

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;
- Công TTĐT của NHNN;
- Lưu: VP, PC, CNTT (03 bản).



Phạm Tiến Dũng