định tại Mục 1.
Client-ID	String [50]	O	Giá trị client_id được nêu tại Mục 1

- Query parameter: Không có

- Response Header:

Content-Type	String	M	Mặc định "application/json"
Request-ID	String	M	Giá trị được lấy từ request header trong API của TPP
Request-DateTime	DateTime	M	Giá trị được lấy từ request header trong API của TPP
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Response body:

+ HTTP STATUS CODE **200 OK:**

accounts			Array		Danh sách tài khoản
	identification		Object	M	Thông tin tài khoản của khách hàng mở tại Ngân hàng.
		accountId	String [34]	M	Số tài khoản của khách hàng
	name		String [70]	M	Tên tài khoản của khách hàng.
	type		String [4]	M	Loại tài khoản quy định trong ISO 20022.
	currency		String [3]	M	Loại tiền tệ quy định theo mã của bộ ISO 4217 với 3 ký tự viết hoa.

	bankCode		String [8]	M	Mã định danh cua Ngân hàng được quy định tại Mục 1
	additionalInfo		Object	O	Thông tin bổ sung (nếu có)

+ **Error Code:** Tham chiếu tại mục 7.2.1. Định dạng phan hồi lỗi và 7.2.2 Bảng mã lỗi chung.

3.6. API Lấy thông tin tài khoản

Endpoint	/v1/accounts/information
Method	POST
Scope	AIS

- Request Header:

Content-Type	String	M	Mặc định "application/json"
Authorization	String	M	- Authorization định dạng: "Bearer + {access_token}": theo tiêu chuẩn RFC 6750. - Mã access_token được cấp theo quy định tại mục 4.1 trong RFC 6749 (Authorization Code Grant).
Request-DateTime	DateTime	M	- Ngày giờ thực hiện. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime). theo tiêu chuẩn RFC 3339.
Request-ID	String [60]	M	Mã định danh duy nhất cho request, thường ở định dạng UUID
PSU-IP-Address	String [50]	O	Địa chỉ IP của khách hàng. Giá trị này phải ở dạng IPv4 hoặc IPv6.
PSU-User-Agent	String [200]	O	Thông tin trình duyệt trong trường hợp khách hàng sử dụng ứng dụng web của TPP hoặc các thông tin khác trong trường hợp khách hàng sử dụng ứng dụng khác của TPP.
PSU-Device-OS	String [100]	O	Hệ điều hành trên thiết bị (máy tính/di động,...) của khách hàng.
Provider-ID	String [8]	M	Mã định danh của Ngân hàng được quy định tại Mục 1.
TPP-ID	String [15]	M	Mã định danh của TPP được quy định tại Mục 1.
Client-ID	String [50]	O	Giá trị client_id được nêu tại Mục 1
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Request Body:

accountId	String [34]	M	Số tài khoản của khách hàng.

- Response Header:

Content-Type	String	M	Mặc định "application/json"
Request-ID	String	M	Giá trị được lấy từ request header trong API của TPP
Request-DateTime	DateTime	M	Giá trị được lấy từ request header trong API của TPP
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Response Body:

+ HTTP STATUS CODE **200 OK:**

identification			Object	M	Thông tin số tài khoản của khách hàng
	accountId		String [34]	M	Số tài khoản của khách hàng
name			String [70]	M	Tên tài khoản của khách hàng.
type			String [4]	M	Loại tài khoản quy định trong ISO 20022.
currency			String [3]	M	Loại tiền tệ quy định theo mã của bộ ISO 4217 với 3 ký tự viết hoa
bankCode			String [8]	M	Mã định danh của Ngân hàng được quy định tại Mục 1 của Phụ lục.
creationDate			Datetime	M	- Ngày tạo tài khoản. - Định dang: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
balances			Array	M	Thông tin về chi tiết số dư
	amount		Object	M	Thông tin về số dư khả dụng

		value	Number	M	Số dư khả dụng trên tài khoản của khách hàng
		currency	String [3]	O	Loại tiền tệ quy định theo mã của bộ ISO 4217 với 3 ký tự viết hoa.
	dateTime		DateTime	M	- Ngày giờ hệ thống thực hiện. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
additionalInfo			Object	O	Thông tin bổ sung (nếu có)

+ Error Code: Tham chiếu tại mục 7.2.1. Định dạng phản hồi lỗi và 7.2.2 Bảng mã lỗi chung.

3.7. API Lấy lịch sử giao dịch

- Khoảng thời gian cho phép truy vấn lịch sử giao dịch tùy thuộc vào quy định của Ngân hàng.

Endpoint	/v1/accounts/transactions
Method	POST
Scope	AIS

- Request Header:

Content-Type	String	M	Mặc định "application/json"
Authorization	String	M	- Authorization định dạng: "Bearer + {access_token}": theo tiêu chuẩn RFC 6750. - Mã access_token được cấp theo quy định tại mục 4.1 trong RFC 6749 (Authorization Code Grant).
Request-DateTime	DateTime	M	- Ngày giờ thực hiện. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime). theo tiêu chuẩn RFC 3339.
Request-ID	String [60]	M	Mã định danh duy nhất cho request. thường ở định dạng UUID.
PSU-IP-Address	String [50]	O	Địa chỉ IP của khách hàng. Giá trị này phải ở dạng Ipv4 hoặc Ipv6.

PSU-User-Agent	String [200]	O	Thông tin trình duyệt trong trường hợp khách hàng sử dụng ứng dụng web của TPP hoặc các thông tin khác trong trường hợp khách hàng sử dụng ứng dụng khác của TPP.
PSU-Device-OS	String [100]	O	Hệ điều hành trên thiết bị (máy tính/di động,...) của khách hàng.
Provider-ID	String [8]	M	Mã định danh của Ngân hàng được quy định tại Mục 1.
TPP-ID	String [15]	M	Mã định danh của TPP được quy định tại Mục 1.
Client-ID	String [50]	O	Giá trị client_id được nêu tại Mục 1.
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1.

- Request Body:

accountId	String [34]	M	Số tài khoản của khách hàng.
fromDate	DateTime	M	- Thời gian giao dịch từ ngày. - Định dạng: yyyy-MM-ddTHH:mm.ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
toDate	DateTime	M	- Thời gian giao dịch đến ngày. - Định dạng: yyyy-MM-ddTHH:mm.ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
page	Number	O	Xác định số trang được yêu cầu. Các trang được đánh số từ 1. Nếu tham số không được chỉ định, API sẽ trả về trang số 1.
size	Number	O	Xác định số lượng bản ghi trên một trang. Nếu tham số không được chỉ định, API sẽ trả về toàn bộ các bản ghi thoả mãn yêu cầu.

- Response Header:

Content-Type	String	M	Mặc định "application/json"
Request-ID	String	M	Giá trị được lấy từ request header trong API của TPP
Request-DateTime	DateTime	M	Giá trị được lấy từ request header trong API của TPP
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Response Body:

+ HTTP STATUS CODE **200 OK:**

pageCount				Number	M	Tổng số trang

pageNumber				Number	M	Trang hiện tai
nextPage				Number	O	Trang tiếp theo
pageSize				Number	M	Số bản ghi trên một trang
totalCount				Number	O	Tổng số bản ghi trên tất cả các trang
transactions				Array	M	Danh sách dữ liệu về lịch sử giao dịch
	amount			Object	M	Thông tin số tiền giao dịch
		value		Number	M	Số tiền giao dịch
		currency		String [3]	M	Loại tiền tệ quy định theo mã của bộ ISO 4217 với 3 ký tự viết hoa
	balances			Object	M	Thông tin số dư
		value		Number	M	Số dư ở thời điểm giao dịch
		currency		String [3]	M	Loai tiền tệ quy định theo mã của bộ ISO 4217 với 3 ký tự viết hoa
	creditDebitIndicator			String [4]	M	- CRDT (Credit) nếu là số dư ghi có - DBIT (Debit) nếu là số dư ghi nợ
	reversalIndicator			boolean	O	Chỉ ra một giao dịch đã bị đảo ngược hoặc huỷ bỏ. Có thể bao gồm các giao dịch bị hoàn tiền, bị huỷ bỏ.
	valueDate			DateTime	M	- Thời gian giao dịch. - Định dạng. yyyy-MM-ddTHH:mm:ssZ (UTC

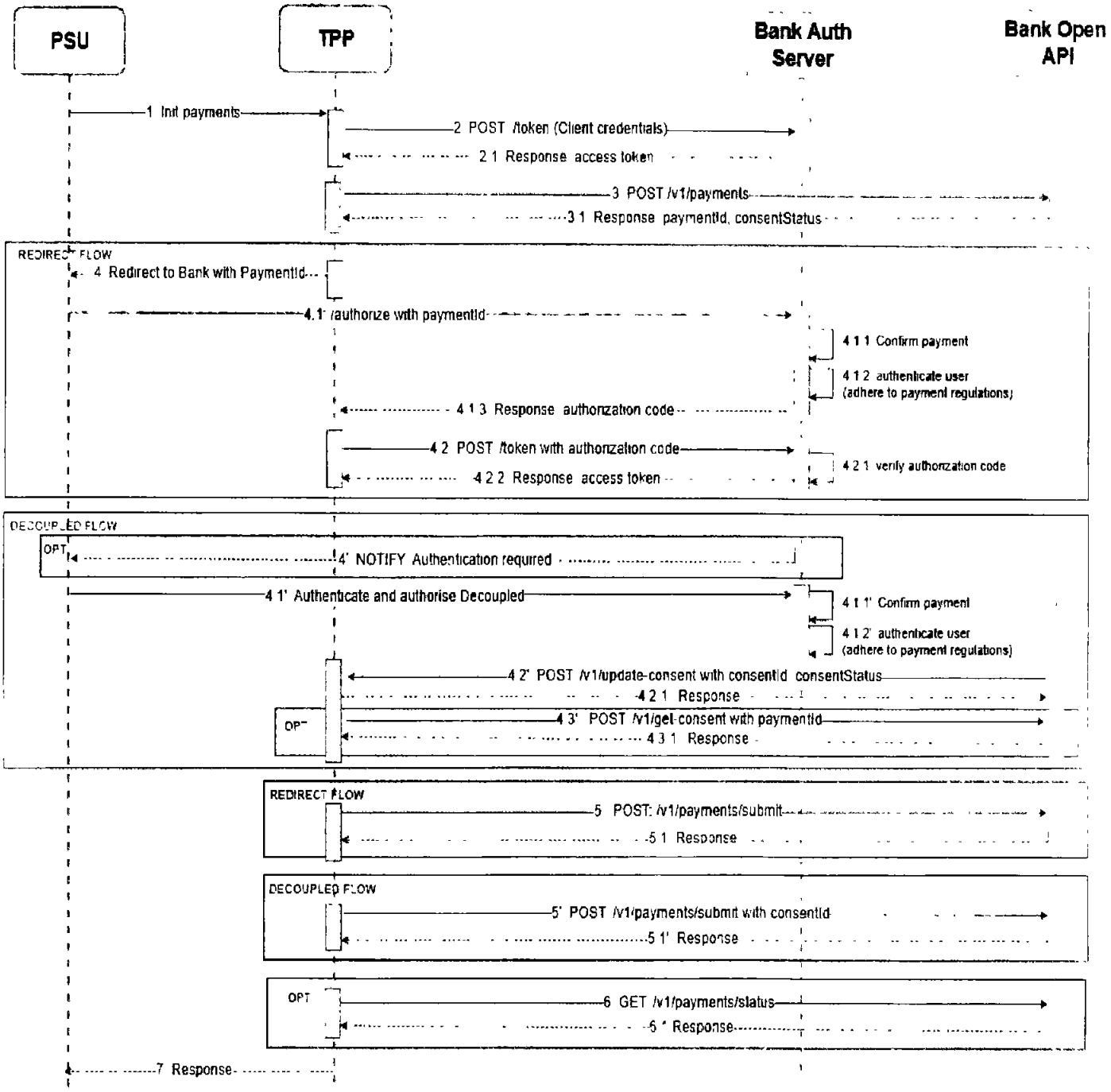
						Mô tả
						DateTime), theo tiêu chuẩn RFC 3339.
	references			Object	M	Thông tin mã định danh giao dịch
		instructionIdentification		String [70]	M	Mã định danh duy nhất cho mỗi giao dịch
	relatedParties			Object	O	Thông tin gửi nhận
		debtor		Object	O	Thông tin bên chuyển tiền
			name	String [140]	O	Tên của bên chuyển tiền
			bankCode	String [8]	O	Mã định danh của Ngân hàng của bên chuyển được quy định tại Mục 1
			accountId	String [34]	O	Số tài khoản.
		creditor		Object	O	Thông tin bên nhận
			name	String [140]	O	Tên cua bên nhận
			bankCode	String [8]	O	Mã định danh của Ngân hàng của bên nhận được quy định tại Mục 1
			accountId	String [34]	O	Số tài khoản của bên nhận
	additionalTransactionInformation			String [255]	M	Nội dung giao dịch
	additionalInfo			Object	O	Thông tin bổ sung (nếu có)

+ Error Code: Tham chiếu tại mục 7.2.1. Định dạng phản hồi lỗi và 7.2.2 Bảng mã lỗi chung.

4. Các Open API khởi tạo thanh toán (điểm c khoản 1 Điều 6)

Chỉ áp dụng với các lệnh thanh toán mà khách hàng chủ động thực hiện trên ứng dụng của TPP.

- Luồng triển khai các API khởi tạo thanh toán:



Hình 4: Luồng triển khai các API thanh toán (PIS)

- Mô tả chi tiết luồng:

+ Bước 1: Khách hàng thực hiện yêu cầu thanh toán trên ứng dụng của TPP.

+ Bước 2: TPP thực hiện yêu cầu lấy **access_token** theo tiêu chuẩn **OAuth2.0** với **grant_type** là **client_credentials** (Chi tiết được mô tả tại mục 4.4 trong RFC 6749).

+ Bước 2.1 Hệ thống xác nhận của Ngân hàng kiểm tra thông tin trong yêu cầu và phan hồi cho TPP **access_token**.

+ Bước 3: TPP thực hiện gửi yêu cầu khởi tạo thanh toán tới Ngân hàng thông qua API ***"Khởi tạo thanh toán"*** tại **mục 4.1**.

+ Bước 3.1. Hệ thống của Ngân hàng thực hiện kiểm tra các thông tin từ yêu cầu của TPP. Khi các thông tin hợp lệ, hệ thống của Ngân hàng trả về cho TPP một mã giao dịch duy nhất (**paymentId**), trạng thái **consentStatus** có giá trị là "AWAITTING_AUTH".

Với luồng redirect (các bước từ 4 đến 5.1):

+ Bước 4: Sau khi TPP nhận được paymentId, TPP điều hướng khách hàng tới trang xác nhận của Ngân hàng để thực hiện xác nhận thanh toán.

+ Bước 4.1: Khách hàng thực hiện đăng nhập. Chi tiết được mô tả tại API "***Xác nhận khách hàng***" tại **mục 4.2**.

+ Bước 4.1.1. Khách hàng xác nhận thông tin thanh toán trên giao diện của Ngân hàng.

+ Bước 4.1.2. Khách hàng xác nhận thanh toán theo các phương thức xác nhận của Ngân hàng bảo đảm tuân thủ quy định của pháp luật.

+ Bước 4.1.3: Hệ thống xác nhận của Ngân hàng chuyển hướng khách hàng về ứng dụng của TPP kèm mã đồng ý (**authorization code**).

+ Bước 4.2: TPP gửi yêu cầu lấy access_token tới hệ thống xác nhận của Ngân hàng. Chi tiết được mô tả tại API "***Lấy mã truy cập***" tại **mục 4.3**

+ Bước 4.2.1: Hệ thống xác nhận của Ngân hàng thực hiện kiểm tra các thông tin mã đồng ý từ yêu cầu của TPP.

+ Bước 4.2.2: Hệ thống xác nhận của Ngân hàng thực hiện phản hồi **access_token** cho TPP.

+ Bước 5: TPP thực hiện gửi yêu cầu xác nhận thanh toán tới Ngân hàng thông qua API "***Xác nhận thanh toán***" tại **mục 4.5**.

+ Bước 5.1. Ngân hàng phản hồi kết quả thanh toán.

Với luồng decoupled (các bước từ 4' đến 5.1'):

+ Bước 4': Tùy theo thiết kế ứng dụng của TPP và Hệ thống cua Ngân hàng mà Hệ thống xác nhận của Ngân hàng thực hiện hoặc không thực hiện gui thông báo tới khách hàng có một thanh toán cần được xác nhận.

+ Bước 4.1': Khách hàng truy cập ứng dụng của Ngân hàng.

+ Bước 4.1.1': Khách hàng xác nhận thông tin thanh toán trên giao diện cua Ngân hàng.

+ Bước 4.1.2': Khách hàng xác nhận thanh toán theo các phương thức xác nhận do Ngân hàng quy định và bảo đảm tuân thủ quy định của pháp luật.

+ Bước 4.2': Hệ thống của Ngân hàng gửi yêu cầu cập nhật trạng thái xác nhận thanh toán của khách hàng tới TPP thông qua API ***"Cập nhật trạng thái xác nhận thanh toán của khách hàng luồng decoupled"*** tại **mục 4.4**.

+ Bước 4.2.1`: TPP nhận được trạng thái xác nhận thanh toán của khách hàng và phản hồi kết quả lại cho hệ thống của Ngân hàng, chi tiết tại **mục 4.4**.

+ Bước 4.3`: Trong trường hợp TPP không nhận được trạng thái xác nhận thanh toán của khách hàng thông qua API ***"Cập nhật trạng thái xác nhận thanh toán của khách hàng luồng decoupled"*** tại **mục 4.4** từ hệ thống của Ngân hàng thì TPP có thể gửi yêu cầu lấy trạng thái xác nhận thanh toán của khách hàng tới hệ thống của Ngân hàng thông qua API ***"Lấy trạng thái xác nhận thanh toán của khách hàng luồng Decoupled"*** tại **mục 4.7**.

+ Bước 4.3.1`: Hệ thống của Ngân hàng nhận được yêu cầu và phản hồi kết quả lại cho TPP.

+ Bước 5`: TPP thực hiện gửi yêu cầu xác nhận thanh toán tới Ngân hàng thông qua API "***Xác nhận thanh toán***" kèm thông tin consentId tại **mục 4.5**.

+ Bước 5.1`: Hệ thống cua Ngân hàng nhận được yêu cầu và phản hồi kết quả lại cho TPP, chi tiết tại **mục 4.5**.

+ Bước 6: Trong trường hợp TPP không nhận được phản hồi kết quả hạch toán từ Ngân hàng, TPP gửi yêu cầu lấy trạng thái giao dịch tới hệ thống của Ngân hàng thông qua API "***Lấy trạng thái giao dịch***" tại **mục 4.6**.

+ Bước 6.1: Hệ thống của Ngân hàng nhận được yêu cầu và phản hồi kết quả lại cho TPP.

+ Bước 7: TPP hiển thị kết quả thanh toán cho khách hàng.

4.1. API Khởi tạo thanh toán

Endpoint	/v1/payments
Method	POST
Scope	PIS

- Request Header:

Content-Type	String	M	Mặc định "application/json"
Authorization	String	M	- Authorization định dạng: "Bearer + {access_token}": theo tiêu chuẩn RFC 6750 - Mã access_token được cấp theo quy định tại mục 4.4 trong RFC 6749 (với grant_type là client_credentials).
Request-DateTime	DateTime	M	- Ngày giờ thực hiện. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
Request-ID	String [60]	M	Mã định danh duy nhất cho request, thường ở định dạng UUID
PSU-IP-Address	String [50]	O	Địa chỉ IP của khách hàng. Giá trị này phải ở dạng IPv4 hoặc IPv6.
PSU-User-Agent	String [200]	O	Thông tin trình duyệt trong trường hợp khách hàng sử dụng ứng dụng

Tham số	Loại dữ liệu	Bắt buộc	Mô tả
			web của TPP hoặc các thông tin khác trong trường hợp khách hàng sử dụng ứng dụng khác của TPP.
PSU-Device-OS	String [100]	O	Hệ điều hành trên thiết bị (máy tính/di động,...) của khách hàng.
Provider-ID	String [8]	M	Mã định danh của Ngân hàng được quy định tại Mục 1.
TPP-ID	String [15]	M	Mã định danh của TPP được quy định tại Mục 1.
Client-ID	String [50]	O	Giá trị client_id được nêu tại Mục 1.
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Request Body:

instructionIdentification		String [50]	M	Mã giao dịch do TPP khởi tạo
debtor		Object	C	Thông tin người thực hiện thanh toán, không bắt buộc trong trường hợp thanh toán với dịch vụ Cổng thanh toán
	name	String [70]	C	Tên tài khoản của người thực hiện thanh toán
	accountId	String [34]	C	Số tài khoản của người thực hiện thanh toán
	bankCode	String [8]	C	Mã định danh của Ngân hàng của người thực hiện thanh toán được quy định tại Mục 1.
remittanceInformation		String [255]	M	Nội dung giao dịch
instructedAmount		Object	M	Thông tin số tiền giao dịch
	value	Number	M	Số tiền giao dịch
	currency	String [3]	M	Loại tiền tệ quy định theo mã của bộ ISO 4217 với 3 ký tự viết hoa.
requestedExecutionDate		DateTime	M	- Ngày thực hiện giao dịch. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
additionalInfo		Object	O	Thông tin bổ sung (nếu có)

- Response Header:

Content-Type	String	M	Mặc định "application/json"
Request-ID	String	M	Giá trị được lấy từ request header trong API của TPP
Request-DateTime	String	M	Giá trị được lấy từ request header trong API của TPP
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Response Body:

+ HTTP STATUS CODE **200 OK:**

paymentId	String [35]	M	Mã giao dịch duy nhất do Ngân hàng cung cấp.
status	String [4]	M	Mã trạng thái của giao dịch. Theo tiêu chuẩn của ISO 20022.
statusDateTime	DateTime	M	- Thời điểm cập nhật trạng thái. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
consentStatus	String [20]	M	Mặc định: "AWAITTING_AUTH"

+ Error Code: Tham chiếu tại mục 7.2.1. Định dạng phản hồi lỗi và 7.2.2 Bang mã lỗi chung.

4.2. API Xác nhận khách hàng luồng Redirect

Endpoint	/authorize
Method	GET

- Request Header:

Content-Type	String	M	application/x-www-form-urlencoded
Host	String	O	Xác định tên miền của máy chủ mà request đang gửi đến

- Query Parameter:

response_type	String	M	Giá trị mặc định "code id_token"
client_id	String	M	Giá trị client_id được nêu tại Mục 1.
scope	String	M	Phạm vi truy cập: PIS
redirect_uri	String	M	Đường dẫn dùng để điều hướng khách hàng về ứng dụng của TPP sau khi hệ thống xác nhận của Ngân hàng hoàn thành xác nhận khách hàng.

state	String	M	Giá trị này được TPP tạo ra để duy trì trạng thái giữa request và respone, được sử dụng để ngăn chặn các cuộc tấn công trong lĩnh vực bảo mật web (Cross-site request forgery)
code_challenge	String	M	code_challenge = BASE64URL-ENCODE(SHA256(ASCII(code_verifier))) Chi tiết tham khảo thêm tại RFC 7636
code_challenge_method	String	O	Thuật toán được sử dụng để tạo ra code_challenge. Mặc định "S256"
request	String	M	Json Web Token (JWT). Sử dụng giá trị paymentId nhận được từ API khởi tạo thanh toán mục 4.1 đưa vào claim trong payload. Chuỗi thông tin JWT bao gồm: + JOSE Header – theo JWT trong RFC 7519, JWS trong RFC 7515. Thuật toán trong header "alg" theo mục 3.1 trong RFC 7518. + payload + signature – JWS trong RFC 7515

- Response:

+ Hệ thống xác nhận của Ngân hàng điều hướng khách hàng về ứng dụng của TPP thông qua redirect_uri kèm với giá trị ở bảng dưới đây:

code	String	M	Mã đồng ý
state	String	M	Giá trị state từ request của TPP.
id_token	String	O	Json Web Token (JWT). Sử dụng giá trị paymentId nhận được từ API khởi tạo thanh toán mục 4.1 đưa vào trong payload. - Chuỗi thông tin JWT bao gồm: + JOSE Header – theo JWT trong RFC 7519, JWS trong RFC 7515. Thuật toán trong header "alg" theo mục 3.1 trong RFC 7518; + payload; + signature – theo JWS trong RFC7515.

+ Error Code: Tham chiếu tại mục 7.1.2. Mã lỗi API Lấy mã truy cập.

4.3. API Lấy mã truy cập luồng Redirect

Request-ID	String	M	Giá trị được lấy từ request header trong API của TPP
Request-DateTime	String	M	Giá trị được lấy từ request header trong API của TPP
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Response Body:

+ HTTP STATUS CODE **200 OK:**

message	String [20]	M	Mặc định "Success"

+ Error Code: Theo quy định của TPP.

4.5. API Xác nhận thanh toán

Endpoint	/v1/payments/submit
Method	POST
Scope	PIS

- Request Header:

Content-Type	String	M	Mặc định "application/json"
Authorization	String	M	- Authorization định dạng: "Bearer + {access_token}": theo tiêu chuẩn RFC 6750. - Đối với Redirect Flow: Mã access_token được cấp theo quy định tại mục 4.1 trong RFC 6749 (Authorization Code Grant). - Đối với Decoupled flow: Mã access_token được cấp theo quy định tại mục 4.4 trong RFC 6749 (với grant_type là client_credentials).
Request-DateTime	DateTime	M	- Ngày giờ thực hiện. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
Request-ID	String [60]	M	Mã định danh duy nhất cho request, thường ở định dạng UUID
PSU-IP-Address	String [50]	O	Địa chỉ IP của khách hàng. Giá trị này phải ở dạng IPv4 hoặc IPv6.
PSU-User-Agent	String [200]	O	Thông tin trình duyệt trong trường hợp khách hàng sử dụng ứng dụng web của TPP hoặc các thông tin khác trong trường hợp khách hàng sử dụng ứng dụng khác của TPP.
PSU-Device-OS	String [100]	O	Hệ điều hành trên thiết bị (máy tính/di động,...) của khách hàng.

			Mô tả
Provider-ID	String [8]	M	Mã định danh của Ngân hàng được quy định tại Mục 1.
TPP-ID	String [15]	M	Mã định danh của TPP được quy định tại Mục 1.
Client-ID	String [50]	O	Giá trị client_id được nêu tại Mục 1.
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Request Body:

paymentId	String [35]	M	Mã giao dịch duy nhất do Ngân hàng cung cấp cho TPP trong API khởi tạo thanh toán mục 4.1
consentId	String [36]	C	Giá trị do Ngân hàng sinh ra sau khi xác nhận thành công trên Ứng dụng của Ngân hàng trong luồng Decoupled.

- Response Header:

Content-Type	String	M	Mặc định "application/json"
Request-ID	String	M	Giá trị được lấy từ request header trong API của TPP
Request-DateTime	String	M	Giá trị được lấy từ request header trong API của TPP
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Response Body:

+ HTTP STATUS CODE **200 OK:**

paymentId	String [35]	M	Mã giao dịch duy nhất do Ngân hàng cung cấp cho TPP trong API khởi tạo thanh toán mục 4.1.
status	String [4]	M	Mã trạng thái của giao dịch. Theo tiêu chuẩn của ISO 20022.
statusDateTime	DateTime	M	- Thời điểm cập nhật trạng thái. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.

+ Error Code: Tham chiếu tại mục 7.2.1. Định dạng phản hồi lỗi và 7.2.2 Bảng mã lỗi chung.

4.6. API Lấy trạng thái giao dịch

Endpoint	/v1/payments/status
Method	POST
Scope	PIS

- Request Header:

[redacted]			
Content-Type	String	M	Mặc định "application/json".
Authorization	String	M	- Authorization định dạng: "Bearer + {access_token}": theo tiêu chuẩn RFC 6750. - Mã access_token được cấp theo quy định tại mục 4.4 trong RFC 6749(với grant_type là client_credentials)
Request-DateTime	DateTime	M	- Ngày giờ thực hiện. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
Request-ID	String [60]	M	Mã định danh duy nhất cho request, thường ở định dạng UUID.
PSU-IP-Address	String [50]	O	Địa chỉ IP của khách hàng. Giá trị này phải ở dạng IPv4 hoặc IPv6.
PSU-User-Agent	String [200]	O	Thông tin trình duyệt trong trường hợp khách hàng sử dụng ứng dụng web của TPP hoặc các thông tin khác trong trường hợp khách hàng sử dụng ứng dụng khác của TPP.
PSU-Device-OS	String [100]	O	Hệ điều hành trên thiết bị (máy tính/di động,...) của khách hàng.
Provider-ID	String [8]	M	Mã định danh của Ngân hàng được quy định tại Mục 1.
TPP-ID	String [15]	M	Mã định danh của TPP được quy định tại Mục 1.
Client-ID	String [50]	O	Giá trị client_id được nêu tại Mục 1.
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1.

- Request Body:

[redacted]			
paymentId	String [35]	M	Mã giao dịch duy nhất do Ngân hàng cung cấp cho TPP trong API khởi tạo thanh toán mục 4.1.

- Response Header:

[redacted]			
Content-Type	String	M	Mặc định "application/json"
Request-ID	String	M	Giá trị được lấy từ request header trong API của TPP
Request-DateTime	String	M	Giá trị được lấy từ request header trong API của TPP
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Response Body:

+ HTTP STATUS CODE **200 OK:**

paymentId	String [35]	M	Mã giao dịch duy nhất do Ngân hàng cung cấp cho TPP trong API khởi tạo thanh toán mục 4.1.
status	String [4]	M	Mã trạng thái của giao dịch. Theo tiêu chuẩn của ISO 20022.
statusDateTime	DateTime	M	- Thời điểm cập nhật trạng thái. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.

+ **Error Code:** Tham chiếu tại mục 7.2.1. Định dạng phản hồi lỗi và 7.2.2 Bảng mã lỗi

4.7. API Lấy trạng thái xác nhận thanh toán của khách hàng luồng Decoupled

TPP gọi API này của Ngân hàng để lấy về trạng thái xác nhận thanh toán của khách hàng cụ thể như sau:

Endpoint	/v1/get-consent
Method	POST
Scope	PIS

- Request Header:

Content-Type	String	M	Mặc định "application/json"
Authorization	String	M	- Authorization định dạng: "Bearer + {access_token}": theo tiêu chuẩn RFC 6750. - Mã access_token được cấp theo quy định tại mục 4.4 trong RFC 6749(với grant_type là client_credentials).
Request-DateTime	DateTime	M	- Ngày giờ thực hiện. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime). theo tiêu chuẩn RFC 3339.
Request-ID	String [60]	M	Mã định danh duy nhất cho request, thường ở định dạng UUID
PSU-IP-Address	String [50]	O	Địa chỉ IP của khách hàng. Giá trị này phải ở dạng IPv4 hoặc IPv6.
PSU-User-Agent	String [200]	O	Thông tin trình duyệt trong trường hợp khách hàng sử dụng ứng dụng web của TPP hoặc các thông tin khác trong

			trường hợp khách hàng sử dụng ứng dụng khác của TPP.
PSU-Device-OS	String [100]	O	Hệ điều hành trên thiết bị (máy tính/di động,...) của khách hàng.
Provider-ID	String [8]	M	Mã định danh của Ngân hàng được quy định tại Mục 1.
TPP-ID	String [15]	M	Mã định danh của TPP được quy định tại Mục 1.
Client-ID	String [50]	O	Giá trị client_id được nêu tại Mục 1.
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1.

- Request Body:

paymentId	String [35]	M	Mã giao dịch duy nhất do Ngân hàng cung cấp cho TPP trong API khởi tạo thanh toán mục 4.1.

- Response Header:

Content-Type	String	M	Mặc định "application/json"
Request-ID	String	M	Giá trị được lấy từ request header trong API của TPP
Request-DateTime	String	M	Giá trị được lấy từ request header trong API của TPP
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Response Body:

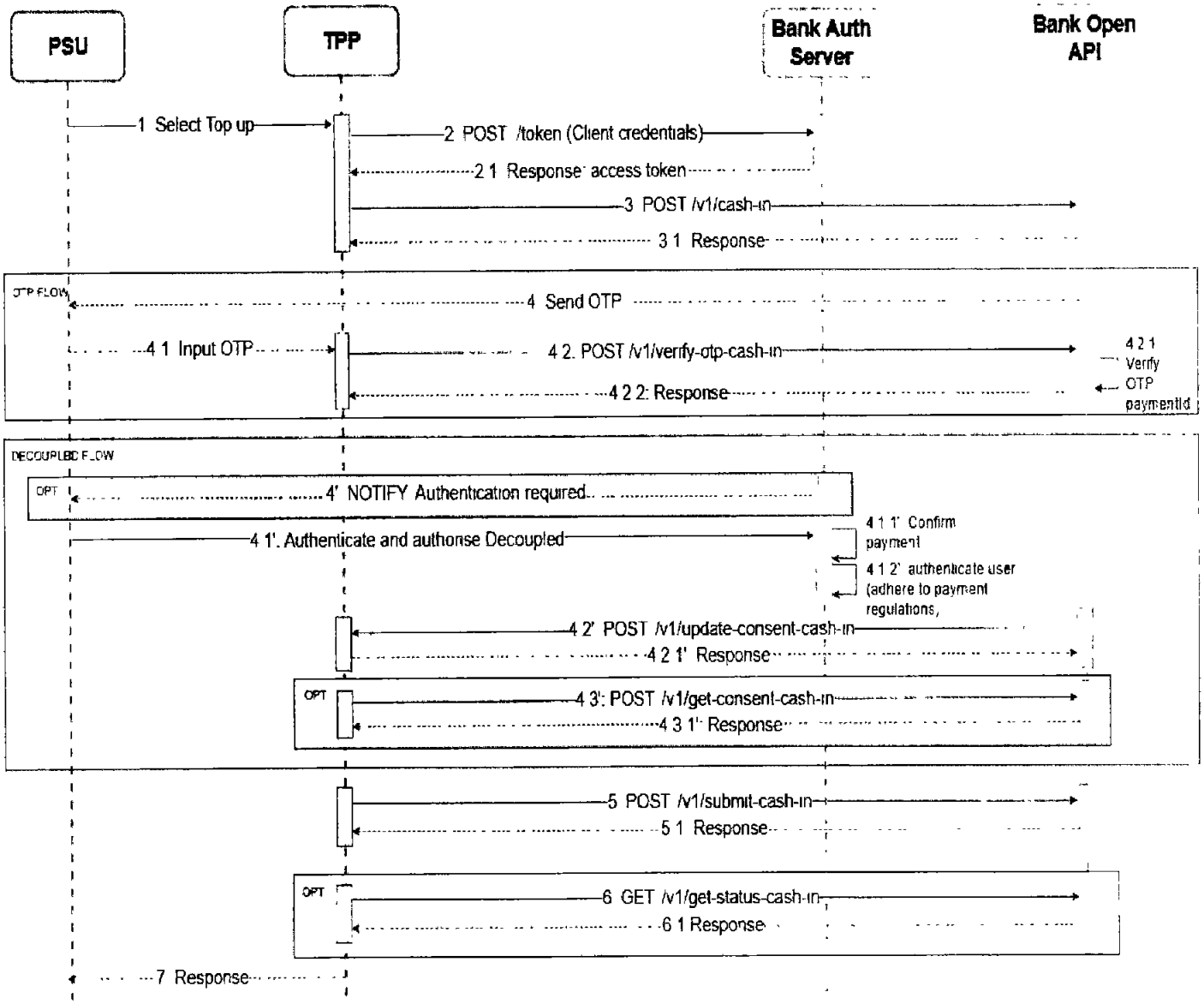
+ HTTP STATUS CODE **200 OK:**

paymentId	String [35]	M	Mã giao dịch duy nhất do Ngân hàng cung cấp cho TPP trong API khởi tạo thanh toán mục 4.1.
consentId	String [36]	M	Giá trị do Ngân hàng sinh ra sau khi xác nhận thành công trên Ứng dụng của Ngân hàng trong luồng Decoupled.
consentStatus	String [20]	M	Nhận một trong các giá trị sau: - "AUTHORISED" khi khách hàng xác nhận thành công. - "REJECTED" khi khách hàng xác nhận sai quy định của Ngân hàng. - "CANCEL" khi khách hàng không xác nhận trên Ứng dụng của Ngân hàng.
expireIn	Number	M	Thời gian hiệu lực của consentId quy định tại Mục 1.

+ **Error Code:** Tham chiếu tại mục 7.2.1. Định dạng phản hồi lỗi và 7.2.2 Bảng mã lỗi

5. Các Open API Nạp tiền vào ví điện tử (điểm c khoản 1 Điều 6)

- Luồng triển khai các API Nạp tiền vào ví điện tử (sau đây gọi là nạp ví điện tử) sau khi khách hàng thực hiện liên kết ví điện tử theo quy định. Khách hàng thực hiện nạp ví điện tử từ tài khoản liên kết trên ứng dụng của TPP.



Hình 5. Luồng nạp ví điện tử (EWLTS)

- Mô tả chi tiết luồng:

+ Bước 1: Sau khi đăng nhập vào ứng dụng của TPP, khách hàng thực hiện yêu cầu nạp ví điện tử.

+ Bước 2: TPP thực hiện một yêu cầu lấy **access_token** theo tiêu chuẩn **OAuth2.0** với **grant_type** là **client_credentials** (Chi tiết được mô tả tại mục 4.4 trong RFC 6749) tới hệ thống xác nhận của Ngân hàng.

+ Bước 2.1. Hệ thống xác nhận của Ngân hàng kiểm tra thông tin trong yêu cầu và phản hồi **access_token** cho TPP.

+ Bước 3: TPP thực hiện gửi yêu cầu khởi tạo nạp ví điện tử tới hệ thống của Ngân hàng thông qua API ***"Nạp ví điện tử"*** tại **mục 5.1**

+ Bước 3.1. Hệ thống của Ngân hàng thực hiện kiểm tra các thông tin từ yêu cầu của TPP. Khi các thông tin hợp lệ, hệ thống của Ngân hàng trả về cho TPP một mã giao dịch duy nhất (**paymentId**).

Việc xác nhận giao dịch nạp ví điện tử theo quy định của Thống đốc Ngân hàng Nhà nước Việt Nam quy định về an toàn, bảo mật cho việc cung cấp dịch vụ trực tuyến trong ngành Ngân hàng. Trong trường hợp thực hiện xác nhận nạp ví điện tử theo OTP hoặc Decoupled thì thực hiện như sau[1]:

Với luồng OTP (các bước từ 4 đến 4.2.2):

+ Bước 4: Hệ thống của Ngân hàng gửi OTP cho khách hàng.

+ Bước 4.1: Khách hàng nhập OTP trên ứng dụng của TPP.

+ Bước 4.2: TPP thực hiện gửi yêu cầu xác nhận OTP tới hệ thống của Ngân hàng thông qua API ***"Xác nhận OTP"*** tại **mục 5.2.**

+ Bước 4.2.1: Hệ thống của Ngân hàng thực hiện kiểm tra các thông tin từ yêu cầu của TPP.

+ Bước 4.2.2: Hệ thống của Ngân hàng thực hiện phản hồi kết quả cho TPP.

Với luồng decoupled (các bước từ 4' đến 4.3.1'):

+ Bước 4': Tùy theo thiết kế ứng dụng của TPP và Hệ thống của Ngân hàng mà Hệ thống xác nhận của Ngân hàng thực hiện hoặc không thực hiện gửi thông báo tới khách hàng có giao dịch nạp ví điện tử cần được xác nhận.

+ Bước 4.1': Khách hàng truy cập vào ứng dụng Ngân hàng.

+ Bước 4.1.1': Khách hàng xác nhận thông tin nạp ví điện tử.

+ Bước 4.1.2': Khách hàng xác nhận nạp ví điện tử theo các phương thức xác nhận do Ngân hàng cung cấp và bảo đảm tuân thủ quy định về an toàn, bảo mật cho việc cung cấp dịch vụ trực tuyến trong ngành Ngân hàng.

+ Bước 4.2': Hệ thống của Ngân hàng gửi yêu cầu cập nhật trạng thái xác nhận nạp ví điện tử của khách hàng tới TPP thông qua API ***"Cập nhật trạng thái xác nhận nạp ví điện tử của khách hàng luồng decoupled"*** tại **mục 5.3**.

+ Bước 4.2.1': TPP nhận được trạng thái và phản hồi kết quả cho Hệ thống của Ngân hàng, chi tiết **tại mục 5.3.**

+ Bước 4.3': Trong trường hợp TPP không nhận được trạng thái xác nhận nạp ví điện tử của khách hàng thông qua API ***"Cập nhật trạng thái xác nhận nạp ví điện tử của khách hàng luồng Decoupled"*** tại **mục 5.3** từ hệ thống của Ngân hàng thì TPP có

[1] Trường hợp sử dụng Soft OTP thì có thể thực hiện theo luồng OTP hoặc luồng Decoupled.

thể gửi yêu cầu lấy trạng thái xác nhận nạp ví điện tử của khách hàng tới hệ thống của Ngân hàng thông qua API ***"Lấy trạng thái xác nhận nạp ví điện tử của khách hàng luồng Decoupled"*** tại **mục 5.4**.

+ Bước 4.3.1`: Hệ thống cua Ngân hàng nhận được yêu cầu và phản hồi kết qua lại cho TPP.

+ Bước 5: TPP thực hiện gửi yêu cầu xác nhận nạp ví điện tử tới Ngân hàng thông qua API ***"Xác nhận nạp ví điện tử"*** tại **mục 5.5**.

+ Bước 5.1. Ngân hàng phản hồi kết quả cho TPP về trạng thái giao dịch.

+ Bước 6: Trong trường hợp TPP không nhận được phản hồi kết qua hạch toán từ Ngân hàng, TPP gửi yêu cầu lấy trạng thái giao dịch tới hệ thống của Ngân hàng thông qua API "***Lấy trạng thái giao dịch***" tại **mục 5.6**.

+ Bước 6.1: Hệ thống của Ngân hàng nhận được yêu cầu và phản hồi kết quả lại cho TPP.

+ Bước 7. TPP hiển thị kết quả thực hiện nạp ví điện tử cho khách hàng.

5.1. API Nạp ví điện tử

Endpoint	/v1/cash-in
Method	POST
Scope	EWLTS

- Request Header:

Content-Type	String	M	Mặc định "application/json"
Authorization	String	M	- Authorization định dạng: "Bearer + {access_token}". theo tiêu chuẩn RFC 6750. - Mã access_token được cấp theo quy định tại mục 4.4 trong RFC 6749 (với grant_type là client_credentials).
Request-DateTime	DateTime	M	-Ngày giờ thực hiện. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
Request-ID	String [60]	M	Mã định danh duy nhất cho request, thường ở định dạng UUID.
PSU-IP-Address	String [50]	O	Địa chỉ IP của khách hàng. Giá trị này phải ở dạng IPv4 hoặc IPv6
PSU-User-Agent	String [200]	O	Thông tin trình duyệt trong trường hợp khách hàng sử dụng ứng dụng web của TPP hoặc các thông tin khác trong trường hợp khách hàng sử dụng ứng dụng khác của TPP.
PSU-Device-OS	String [100]	O	Hệ điều hành trên thiết bị (máy tính/di động,...) của khách hàng.

		Bắt buộc	Mô tả
Provider-ID	String [8]	M	Mã định danh của Ngân hàng được quy định tại Mục 1.
TPP-ID	String [15]	M	Mã định danh của TPP được quy định tại Mục 1.
Client-ID	String [50]	O	Giá trị client_id được nêu tại Mục 1.
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1.

- Request Body:

instructionIdentification		String [50]	M	Mã giao dịch do TPP khởi tạo
remittanceInformation		String [255]	M	Nội dung giao dịch
instructedAmount		Object	M	Thông tin số tiền giao dịch
	value	Number	M	Số tiền giao dịch
	currency	String [3]	M	Loại tiền tệ quy định theo mã của bộ ISO 4217 với 3 ký tự viết hoa.
requestedExecutionDate		DateTime	M	- Ngày thực hiện giao dịch. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
ewalletToken		String [30]	M	Mã được sinh ra khi thực hiện liên kết ví điện tử giữa TPP và ngân hàng.
additionalInfo		Object	O	Thông tin bổ sung (nếu có).

- Response Header:

Content-Type	M	String	Mặc định "application/json"
Request-ID	M	String	Giá trị được lấy từ request header trong API của TPP
Request-DateTime	M	String	Giá trị được lấy từ request header trong API của TPP
JWS-Signature	M	String	Chữ ký JWS theo quy định tại Mục 1

- Response Body:

+ HTTP STATUS CODE **200 OK:**

[illegible]	[illegible]	[illegible]	Mô tả
paymentId	String [35]	M	Mã giao dịch duy nhất do Ngân hàng cung cấp.
status	String [4]	M	Mã trạng thái của giao dịch. Theo tiêu chuẩn của ISO 20022.
statusDateTime	DateTime	M	- Thời điểm cập nhật trạng thái. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime) , theo tiêu chuẩn RFC 3339.
authenType	String [10]	M	Nhận một trong các giá trị sau: - "OTP": thực hiện theo luồng OTP - "DECOUPLED": thực hiện theo luồng Decoupled. - "NONE": trong trường hợp không thực hiện theo luồng OTP và luồng Decoupled.
additionalInfo	Object	O	Thông tin bổ sung (nếu có)

+ Error Code: Tham chiếu tại mục 7.2.1. Định dạng phản hồi lỗi và 7.2.2 Bảng mã lỗi

5.2. API Xác nhận OTP

Endpoint	/v1/verify-otp-cash-in
Method	POST
Scope	EWLTS

- Request Header:

[illegible]	[illegible]	[illegible]	[illegible]
Content-Type	String	M	Mặc định "application/json"
Authorization	String	M	- Authorization định dạng: "Bearer + {access_token}": theo tiêu chuẩn RFC 6750. - Mã access_token được cấp theo quy định tại mục 4.4 trong RFC 6749 (với grant_type là client_credentials).
Request-DateTime	DateTime	M	- Ngày giờ thực hiện. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
Request-ID	String [60]	M	Mã định danh duy nhất cho request, thường ở định dạng UUID
PSU-IP-Address	String [50]	O	Địa chỉ IP của khách hàng. Giá trị này phải ở dạng IPv4 hoặc IPv6.
PSU-User-Agent	String [200]	O	Thông tin trình duyệt trong trường hợp khách hàng sử dụng ứng dụng web của TPP hoặc các thông tin khác

[illegible]	Loại dữ [illegible]	Bắt buộc	Mô tả
			trong trường hợp khách hàng sử dụng ứng dụng khác của TPP.
PSU-Device-OS	String [100]	O	Hệ điều hành trên thiết bị (máy tính/di động,…) của khách hàng.
Provider-ID	String [8]	M	Mã định danh của Ngân hàng được quy định tại Mục 1.
TPP-ID	String [15]	M	Mã định danh của TPP được quy định tại Mục 1.
Client-ID	String [50]	O	Giá trị client_id được nêu tại Mục 1.
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1.

- Request Body:

[illegible]			
paymentId	String [35]	M	Mã giao dịch duy nhất do Ngân hàng cung cấp trả về trong API Nạp ví điện tử mục 5.1.
otp	String [6]	M	Mã OTP Ngân hàng trả về cho khách hàng.
ewalletToken	String [30]	M	Mã được sinh ra khi thực hiện liên kết ví điện tử giữa TPP và ngân hàng.
additionalInfo	Object	O	Thông tin bổ sung (nếu có).

- Response Header:

[illegible]			
Content-Type	String	M	Mặc định "application/json"
Request-ID	String	M	Giá trị được lấy từ request header trong API của TPP
Request-DateTime	String	M	Giá trị được lấy từ request header trong API của TPP
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Response Body:

+ HTTP STATUS CODE **200 OK:**

[illegible]			
paymentId	String [35]	M	Mã giao dịch duy nhất do Ngân hàng cung cấp cho TPP trong API Nạp ví điện tử mục 5.1.
consentId	String [36]	M	Giá trị do Ngân hàng sinh ra sau khi verify OTP thành công trong luồng OTP.

expireIn	Number	M	Thời gian hiệu lực của consentId quy định tại Mục 1.

+ Error Code: Tham chiếu tại mục 7.2.1. Định dạng phản hồi lỗi và 7.2.2 Bảng mã lỗi

5.3. API Cập nhật trạng thái xác nhận nạp ví điện tử của khách hàng luồng Decoupled

Ngân hàng thực hiện gọi API này của TPP để trả về trạng thái xác nhận nạp ví điện tử của khách hàng cụ thể như sau:

Endpoint	/v1/update-consent-cash-in
Method	POST

- Request Header:

Content-Type	String	M	Mặc định "application/json"
Authorization	String	M	- Authorization định dạng: "Bearer + {access_token}": theo tiêu chuẩn RFC 6750. - Mã access_token được cấp theo quy định tại mục 4.4 trong RFC 6749(với grant_type là client_credentials).
Request-DateTime	DateTime	M	- Ngày giờ thực hiện. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
Request-ID	String [60]	M	Mã định danh duy nhất cho request. thường ở định dạng UUID.
Provider-ID	String [8]	M	Mã định danh của Ngân hàng được quy định tại Mục 1.
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1.

- Request Body:

paymentId	String [35]	M	Mã giao dịch duy nhất do Ngân hàng cung cấp cho TPP trong API Nạp ví điện tử mục 5.1.
consentId	String [36]	M	Giá trị do Ngân hàng sinh ra sau khi xác nhận thành công trên Ứng dụng của Ngân hàng trong luồng Decoupled.
consentStatus	String [20]	M	Nhận một trong các giá trị sau: - "AUTHORISED" khi khách hàng xác thực thành công.

			- "REJECTED" khi khách hàng xác nhận sai quy định của Ngân hàng. - "CANCEL" khi khách hàng không xác nhận trên Ứng dụng của Ngân hàng.
ewalletToken	String [30]	M	Mã được sinh ra khi thực hiện liên kết ví điện tử giữa TPP và ngân hàng
expireIn	Number	M	Thời gian hiệu lực của consentId quy định tại Mục 1.

- Response Header:

Content-Type	String	M	Mặc định "application/json"
Request-ID	String	M	Giá trị được lấy từ request header trong API của TPP
Request-DateTime	String	M	Giá trị được lấy từ request header trong API của TPP
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Response Body:

+ HTTP STATUS CODE **200 OK:**

message	String [20]	M	Mặc định "Success"

+ Error Code: Theo quy định của TPP.

5.4. API Lấy trạng thái xác nhận nạp ví điện tử của khách hàng luồng Decoupled

TPP gọi API này của Ngân hàng để lấy về trạng thái xác nhận nạp ví điện tử của khách hàng cụ thể như sau:

Endpoint	/v1/get-consent-cash-in
Method	POST
Scope	EWLTS

- Request Header:

Content-Type	String	M	Mặc định "application/json"
Authorization	String	M	- Authorization định dạng: "Bearer + {access_token}": theo tiêu chuẩn RFC 6750. - Mã access_token được cấp theo quy định tại mục 4.4 trong RFC 6749(với grant_type là client_credentials).
Request-DateTime	DateTime	M	- Ngày giờ thực hiện.

[redacted]	[redacted]	[redacted]	Mô tả
			- Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
Request-ID	String [60]	M	Mã định danh duy nhất cho request, thường ở định dạng UUID
PSU-IP-Address	String [50]	O	Địa chỉ IP của khách hàng. Giá trị này phải ở dạng IPv4 hoặc IPv6.
PSU-User-Agent	String [200]	O	Thông tin trình duyệt trong trường hợp khách hàng sử dụng ứng dụng web của TPP hoặc các thông tin khác trong trường hợp khách hàng sử dụng ứng dụng khác của TPP.
PSU-Device-OS	String [100]	O	Hệ điều hành trên thiết bị (máy tính/di động,...) của khách hàng.
Provider-ID	String [8]	M	Mã định danh của Ngân hàng được quy định tại Mục 1.
TPP-ID	String [15]	M	Mã định danh của TPP được quy định tại Mục 1.
Client-ID	String [50]	O	Giá trị client_id được nêu tại Mục 1.
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Request Body:

[redacted]			
paymentId	String [35]	M	Mã giao dịch duy nhất do Ngân hàng cung cấp cho TPP trong API Nạp ví điện tử mục 5.1.
ewalletToken	String [30]	M	Mã được sinh ra khi thực hiện liên kết ví điện tử giữa TPP và ngân hàng.

- Response Header:

[redacted]			
Content-Type	String	M	Mặc định "application/json"
Request-ID	String	M	Giá trị được lấy từ request header trong API của TPP
Request-DateTime	String	M	Giá trị được lấy từ request header trong API của TPP
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Response Body:

+ HTTP STATUS CODE **200 OK:**

[redacted]

paymentId	String [35]	M	Mã giao dịch duy nhất do Ngân hàng cung cấp cho TPP trong API Nạp ví điện tử mục 5.1
consentId	String [36]	M	- Giá trị do Ngân hàng sinh ra sau khi xác nhận thành công trên Ứng dụng của Ngân hàng .
consentStatus	String [20]	M	Nhận một trong các giá trị sau: - "AUTHORISED" khi khách hàng xác nhận thành công. - "REJECTED" khi khách hàng xác nhận sai quy định của Ngân hàng. - "CANCEL" khi khách hàng không xác nhận trên Ứng dụng của Ngân hàng.
expireIn	Number	M	Thời gian hiệu lực của consentId quy định tại Mục 1.
ewalletToken	String [30]	M	Mã được sinh ra khi thực hiện liên kết ví điện tử giữa TPP và ngân hàng.

+ Error Code: Tham chiếu tại mục 7.2.1. Định dạng phản hồi lỗi và 7.2.2 Bảng mã lỗi

5.5. API Xác nhận nạp ví điện tử

Endpoint	/v1/submit-cash-in
Method	POST
Scope	EWLTS

- Request Header:

Content-Type	String	M	Mặc định "application/json"
Authorization	String	M	- Authorization định dạng: "Bearer + {access_token}": theo tiêu chuẩn RFC 6750. - Mã access_token được cấp theo quy định tại mục 4.4 trong RFC 6749 (với grant_type là client_credentials).
Request-DateTime	DateTime	M	- Ngày giờ thực hiện. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime). theo tiêu chuẩn RFC 3339.
Request-ID	String [60]	M	Mã định danh duy nhất cho request, thường ở định dạng UUID.
PSU-IP-Address	String [50]	O	Địa chỉ IP của khách hàng. Giá trị này phải ở dạng IPv4 hoặc IPv6.
PSU-User-Agent	String [200]	O	Thông tin trình duyệt trong trường hợp khách hàng sử dụng ứng dụng web của TPP hoặc các thông tin khác trong trường hợp khách hàng sử dụng ứng dụng khác của TPP.

Tham số	Loại dữ liệu	Bắt buộc	Mô tả
PSU-Device-OS	String [100]	O	Hệ điều hành trên thiết bị (máy tính/di động....) của khách hàng.
Provider-ID	String [8]	M	Mã định danh của Ngân hàng được quy định tại Mục 1.
TPP-ID	String [15]	M	Mã định danh của TPP được quy định tại Mục 1.
Client-ID	String [50]	O	Giá trị client_id được nêu tại Mục 1.
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1.

- Request Body:

paymentId	String [35]	M	Mã giao dịch duy nhất do Ngân hàng cung cấp cho TPP trong API Nạp ví điện tử mục 5.1.
consentId	String [36]	C	Giá trị do Ngân hàng sinh ra sau khi xác nhận thành công trên Ứng dụng của Ngân hàng trong luồng Decoupled hoặc xác nhận OTP thành công trong luồng OTP.
ewalletToken	String [30]	M	Mã được sinh ra khi thực hiện liên kết ví điện tử giữa TPP và ngân hàng.

- Response Header:

Content-Type	String	M	Mặc định "application/json"
Request-ID	String	M	Giá trị được lấy từ request header trong API của TPP
Request-DateTime	String	M	Giá trị được lấy từ request header trong API của TPP
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Response Body:

+ HTTP STATUS CODE **200 OK:**

paymentId	String [35]	M	Mã giao dịch duy nhất do Ngân hàng cung cấp cho TPP trong API Nạp ví điện tử mục 5.1.
status	String [4]	M	Mã trạng thái của giao dịch. Theo tiêu chuẩn của ISO 20022.
statusDateTime	DateTime	M	- Thời điểm cập nhật trạng thái. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.

+ **Error Code:** Tham chiếu tại mục 7.2.1. Định dạng phản hồi lỗi và 7.2.2 Bảng mã lỗi chung.

5.6. API Lấy trạng thái giao dịch

Endpoint	/v1/get-status-cash-in
Method	POST
Scope	EWLTS

- Request Header:

Content-Type	String	M	Mặc định "application/json"
Authorization	String	M	- Authorization định dạng: "Bearer + {access_token}": theo tiêu chuẩn RFC 6750. - Mã access_token được cấp theo quy định tại mục 4.4 trong RFC 6749(với grant_type là client_credentials)
Request-DateTime	DateTime	M	- Ngày giờ thực hiện. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339
Request-ID	String [60]	M	Mã định danh duy nhất cho request. thường ở định dạng UUID.
PSU-IP-Address	String [50]	O	Địa chỉ IP của khách hàng Giá trị này phải ở dạng IPv4 hoặc IPv6.
PSU-User-Agent	String [200]	O	Thông tin trình duyệt trong trường hợp khách hàng sử dụng ứng dụng web của TPP hoặc các thông tin khác trong trường hợp khách hàng sử dụng ứng dụng khác của TPP.
PSU-Device-OS	String [100]	O	Hệ điều hành trên thiết bị (máy tính/di động,...) của khách hàng.
Provider-ID	String [8]	M	Mã định danh của Ngân hàng được quy định tại Mục 1.
TPP-ID	String [15]	M	Mã định danh của TPP được quy định tại Mục 1.
Client-ID	String [50]	O	Giá trị client_id được nêu tại Mục 1.
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1.

- Request Body:

paymentId	String [35]	M	Mã giao dịch duy nhất do Ngân hàng cung cấp cho TPP trong API Nạp ví điện tử mục 5.1.
ewalletToken	String [30]	M	Mã được sinh ra khi thực hiện liên kết ví điện tử giữa TPP và ngân hàng.

- Response Header:

[redacted]	[redacted]	[redacted]	Mô tả
Content-Type	String	M	Mặc định "application/json"
Request-ID	String	M	Giá trị được lấy từ request header trong API của TPP
Request-DateTime	String	M	Giá trị được lấy từ request header trong API của TPP
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Response Body:

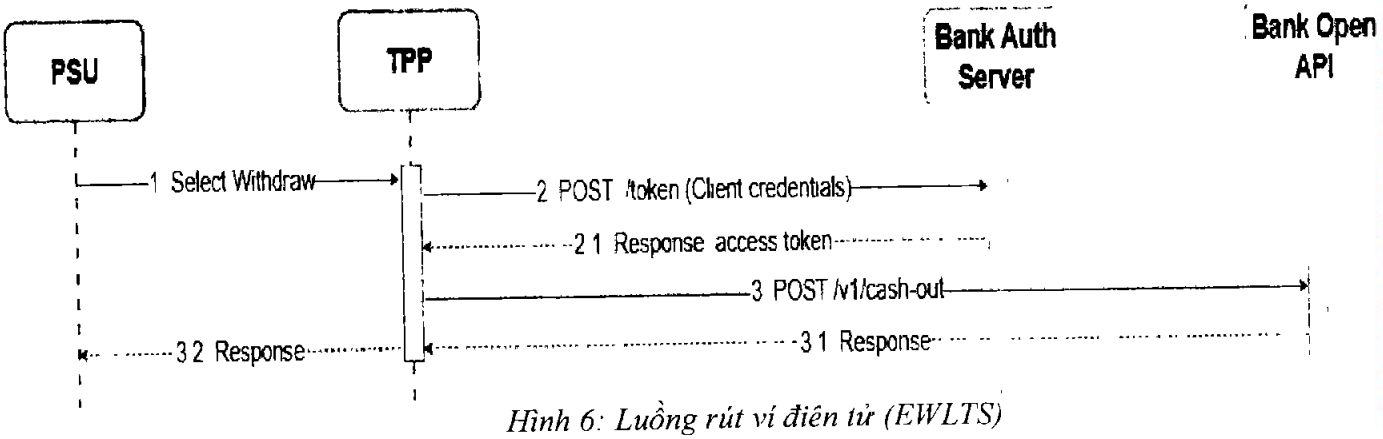
+ HTTP STATUS CODE **200 OK:**

[redacted]			
paymentId	String [35]	M	Mã giao dịch duy nhất do Ngân hàng cung cấp cho TPP trong API Nạp ví điện tư mục 5.1
status	String [4]	M	Mã trạng thái của giao dịch. Theo tiêu chuẩn của ISO 20022.
statusDateTime	DateTime	M	- Thời điểm cập nhật trạng thái. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.

+ **Error Code:** Tham chiếu tại mục 7.2.1. Định dạng phản hồi lỗi và 7.2.2 Bảng mã lỗi

6. Open API Rút tiền ra khỏi ví điện tử (điểm c khoản 1 Điều 6)

- Luồng triển khai API Rút tiền ra khỏi ví điện tử (sau đây gọi là rút ví điện tử):



Hình 6: Luồng rút ví điện tử (EWLTS)

- Mô tả chi tiết luồng:

+ Bước 1: Sau khi đăng nhập vào ứng dụng của TPP, khách hàng thực hiện yêu cầu rút ví điện tử.

+ Bước 2: TPP thực hiện một yêu cầu lấy **access_token** theo tiêu chuẩn **OAuth2.0** với **grant_type** là **client_credentials** (Chi tiết được mô tả tại mục 4.4 trong RFC 6749) tới hệ thống xác nhận của Ngân hàng.

+ Bước 2.1. Hệ thống xác nhận của Ngân hàng kiểm tra thông tin trong yêu cầu và phản hồi cho TPP **access_token**.

+ Bước 3: TPP thực hiện gửi yêu cầu rút ví điện tử tới Ngân hàng theo API mô tả dưới đây.

+ Bước 3.1. Hệ thống của Ngân hàng phản hồi kết quả cho TPP.

+ Bước 3.2. Ứng dụng của TPP hiển thị kết quả cho khách hàng.

Endpoint	/v1/cash-out
Method	POST
Scope	EWLTS

- Request Header:

Content-Type	String	M	Mặc định "application/json"
Authorization	String	M	- Authorization định dạng: "Bearer + {access_token}": theo tiêu chuẩn RFC 6750. - Mã access_token được cấp theo quy định tại mục 4.4 trong RFC 6749(với grant_type là client_credentials).
Request-DateTime	DateTime	M	- Ngày giờ thực hiện. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
Request-ID	String [60]	M	Mã định danh duy nhất cho request, thường ở định dạng UUID.
PSU-IP-Address	String [50]	O	Địa chỉ IP của khách hàng. Giá trị này phải ở dạng IPv4 hoặc IPv6.
PSU-User-Agent	String [200]	O	Thông tin trình duyệt trong trường hợp khách hàng sử dụng ứng dụng web của TPP hoặc các thông tin khác trong trường hợp khách hàng sử dụng ứng dụng khác của TPP.
PSU-Device-OS	String [100]	O	Hệ điều hành trên thiết bị (máy tính/di động,...) của khách hàng.
Provider-ID	String [8]	M	Mã định danh của Ngân hàng được quy định tại Mục 1.
TPP-ID	String [15]	M	Mã định danh của TPP được quy định tại Mục 1
Client-ID	String [50]	O	Giá trị client_id được nêu tại Mục 1.

JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1.

- Request Body:

instructionIdentification		String [50]	M	Mã giao dịch do TPP khởi tạo
remittanceInformation		String [255]	M	Nội dung giao dịch
instructedAmount		Object	M	Thông tin số tiền giao dịch
	value	Number	M	Số tiền giao dịch
	currency	String [3]	M	Loại tiền tệ quy định theo mã của bộ ISO 4217 với 3 ký tự viết hoa.
requestedExecutionDate		DateTime	M	- Ngày thực hiện giao dịch. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.
ewalletToken		String [30]	M	Mã được sinh ra khi thực hiện liên kết ví điện tử giữa TPP và ngân hàng
additionalInfo		Object	O	Thông tin bổ sung (nếu có)

- Response Header:

Content-Type	String	M	Mặc định "application/json"
Request-ID	String	M	Giá trị được lấy từ request header trong API của TPP
Request-DateTime	String	M	Giá trị được lấy từ request header trong API của TPP
JWS-Signature	String	M	Chữ ký JWS theo quy định tại Mục 1

- Response Body:

+ HTTP STATUS CODE **200 OK:**

status	String [4]	M	Mã trạng thái của giao dịch. Theo tiêu chuẩn của ISO 20022.
statusDateTime	DateTime	M	- Thời điểm cập nhật trạng thái. - Định dạng: yyyy-MM-ddTHH:mm:ssZ (UTC DateTime), theo tiêu chuẩn RFC 3339.

+ **Error Code:** Tham chiếu tại mục 7.2.1. Định dang phản hồi lỗi và 7.2.2 Bảng mã lỗi chung.

7. Mã lỗi

7.1. Mã lỗi luồng lấy mã truy cập của khách hàng.

7.1.1. Mã lỗi API xác nhận và lấy sự đồng ý của khách hàng

Trường hợp tham số "redirect_uri" thiếu hoặc không khớp đường dẫn mà TPP đã đăng ký với Ngân hàng. Ngân hàng cần điều hướng khách hàng tới trang thông báo lỗi và mô tả rõ lỗi cho khách hàng.

Trường hợp lỗi như khách hàng từ chối đồng ý hoặc lỗi ở đây không liên quan đến đường dẫn điều hướng "redirect_uri" thì Ngân hàng sẽ thông báo cho TPP bằng cách thêm các giá trị, tham số ở bảng bên dưới vào đường dẫn "redirect_uri":

error	String	M	Mã lỗi do hệ thống trả về. Danh sách mã lỗi được áp dụng dựa trên tiêu chuẩn OAuth 2.0. Được liệt kê ở bảng mã lỗi
error_description	String	M	Cung cấp thông tin bổ sung, được sử dụng để hỗ trợ TPP hiểu lỗi đã xảy ra.
state	String	M	Giá trị từ request của TPP.

Bảng mã lỗi:

1	INVALID_REQUEST	Request bị thiếu tham số bắt buộc hoặc tham số không hợp lệ, không đúng định dạng.
2	UNAUTHORIZED_CLIENT	TPP không được phép yêu cầu lấy mã đồng ý bằng phương pháp này
3	ACCESS_DENIED	Chủ sở hữu tài nguyên hoặc máy chủ lấy sự đồng ý đã từ chối yêu cầu.
4	UNSUPPORTED_RESPONSE_TYPE	Máy chủ lấy sự đồng ý không hỗ trợ lấy mã đồng ý bằng phương pháp này.
5	INVALID_SCOPE	Phạm vi scope được yêu cầu không hợp lệ, không xác định hoặc không đúng định dạng.
6	SERVER_ERROR	Máy chủ lấy sự đồng ý đã gặp phải một tình trạng không mong muốn khiến nó không thể thực hiện được yêu cầu.
7	TEMPORARILY_UNAVAILABLE	Máy chủ lấy sự đồng ý hiện không thể xử lý yêu cầu do máy chủ tạm thời bị quá tải hoặc bảo trì.

7.1.2. Mã lỗi API Lấy mã truy cập

Máy chủ xác nhận và lấy sự đồng ý trả về mã lỗi HTTP 400 (Bad Request) cho TPP kèm theo chi tiết các lỗi dưới đây và các lỗi này được tham khảo dựa trên mục "5.2 *Error Response*" của tiêu chuẩn RFC 6749:

Định dạng mã lỗi:

error	M	Mã lỗi do hệ thống trả về. Danh sách mã lỗi được áp dụng dựa trên tiêu chuẩn OAuth 2.0 được liệt kê ở bảng mã lỗi.
error_description	O	Cung cấp thông tin bổ sung, được sử dụng để hỗ trợ TPP hiểu lỗi đã xảy ra.
error_uri	O	URI xác định trang web mà con người có thể đọc được cùng với thông tin về lỗi, được sử dụng để cung cấp cho thông tin bổ sung về lỗi.

Bảng mã lỗi:

400	INVALID_REQUEST	Request bị thiếu tham số bắt buộc hoặc tham số không hợp lệ, không đúng định dạng.
400	INVALID_CLIENT	Xác nhận thông tin ứng dụng khách không thành công.
400	UNAUTHORIZED_CLIENT	TPP không được phép sử dụng mã loại truy cập này.
400	INVALID_SCOPE	Phạm vi scope được yêu cầu không hợp lệ, không xác định hoặc không đúng định dạng.
400	UNSUPPORTED_GRANT_TYPE	Loại cấp quyền không được máy chủ hỗ trợ.

7.2. Mã lỗi API khác trong phụ lục này

7.2.1. Định dạng phản hồi lỗi

Trong trường hợp có lỗi xảy ra thì hệ thống của Ngân hàng cần trả về nội dung trong body phản hồi theo bảng dưới đây:

code	String	M	Mã lỗi trả về và HTTP code tham chiếu tại mục 7.2.2 Bảng mã lỗi chung
description	String	M	Thông tin bổ sung thêm chi tiết về lỗi

7.2.2. Bảng mã lỗi chung

400	ACCOUNT_ID_REQUIRED	Dữ liệu trường accountId không được rỗng
400	ACCOUNT_NOT_EXISTED	Tài khoản không tồn tại
400	CONSENTID_NOT_EXISTED	consentId không tồn tại

400	CREDITOR_ACCOUNTID_REQUIRED	Dữ liệu trường creditor accountId không được rỗng
400	CREDITOR_ACCOUNTID_NOT_EXISTED	creditor accountId không tồn tại
400	CREDITOR_BANKCODE_REQUIRED	Dữ liệu trường creditor bankCode không được rỗng
400	CREDITOR_NAME_REQUIRED	Dữ liệu trường creditor name không được rỗng
400	DEBTOR_ACCOUNTID_NOT_EXISTED	debtor accountId không tồn tại
400	DEBTOR_ACCOUNTID_REQUIRED	Dữ liệu trường debtor accountId không được rỗng
400	DEBTOR_NAME_REQUIRED	Dữ liệu trường debtor name không được rỗng
400	EWALLETTOKEN_REQUIRED	Dữ liệu trường ewalletToken không được rỗng
400	EWALLETTOKEN_NOT_EXISTED	ewalletToken không tồn tại
400	EXPIRE_CONSENTID	consentId đã hết hạn
400	FROMDATE_INVALID	Dữ liệu trường fromDate không hợp lệ
400	FROMDATE_REQUIRED	Dữ liệu trường fromDate không được rỗng
400	INSTRUCTED_AMOUNT_CURRENCY_INVALID	Dữ liệu trường instructedAmount currency không hợp lệ
400	INSTRUCTED_AMOUNT_CURRENCY_REQUIRED	Dữ liệu trường instructedAmount currency không được rỗng
400	INSTRUCTED_AMOUNT_VALUE_REQUIRED	Dữ liệu trường instructedAmount value không được rỗng
400	INSTRUCTION_IDENTIFICATION_REQUIRED	Dữ liệu trường instructionIdentification không được rỗng
400	JWS_SIGNATURE_REQUIRED	Dữ liệu trường JWS-Signature không được rỗng
400	PAGE_INVALID	Dữ liệu trường page không hợp lệ
400	PAYMENTID_REQUIRED	Dữ liệu trường paymentId không được rỗng
400	PAYMENTID_NOT_EXISTED	paymentId không tồn tại
400	PROVIDER_ID_REQUIRED	Dữ liệu trường Provider-ID không không được rỗng
400	PSU_IP_ADDRESS_INVALID	Dữ liệu trường PSU-IP-Address không hợp lệ (Trường hợp có dữ liệu)
400	REMITTANCE_INFORMATION_REQUIRED	Dữ liệu trường remittanceInformation không được rỗng
400	REQUEST_DATETIME_REQUIRED	Dữ liệu trường Request-DateTime không được rỗng

400	REQUEST_ID_REQUIRED	Dữ liệu trường Request-ID không không được rỗng
400	REQUESTED_EXECUTION DATE_REQUIRED	Dữ liệu trường requestedExecutionDate không được rỗng
400	SIZE_INVALID	Dữ liệu trường size không hợp lê
400	TODATE_INVALID	Dữ liệu trường toDate không hợp lệ
400	TODATE_REQUIRED	Dữ liệu trường toDate không được rỗng
400	TPP_ID_REQUIRED	Dữ liệu trường TPP-ID không không được rỗng
400	TPP_UNVERIFIED	TPP chưa được xác nhận
400	OTHER	Lỗi khác liên quan tới yêu cầu API từ phía TPP do ngân hàng mô tả.
401	EXPIRED_TOKEN	OAuth 2 token đã hết hạn
401	JWS_SIGNATURE_UNVER IFIED	JWS-Signature xác nhận thất bại
403	FORBIDDEN	Mã thông báo OAuth hợp lệ đã được nhận, nhưng quyền truy cập đã bị từ chối.
405	WRONG_METHOD	Sai phương thức HTTP.
500	INTERNAL_ERROR	Máy chủ gặp phải tình trạng không mong muốn khiến nó không thể thực hiện yêu cầu.
502	BAD_GATEWAY	Máy chủ nhận được phản hồi không hợp lệ từ máy chủ đích.
504	GATEWAY_TIMEOUT	Máy chủ không nhận được phản hồi từ máy chủ đích để hoàn thành yêu cầu.
500	OTHER	Lỗi khác liên quan tới máy chủ xử lý yêu cầu API do ngân hàng mô tả.

PHỤ LỤC 02

TIÊU CHUẨN KỸ THUẬT TRIỂN KHAI OPEN API TRONG NGÀNH NGÂN HÀNG

(Ban hành kèm theo Thông tư số 64/2024/TT-NHNN ngày 31 tháng 12 năm 2024 của Thống đốc Ngân hàng Nhà nước Việt Nam)

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1	**Tiêu chuẩn kiến trúc**			
1.1	Trao đổi dữ liệu			
		REST	REpresentational State Transfer	Bắt buộc áp dụng
		SOAP	Simple Object Access Protocol	Khuyến nghị áp dụng đối với các API khác của Ngân hàng.
1.2	Định dạng trao đổi dữ liệu			
		JSON	JavaScript Object Notation	Bắt buộc áp dụng
		XML	eXtensible Markup Language	Khuyến nghị áp dụng đối với các API khác của Ngân hàng
2	**Tiêu chuẩn dữ liệu**			
	Định dạng dữ liệu	ISO 20022	International Organization for Standardization 20022	Khuyến nghị áp dụng một trong các tiêu chuẩn đối với API khác của Ngân hàng
		ISO 8583	International Organization for Standardization 8583	
		OFX	Open Financial Exchange	

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		ISO 4217	International Organization for Standardization 4217	Bắt buộc áp dụng
		RFC 3339	Date and Time on the Internet: Timestamps	Bắt buộc áp dụng
3	**Tiêu chuẩn an toàn thông tin**			
3.1	Giải pháp xác thực, lấy sự đồng ý của khách hàng	RFC 6749	The OAuth 2.0 Authorization Framework	- Bắt buộc áp dụng theo tiêu chuẩn RFC 6749, RFC 6750, RFC 7636. - Có thể kết hợp tiêu chuẩn RFC 6749, RFC 6750 với các tiêu chuẩn RFC 7636, OIDC tùy theo các trường hợp áp dụng
		RFC 6750	The OAuth 2.0 Authorization Framework: Bearer Token Usage	
		RFC 7636	Proof Key for Code Exchange by OAuth Public Clients	
		RFC 7009	OAuth 2.0 Token Revocation	
		OIDC	OpenID Connect	
		SAML v2.0	Security Assertion Markup Language version 2.0	Khuyến nghị áp dụng đối với API khác cua Ngân hàng
3.2	An toàn tầng giao vận	HTTPS	HyperText Transfer Protocol Secure	Bắt buộc áp dụng
		TLS v1.2 trở lên[1]	Transport Layer Security version 1.2+	Bắt buộc áp dụng

[1] Khuyến nghị áp dụng mTLS.

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
3.3	Giải thuật mã hóa	TCVN 7816:2007	Công nghệ thông tin - Kỹ thuật mật mã - Thuật toán mã dữ liệu AES	Khuyến nghị áp dụng
		PKCS #1	RSA Cryptography Standard	Khuyến nghị áp dụng. Sử dụng phiên bản 2.1 trở lên và lược đồ RSAES-OAEP để mã hóa. Độ dài khóa tối thiểu là 2048 bit
		ECC	Elliptic Curve Cryptography	Khuyến nghị áp dụng. Độ dài khóa tối thiểu 256 bit
		JWE	JSON Web Encryption	Khuyến nghị áp dụng theo tiêu chuẩn RFC 7516
		TCVN 11367-2:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 2: Mật mã phi đối xứng.	Khuyến nghị áp dụng
3.4	Chữ ký điện tử	JWS	JSON Web Signature	Bắt buộc áp dụng: - Theo tiêu chuẩn RFC 7515. - Độ dài khóa tối thiểu là 2048 bit đối với RSA và

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
				256 bit đối với ECDSA.
		PKCS #1	RSA Cryptography Standard	Khuyến nghị áp dụng một trong các tiêu chuẩn. - Đối với tiêu chuẩn RSA: + Sử dụng phiên bản 2.1 trở lên. + Độ dài khóa tối thiểu là 2048 bit. - Đối với tiêu chuẩn ECDSA: Độ dài khóa tối thiểu là 256 bit.
		ECDSA	Elliptic Curve Digital Signature Algorithm	
		TCVN 7635:2007	Kỹ thuật mật mã – Chữ ký số	
3.5	Giải thuật băm cho chữ ký số	FIPS PUB 180-4	Secure Hash Standard	Khuyến nghị áp dụng một trong các hàm băm sau: SHA2-56. SHA-384, SHA-512, SHA-512/256. SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256
		FIPS PUB 202	SHA-3 Standard: Permutation Based Hash and Extendable Output Functions	
3.6	An toàn Hệ thống thông tin	ISO27001:2022	International Organization for Standardization 27001:2022	Bắt buộc áp dụng một trong hai tiêu chuẩn.
		TCVN 11930:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu cơ bản về an	

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
			toàn hệ thống thông tin theo cấp độ	