GoPaperless SSO SaaS

Đăng nhập OIDC/FAPI · Passkey · Xác thực Palm/Facial bằng Web SDK

Một cách gọi.
Nhiều phương thức.
Ngân hàng chủ động.

Đóng gói trải nghiệm xác thực vào kênh giao dịch hiện hữu của TCTC.



Giá trị cốt lõi Tích hợp một lần, tái sử dụng hợp đồng; cấu hình và kiểm thử theo từng môi trường.

Đọc theo quyết định cần đưa ra

Phần điều hành và phụ lục kỹ thuật trong một tài liệu thống nhất

01	**Giá trị, phạm vi và kiến trúc** TCTC nhận gì; ai quản lý gì	03–07
02	**Tích hợp nhẹ và trải nghiệm** Một lệnh JS; Palm, Facial và Passkey	08–19
03	**Sẵn sàng triển khai** Bộ công cụ, dữ liệu, trách nhiệm, SLA và kế hoạch	20–27
04	**Hợp đồng và kiểm soát kỹ thuật** API, SDK, Capture, JWT, trạng thái và trust	28–36
05	**Nghiệm thu và nguồn chứng minh** Kiểm âm, chứng nhận, nguồn và enrollment	37–42

Cách đọc CEO/CIO: phần chính. Kiến trúc, ATTT và developer: đối chiếu thêm phụ lục.

Bổ sung xác thực, tận dụng hệ thống ngân hàng

Đo hiệu quả trên một nghiệp vụ và một nhóm người dùng trước khi mở rộng

01

TCTC chủ động

Giữ tài khoản, hạn mức, quyền và quyết định thực thi tại hệ thống ngân hàng.

02

Người dùng thuận tiện

Một hành trình rõ ràng: xem nội dung, xác thực, nhận đúng trạng thái.

03

Kỹ thuật tích hợp nhẹ

BFF cho đăng nhập; Web SDK cho trải nghiệm; Backend cho kiểm chứng.

Góc nhìn	Chỉ số cần đo	Nguồn đo
Trải nghiệm	Hoàn tất, bỏ dở, thử lại; P50/P95	Kênh ngân hàng + sự kiện SaaS
Tích hợp / vận hành	Công triển khai, lỗi, fallback và hỗ trợ	UAT, nhật ký và báo cáo pilot

Phạm vi đầu tiên Chọn một điểm chạm có chủ nghiệp vụ, tiêu chí nghiệm thu và phương thức thay thế.

Tin cậy từ nền tảng định danh đến vận hành

Năng lực số hóa, định danh, xác thực và dịch vụ tin cậy; hồ sơ phải đúng phạm vi


CERTIFICATE OF REGISTRATION

IAS ACCREDITED Management Systems Certification Body MSCB-111

IAF

SIS CERT.™ We Do Not Sell, We Certify!

This Certificate has been awarded to

MOBILE-ID TECHNOLOGIES AND SERVICES JOINT STOCK COMPANY

Head Office: 1/11/74 Dang Thuy Tram Street, 13 Ward, Binh Thanh District, Ho Chi Minh City, Vietnam

Representative Office: Level 9, Thuy Loi 4 Building, 286-288 Nguyen Xi Street, Ward 13, Binh Thanh District, Ho Chi Minh City, Vietnam

In recognition of the organization's Management System which complies with

ISO/IEC 27001:2022

Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems

The scope of activities covered by this certificate is defined below

Solutions for digital identity, secure authentication and digital signing - Trusted Hub, GoPaperless, Mobile-ID, CheckID, Facial Sense, Trusted Pay, Trusted Care, TrustedID, Trusted Kioware, X-Avenue, MRConnect, Qrypto, Blockchain Services Infrastructure, Remote Signing, Time-Stamping Authority, PKI tokens, eID cards and ePassport certificates.

SoA Deatails : SOA.01, Version: V.02, Dated: 01/10/2024

SYNDICATE OF INTERNATIONAL SYSTEM CERTIFICATIONS

Certificate Number: SIS3512241008
Date of Initial Registration: 05.12.2024
Latest Date of Issue: 05.12.2024
Next surveillance due on: 05.11.2025
Expiry Date: 04.12.2027
Re-certification Due on: 05.11.2027

Managing Director

Note: The certificates is the property of SIS Certifications & the Validity of the Certificate is subject to the successful completion of Surveillance Audit on or before the due date. (In case Surveillance Audit is not allowed to be conducted, this Certificate shall be suspended and must be returned immediately upon request.)

Certified Organization is responsible for maintaining the compliance of the relevant standard rules. Any significant changes in the scope of the certification or standard referred above render this certificate invalid

Corporate office- SIS Certifications Pvt. Ltd.
Unit No. 514, 5th Floor, Vipul Business Park, Sector-48, Sohna Road, Gurgaon-122018, Haryana, India.
International Subcontractor Key Locations: Qatar, Egypt, Italy, Canada & USA.
Email us:- support@siscertifications.com, Call /Whatsapp: +91-9643073391
The status of this certificate can be verified on "https://siscertifications.com
Web:- www.siscertifications.com

Issue No: 01

Quản trị an toàn thông tin

ISO/IEC 27001:2022 · SIS3512241008 · SIS Certifications. Hồ sơ ISMS có thời hạn in đến 04/12/2027.

Định danh và xác thực

Hồ sơ eID HIGH và PAD của mô-đun Trusted Hub; đối chiếu đúng sản phẩm, nền tảng và cấu hình.

Năng lực triển khai

Kiến trúc, backend, frontend/SDK, sinh trắc, ATTT, vận hành và hỗ trợ phối hợp theo phạm vi dự án.

Phạm vi hồ sơ Chứng nhận mô-đun không thay kiểm thử Palm/Facial; tình trạng duy trì cần xác minh.

SaaS và bộ tích hợp từ Mobile-ID

TCTC quản lý kênh số và nghiệp vụ; phạm vi bàn giao được chốt theo hợp đồng

GoPaperless SSO SaaS

OIDC/Passkey và điều phối xác thực.

Capture, Palm/Facial và kết quả gắn yêu cầu.

Tenant, chính sách, log và vận hành.

Web SDK + API

Component nhúng, hợp đồng yêu cầu/kết quả và mã tham chiếu.

Thiết bị + connector

PalmDevice, driver/bộ cài và cấu hình được kiểm chứng.

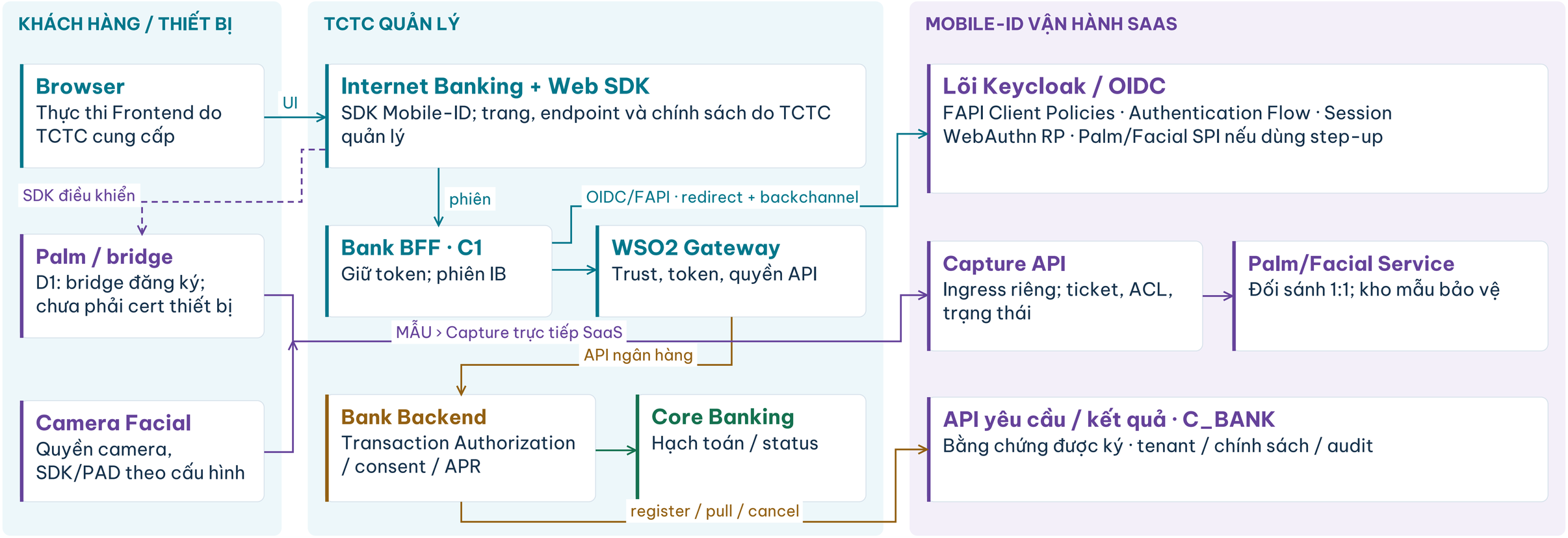
Hạ tầng TCTC

Frontend, BFF, WSO2, Backend và Core do TCTC quản lý. Mobile-ID hỗ trợ tích hợp theo phạm vi; không mặc định cung cấp license/vận hành WSO2.

Trạng thái cung cấp SDK, API và connector cần đối chiếu readiness trước khi cam kết ngày khởi động.

Ba vùng sở hữu, một hành trình xác thực

OIDC/FAPI bảo vệ tuyến OAuth/API; Web SDK và Capture là phần mở rộng GoPaperless



Tuyến mẫu không qua BFF/token endpoint. Các khối là module logic, không phải số lượng máy chủ.

Quyền quyết định GoPaperless xác thực; Backend kiểm chứng và cho phép; Core hạch toán.

BFF, Frontend và Backend có hợp đồng riêng

Tái sử dụng cùng mô hình khi bổ sung phương thức xác thực

01 → 02 → 03

01 / BFF

OIDC/FAPI: metadata, client, callback, token và phiên Internet Banking.

02 / Frontend

Web SDK: khởi chạy Palm/Facial, giao diện, cancel/retry và trạng thái.

03 / Backend

REST API: tạo yêu cầu, lấy bằng chứng, kiểm context và quyết định đúng lệnh.

Điểm tích hợp	Mobile-ID bàn giao	TCTC thực hiện
BFF	Profile, sandbox và hướng dẫn	Tích hợp client; kiểm callback/token
Frontend	Web SDK, component và connector	Gắn SDK; phê duyệt CSP/origin/cài đặt
Backend	API/schema, bằng chứng và mẫu verify	Consent, APR, quyền và Core contract

Giữ bí mật Khóa client và token ngân hàng ở phía máy chủ; Frontend dùng phiên được bảo vệ.

Một lệnh JavaScript để khởi chạy Palm hoặc Facial

GoPaperless đóng gói giao diện, thu nhận và đối sánh; TCTC giữ quyết định nghiệp vụ

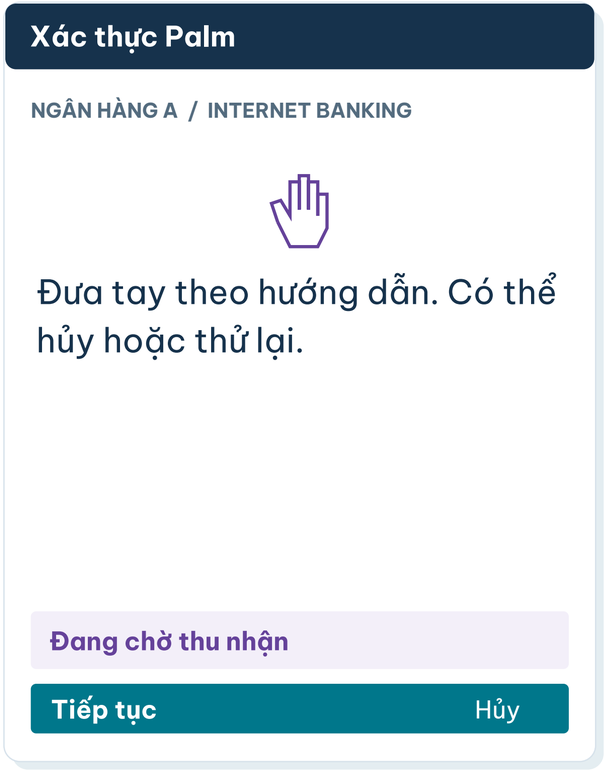
HỢP ĐỒNG SDK ĐỀ XUẤT

```
const result = await
 GoPaperless.authenticate({
  requestToken,
  method: "palm",
  container: "#authentication"
 });
```

Đổi method thành "facial" để dùng camera.

requestToken do Backend cấp; có hạn và gắn đúng người, lệnh, phiên bản.

result chỉ phục vụ cập nhật giao diện.



Giao diện minh họa · Dữ liệu giả lập

01 / Khởi tạo

Backend tạo yêu cầu chính thức.

02 / Thu nhận

SDK + Capture + đối sánh.

03 / Kiểm chứng

Backend lấy bằng chứng và cho phép.

Phân biệt kết quả SDK hoàn tất không đồng nghĩa giao dịch đã được cho phép hoặc hạch toán.

Đơn giản cho Frontend, kiểm soát ở máy chủ

Profile API-only verification đề xuất cho SDK nhúng; đăng nhập OIDC là luồng độc lập

01

Backend đăng ký

TCTC xác định chủ thể, TXN, hash, phiên bản, thời hạn và phương thức được phép.

02

Frontend gọi SDK

Nhận launch token ngắn hạn; hiển thị nội dung và khởi chạy trải nghiệm.

03

Backend kiểm chứng

Pull bằng chứng từ SaaS; kiểm consent, context và trạng thái trước APR.

GoPaperless xử lý

Giao diện, kết nối thiết bị/camera, chất lượng/PAD, Capture, đối sánh 1:1 và kết quả.

TCTC kiểm soát

Dữ liệu lệnh, nội dung hiển thị, quyền người dùng, quyết định thực thi và trạng thái Core.

Không đánh đồng requestToken là quyền khởi chạy giới hạn; không phải access token ngân hàng.

Giống sự thuận tiện, phân biệt mức bảo đảm

SPC là tham chiếu trải nghiệm gọi API; SDK đối sánh máy chủ là cơ chế khác

Phạm vi	SPC / WebAuthn	Web SDK GoPaperless đề xuất
Khởi chạy	API JavaScript của trình duyệt	API JavaScript do Mobile-ID đóng gói
Giao diện xác nhận	Trình duyệt kiểm soát theo SPC	Component/trang web tùy biến
Cơ chế xác thực	Credential khóa công khai	Thu nhận và đối sánh sinh trắc tại SaaS
Dữ liệu sinh trắc	WebAuthn không gửi mẫu cho RP	Truyền mẫu tới Capture theo phương án
Kiểm chứng	Backend kiểm assertion / challenge	Backend kiểm bằng chứng / context

Giới hạn HTML/SDK tùy biến không mặc định có bảo đảm hiển thị tương đương SPC.

Cài bộ nền một lần, ứng dụng gọi SDK

Chốt model, firmware, OS/browser và cơ chế kết nối trước ngày khởi động

01

Web SDK

Điểm gọi thống nhất trong Frontend; kiểm môi trường và hiển thị hướng dẫn.

02

Connector / bridge

Bộ cài ký số; onboarding D1; chỉ cho phép origin đã đăng ký.

03

SDK / PalmDevice

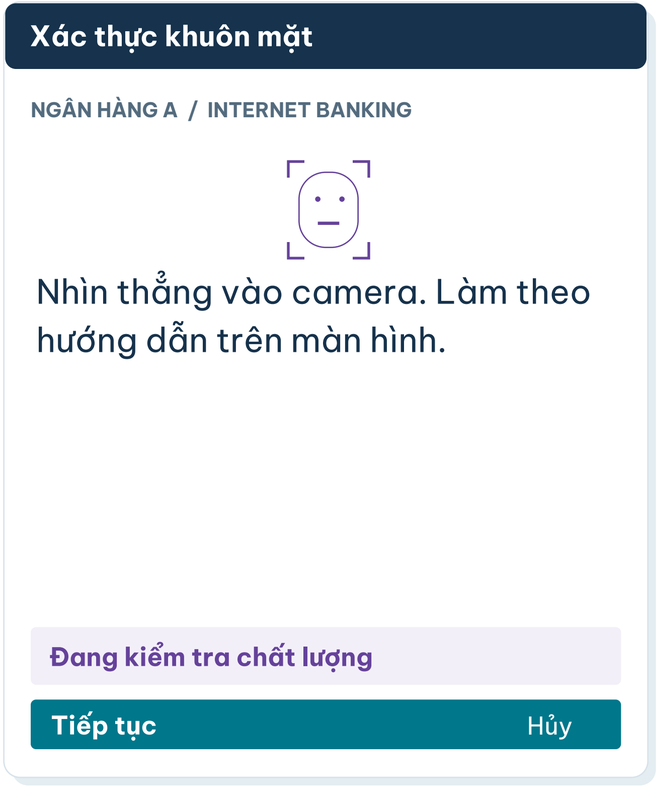
Thu nhận theo SDK nhà sản xuất; kiểm chất lượng/PAD theo hồ sơ.

Vòng đời	Kiểm soát cần có	Điểm nghiệm thu
Cấp và cài đặt	Installer được phê duyệt; đăng ký bridge/khóa	Đúng tenant, máy trạm và origin
Cập nhật / gia hạn	Phiên bản, rollout theo nhóm, thay khóa	Tương thích và rollback
Thu hồi / thay máy	Chặn bridge, ticket và capture liên quan	Thiết bị bị thu hồi không được dùng

Giới hạn thiết bị Không tự khẳng định USB/HID/UVC, attestation hoặc chứng thư nhúng trong PalmDevice.

Dùng cùng SDK, kiểm soát riêng cho Facial

Quyền camera, chất lượng, PAD và chống injection phải theo hồ sơ triển khai thực tế



Giao diện minh họa · Dữ liệu giả lập

01

Cho phép camera

HTTPS; quyền người dùng; không cấp quyền âm thầm.

02

Thu nhận có hướng dẫn

Ánh sáng, tư thế, chất lượng và PAD theo SDK.

03

Gửi Capture SaaS

Phiên mới, ticket ngắn hạn và dữ liệu theo profile.

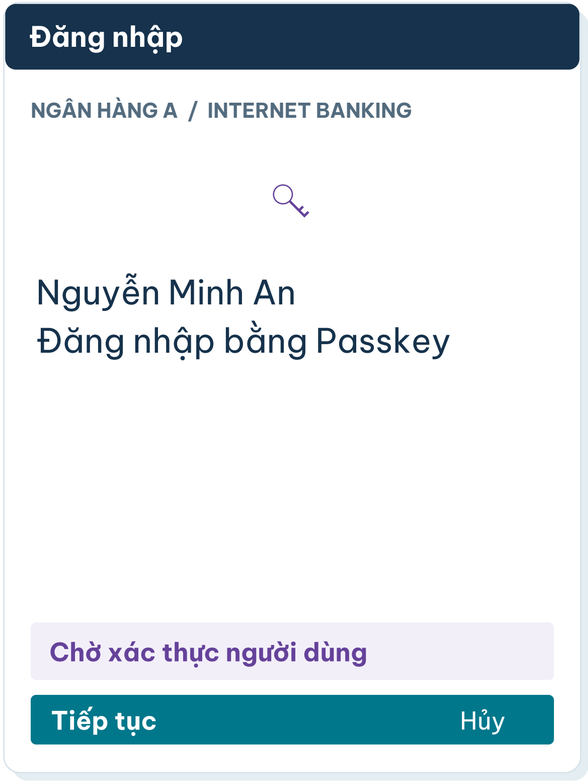
Thiết bị / OS / browser

Phê duyệt ma trận tương thích; cơ chế nhúng/iframe phải kiểm CSP, camera Permissions Policy và quyền origin.

Phân biệt Lấy được ảnh camera không đồng nghĩa đã có PAD hoặc chống giả mạo đạt yêu cầu.

Đăng nhập qua SaaS, phiên ngân hàng tại BFF

Browser redirect đúng OIDC; profile tham chiếu dùng mTLS và access token certificate-bound



Giao diện minh họa · Dữ liệu giả lập

A01 / Browser > BFF
Phiên liên kết, state, nonce, PKCE.

A02 / BFF / SaaS
PAR; client auth C1; browser redirect.

A03 / WebAuthn
Keycloak RP kiểm assertion và context.

code qua browser; token qua backchannel

A04 / Code > BFF
Đổi code; kiểm token; tạo phiên IB.

A05 / API ngân hàng
BFF > WSO2 > Backend > Core.

A06 / Trả dữ liệu
Đúng đường về browser; theo quyền.

Khóa riêng ở authenticator. Token ở BFF. RP ID minh họa: sso.example.com.

Kết quả Đã đăng nhập và truy cập API theo quyền; chưa xác nhận một lệnh chuyển tiền cụ thể.

Từ lệnh chính thức đến hạch toán có kiểm soát

API-only verification đề xuất: SDK nhúng; bằng chứng được Backend lấy trực tiếp từ SaaS



Giao diện minh họa · Dữ liệu giả lập

B01 / Tạo lệnh
Backend kiểm tài khoản, quyền, hạn mức; lưu TXN/v1.

B02 / Đăng ký AR
C_BANK › SaaS; subject, hash, hạn; launch token.

B03 / Xem & đồng ý
Hiển thị đúng nội dung; lưu consent; gọi SDK.

khởi chạy trải nghiệm SDK

B04 / Palm mới
SDK › bridge › Capture › đối sánh 1:1.

B05 / Kiểm chứng
Backend pull JWT_AUTH; kiểm context; tạo APR.

B06 / Gọi Core
Giữ chỗ APR bền vững; stable reference; status.

01 XÁC THỰC ĐẠT

02 TCTC CHO PHÉP

03 CORE THÀNH CÔNG

B07 / Trả trạng thái Thành công, từ chối hoặc chờ đối soát; SDK hoàn tất không thay kết quả Core.

Nội dung rõ, hành động ngắn, kết quả đúng

Nguyễn Minh An · Nguồn ****0128 · Trần Gia Bảo ****8899 · Phí 0 VND

01 / Xem lệnh

NGÂN HÀNG A / INTERNET BANKING

50.000.000 VND

Trần Gia Bảo · ****8899

Thanh toán hợp đồng HD-1026

Nguồn ****0128 · Phí 0 VND

Kiểm tra nội dung trước khi tiếp tục.

Lệnh TXN_0087 / v1

Tiếp tục | Hủy

02 / Thu nhận

NGÂN HÀNG A / INTERNET BANKING



Đưa tay theo hướng dẫn.
Không cần chọn lại tài khoản.

Đang thu nhận mới

Đang thu nhận | Hủy

03 / Xác thực đạt

NGÂN HÀNG A / INTERNET BANKING



Đang chờ ngân hàng kiểm chứng và xử lý giao dịch.

Chưa có kết quả Core

Tra cứu trạng thái

04 / Nhận kết quả

NGÂN HÀNG A / INTERNET BANKING



Thành công
Biên nhận RCPT_0087
Tham chiếu CB_0087

Core đã xác nhận

Xem biên nhận

Giao diện minh họa · Dữ liệu giả lập

Khi chưa rõ Core Hiển thị chờ đối soát và tra cứu lệnh gốc; không hướng dẫn tạo lại lệnh mới.

Đổi phương thức, giữ hợp đồng tích hợp

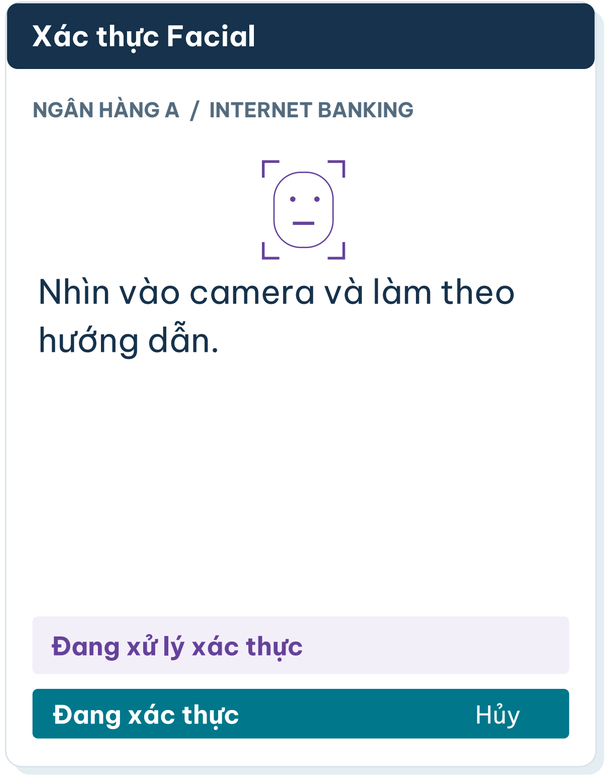
Cùng người dùng, lệnh và Backend; thay pipeline thu nhận bằng camera và Facial Service

HỢP ĐỒNG SDK ĐỀ XUẤT

```
const result = await
 GoPaperless.authenticate({
  requestToken,
  method: "facial",
  container: "#authentication"
 });
```

Tái sử dụng: AR, status API, bằng chứng và kiểm chứng Backend.

Thay đổi: quyền camera, chất lượng/PAD và tương thích.



Giao diện minh họa · Dữ liệu giả lập

C01 / Cấp quyền

Camera, HTTPS và origin hợp lệ.

C02 / Thu nhận mới

Chất lượng, PAD, ticket và Capture.

C03 / Kiểm chứng

Backend kiểm JWT_AUTH/consent; quyết định.

Phạm vi chứng nhận Facial và Palm có hồ sơ kiểm thử riêng; không chuyển phạm vi chứng nhận giữa hai phương thức.

Cấu hình theo tenant, triển khai có kiểm soát

Mô hình quản trị đề xuất; quyền sửa, phê duyệt và audit được chốt theo dự án

GoPaperless / Tenant ngân hàng A / Chính sách ứng dụng

- Tổng quan
- Ứng dụng
- **Phương thức**
- Thiết bị / bridge
- Trust / khóa
- Nhật ký

Ứng dụng: Internet Banking

Origin SDK: https://ib.bank.example

Phương thức: Palm / Facial

Giao diện: Logo, màu, tiếng Việt

Chính sách: Thu nhận mới cho giao dịch

Trạng thái: Bản nháp / Chờ phê duyệt

Xem trước SDK

NGÂN HÀNG A / INTERNET BANKING

Đưa tay theo hướng dẫn

Chờ thu nhận

Tiếp tục | Hủy

Giao diện minh họa · Không xác nhận tính năng quản trị đã phát hành

Vòng đời cấu hình Nháp > duyệt > thử nhóm > triển khai > theo dõi > khôi phục theo phân quyền.

Khách hàng luôn biết bước tiếp theo

Trạng thái SDK, yêu cầu xác thực và kết quả Core được quản lý riêng

Tình huống	Trải nghiệm khách hàng	Xử lý phía máy chủ
Hủy / hết hạn	Đã hủy hoặc yêu cầu đã hết hạn	Chặn hoàn tất muộn; query trạng thái gốc
Không khớp / PAD không đạt	Thử lại theo chính sách hoặc cách khác	Giới hạn lần thử; audit; không cấp APR
Mất thiết bị / từ chối camera	Hướng dẫn kiểm tra quyền, cài đặt	Không xác nhận ngầm; giữ context hợp lệ
Mất phản hồi upload	Đang kiểm tra kết quả thu nhận	Query CAP trước khi gửi lại
Core chưa rõ kết quả	Đang xử lý / chờ đối soát	Tra stable reference; không tạo lệnh mới

Fallback Chỉ chuyển phương thức được TCTC cho phép; phải giữ đúng lệnh, chủ thể và chính sách.

Ba kết quả độc lập, ba trách nhiệm rõ ràng

Không gộp tất cả thành một thông báo “Success”

Xác thực người dùng

GoPaperless kiểm phương thức và context; phát hành bằng chứng gắn yêu cầu.

Cho phép đúng lệnh

Backend kiểm bằng chứng, consent, quyền, nội dung và trạng thái; quản lý APR.

Hạch toán

Core xử lý theo mã ổn định; trả thành công, thất bại hoặc chưa rõ.

SDK callback chỉ cập nhật giao diện.

Trạng thái giao dịch hiển thị cho người dùng lấy từ nguồn Backend TCTC có thẩm quyền.

Bằng chứng dịch vụ Chữ ký của dịch vụ xác thực không mặc định là chữ ký pháp lý của khách hàng.

Đủ bộ nền trước khi hứa tích hợp nhanh

Trong đầu vào chưa có SDK/model production; các hợp đồng trong gói này là đề xuất

Hạng mục	Bộ bàn giao cần có	Điều kiện sẵn sàng
Web SDK / giao diện	Gói phiên bản, demo, docs và mã lỗi	Kiểm origin/CSP, hủy/retry và tương thích
Palm connector / thiết bị	BOM, driver, installer ký số, hướng dẫn	Model/firmware/OS/browser và PAD đã kiểm
Facial SDK	Camera, chất lượng, PAD và chống injection	Hồ sơ cấu hình, quyền và kiểm thử
Backend / BFF	OpenAPI, OIDC/FAPI, mẫu verify và trust	Sandbox, khóa/chứng thư và integration test
Vận hành	Runbook, rollback, UAT, SLA và hỗ trợ	Đầu mối, phê duyệt và tiêu chí nghiệm thu

Phân loại Đã có bằng chứng / cần cấu hình / cần phát triển / chưa có hồ sơ xác nhận.

Mẫu sinh trắc tách khỏi dữ liệu nghiệp vụ

Quyền xử lý và vị trí lưu trữ được chốt theo hợp đồng và phương án dữ liệu

01 → 02 → 03

Thu nhận

Chỉ lấy dữ liệu theo mục đích, quyền và yêu cầu hợp lệ.

Xử lý / lưu

Capture, đối sánh và kho mẫu bảo vệ trong phạm vi tenant.

Chia sẻ / kết thúc

TCTC nhận kết quả theo quyền; lưu/xóa và thu hồi theo lịch.

Miền dữ liệu	Bên quản lý theo mô hình	Quy tắc đề xuất
TXN / consent / APR	TCTC	Nội dung chính thức và quyết định nghiệp vụ
Mẫu / hồ sơ xác thực	GoPaperless theo hợp đồng xử lý	Mã hóa, ACL, retention, xóa và backup
Log / bằng chứng chia sẻ	Theo phạm vi hợp đồng	Không ảnh/template/token/khóa trong log

Cách ly tenant Không mặc định dùng chung mẫu giữa các TCTC hoặc nhận dạng 1:N liên ngân hàng.

Bảo vệ kênh, phiên, thu nhận và quyết định

Mỗi lớp có kiểm soát riêng; TLS hoặc chữ ký không tự giải quyết mọi rủi ro

Lớp	Kiểm soát thiết kế	Giới hạn cần hiểu
Browser / SDK	Origin allowlist, CSP, phiên bảo vệ, launch token ngắn hạn	Trang bị xâm nhập có thể làm sai nội dung hiển thị
Bridge / Capture	Onboarding, khóa, ticket, trạng thái và pipeline kiểm chứng	mTLS không tự chứng minh mẫu mới từ thiết bị thật
Kết quả / Backend	JWS, context, consent, replay và quyền trên lệnh	Đúng chữ ký nhưng sai lệnh vẫn phải từ chối
Thực thi / Core	Durable APR/dispatch, stable reference và đối soát	Idempotency key không tự bảo đảm exactly-once

Tính mới thu nhận Gắn challenge mới vào mẫu cũ không tự chứng minh vừa thu từ người dùng.

Giữ đúng vai trò từ tích hợp đến vận hành

Không suy ra quyền sở hữu hoặc quyền xử lý dữ liệu chỉ từ nơi đặt hệ thống

Thành phần	Mobile-ID	TCTC
SaaS / Capture / bằng chứng	Cung cấp, quản trị và vận hành theo SLA	Phê duyệt cấu hình, dữ liệu và trust
Web SDK / connector / thiết bị	Bàn giao theo model, phiên bản, phạm vi	Tích hợp, phê duyệt cài đặt và rollout
Frontend / BFF / WSO2	Hướng dẫn, hỗ trợ liên thông theo dự án	Sở hữu/quản lý và vận hành
Backend / consent / APR	Cung cấp kết quả xác thực	Kiểm chứng và quyết định đúng lệnh
Core / hạch toán	Không quyết định hạch toán	Xử lý giao dịch và nguồn kết quả
Trust / nghiệm thu	Đầu mối kỹ thuật SaaS	Đầu mối nghiệp vụ, Core và ATTT

Thương mại License/subscription WSO2 không thuộc giá SaaS mặc định nếu chưa có thỏa thuận riêng.

Hỗ trợ theo gói, đo đúng phạm vi

Các chỉ tiêu số cần thống nhất trong hồ sơ thương mại trước khi trở thành cam kết

Nhóm	Nội dung cần chốt	Ranh giới
P1–P4	Mức ảnh hưởng, thời gian phản hồi, cập nhật và mục tiêu khôi phục	Đầu mối và escalation hai bên
Availability / bảo trì	Cách đo, cửa sổ bảo trì, loại trừ và báo cáo	SaaS Mobile-ID; hạ tầng TCTC đo riêng
Khôi phục	RTO/RPO, backup/restore và diễn tập	Phụ thuộc phương án dữ liệu đã duyệt
Hỗ trợ / thay thiết bị	24/7 theo gói; hỗ trợ từ xa/tại chỗ; đổi máy	BOM, địa bàn và hợp đồng
Sự cố / kết thúc dịch vụ	Thông báo, điều tra, export và thu hồi quyền	Dữ liệu, bằng chứng, retention và xóa

Trạng thái chỉ tiêu Chưa có SLA số được phê duyệt trong đầu vào; không tạo số uptime/response giả.

Hai tuần cho phạm vi đã sẵn sàng

Mục tiêu tích hợp có điều kiện; go-live có kiểm soát khác triển khai đại trà

Thời gian	Đầu ra	Điều kiện chuyển chặng
Ngày 1–2	Tenant sandbox, thiết bị, kết nối và trust	Ngày 0 đạt; phiên bản/model chốt
Ngày 3–4	OIDC/FAPI/Passkey tại BFF	Callback, token và kiểm âm đạt
Ngày 5–6	Web SDK Palm/Facial và Backend contract	Capture và kiểm chứng đúng context
Ngày 7–8	UAT, lỗi, replay và đối soát	Tiêu chí đạt; lỗi tồn có chủ xử lý
Ngày 9	Production config, runbook và rollback	Phê duyệt ATTT/vận hành và trust
Ngày 10	Go-live phạm vi nghiệm thu; hỗ trợ tăng cường	Người phê duyệt cho phép triển khai

Điều kiện ngày 0 SDK/thiết bị/API sẵn sàng; môi trường, quyền cài, dữ liệu và đầu mối đã thống nhất.

Chốt gói theo quy mô và yêu cầu dịch vụ

Tách khởi tạo, thuê nền tảng, thiết bị và hỗ trợ; không tự đặt đơn giá

Pilot kiểm soát

Một nghiệp vụ, nhóm người dùng/điểm và tiêu chí nghiệm thu cụ thể.

Mở rộng triển khai

Tái sử dụng hợp đồng; quản lý tenant, thiết bị và rollout theo nhóm.

Dịch vụ theo yêu cầu

Cấu hình, dữ liệu, SLA và hỗ trợ phù hợp mô hình ngân hàng.

Cấu phần	Cơ sở chốt	Cần xác nhận
Khởi tạo / tích hợp	Phạm vi, môi trường và phần bổ sung	SDK/connector đã có hay cần phát triển
SaaS / mức sử dụng	Tenant, phương thức và sản lượng	Đơn vị tính, retry/hủy và vượt gói
Thiết bị / hỗ trợ	BOM, số lượng, địa điểm và SLA	Bảo hành, thay máy và kết thúc dịch vụ

Không che công phát triển Hai tuần chỉ áp dụng bộ nền sẵn sàng và phạm vi tích hợp chuẩn đã thống nhất.

Bắt đầu bằng khảo sát tích hợp và sandbox

Mobile-ID là đầu mối đề xuất; pháp nhân hợp đồng chốt trong hồ sơ thương mại

Chọn nghiệp vụ ưu tiên

Đăng nhập, xác nhận chuyển tiền hoặc một điểm chạm phù hợp.

Chốt bộ tích hợp

Model Palm, Facial SDK, Web SDK, BFF và API Backend.

Thống nhất pilot

Ngày 0, UAT, KPI, SLA và kế hoạch 10 ngày làm việc.

MOBILE-ID Anytime, Anywhere

Công ty Cổ phần Công nghệ và Dịch vụ Mobile-ID

info@mobile-id.vn

1900 6884 | +84 28 3622 2982

www.mobile-id.vn

gopaperless.mobile-id.vn

Tầng 9, Tòa nhà Thủy Lợi 4
286–288 Nguyễn Xí, Phường Bình Lợi Trung
TP. Hồ Chí Minh

Đăng ký khảo sát Nhận sandbox và bộ tích hợp — thống nhất phạm vi triển khai hai tuần.

Chuẩn nền tảng và phần mở rộng có ranh giới

Profile triển khai và tính sẵn sàng cần được xác nhận theo phiên bản thực tế

Phạm vi	Cơ sở	Áp dụng trong proposal
Đăng nhập	OpenID Connect	BFF + browser redirect; kiểm ID token
OAuth / bảo vệ API	FAPI 2.0 và RFC áp dụng	PAR, PKCE, client auth, token ràng buộc bên gửi
Passkey	WebAuthn / FIDO2	Khóa công khai; RP xác minh assertion
Xác nhận native	SPC nếu tương thích	Roadmap; không bắt buộc cho pilot hai tuần
Quyền chi tiết	OAuth RAR · RFC 9396	Tùy chọn cần đánh giá hỗ trợ
Palm/Facial / bằng chứng	Phần mở rộng GoPaperless	SDK, Capture, JWT_AUTH và API-only profile

SPI không phải SPC SPI là điểm mở rộng máy chủ Keycloak; không phải giao thức thiết bị hoặc API SPC.

Một hợp đồng yêu cầu và kết quả cho nhiều phương thức

Tên endpoint/schema là đề xuất; không khẳng định API production đã phát hành

Thao tác / endpoint dự thảo	Dữ liệu và quyền	Kết quả
POST /verification-requests	C_BANK; tenant/subject/TXN/hash/version; methods; consent policy	AR + trạng thái + thời hạn
POST /verification-requests/{id}/launches	Backend xác thực phiên; method từ tập cho phép; origin đã đăng ký	requestToken ngắn hạn; không URL query
GET /verification-requests/{id}	C_BANK; ACL tenant/subject/request	Trạng thái xác thực; không phải Core
GET /verification-requests/{id}/evidence	C_BANK; ACL và trạng thái bằng chứng	JWT_AUTH khi VERIFIED; pending khi chưa có
POST /verification-requests/{id}/cancel	C_BANK; kiểm trạng thái/đua với hoàn tất	Trạng thái cuối có thẩm quyền

Auth / retry Service principal riêng; idempotency + fingerprint; GET trạng thái sau timeout.

Hợp đồng SDK có đầu vào nhỏ, trạng thái rõ

Đặc tả thiết kế trong gói; không có SDK production hoặc thiết bị thật để kiểm thử

Thành phần	Hợp đồng đề xuất	Ràng buộc
authenticate(options)	requestToken; method; container; AbortSignal tùy chọn	Method phải được server cho phép
Kết quả hoàn tất	status; requestId; captureId nếu có; errorCode	Không có ảnh/template hoặc quyền chi tiền
Trạng thái giao diện	PREPARING / READY / CAPTURING / PROCESSING	Chỉ tín hiệu UX; không thay trạng thái Backend
Trạng thái cuối	COMPLETED / NOT_VERIFIED / CANCELLED / EXPIRED	COMPLETED chỉ kết thúc hành trình SDK
Lỗi tích hợp	DEVICE_UNAVAILABLE / CAMERA_DENIED / NETWORK_ERROR	Phân loại lỗi; query trạng thái trước retry
Hủy / phục hồi	signal; server cancel qua Backend; bounded retry	Ngừng local không tự hủy yêu cầu server

Mặc định an toàn Launch token không lưu localStorage, không log, không nằm trong URL; hết hạn phải cấp lại.

Ticket ràng buộc phiên; pipeline bảo vệ tính mới

Capture trực tiếp SaaS; profile proxy/egress ngân hàng là tùy chọn tách biệt

Chặng	Kiểm soát	Khi lỗi hoặc thử lại
P01 / SDK > bridge	Origin/extension allowlist; yêu cầu server; D1 đã đăng ký	Không có bridge: hướng dẫn cài; không bypass
P02 / Thiết bị thu nhận	SDK/model; chất lượng, PAD và chống injection theo hồ sơ	Mẫu cũ + challenge mới không chứng minh freshness
P03 / Upload Capture	CT có hạn; tenant/AR/CAP/subject/bridge; ACL ingress	Query CAP sau mất phản hồi; không upload mù
P04 / Đối sánh / kết quả	1:1; hash payload; trạng thái chống replay; audit	Cùng CAP khác payload bị chặn; retry có kiểm soát

Hợp đồng thu nhận mTLS D1 xác thực bridge; không tự chứng minh mẫu đến từ thiết bị thật vừa thu.

Đúng chữ ký là cần thiết, chưa đủ để cho phép lệnh

JWT_AUTH là profile bằng chứng GoPaperless; không phải token thanh toán mặc định FAPI

Đối tượng	Mục đích / nơi kiểm	Không được suy diễn
ID token	BFF kiểm OIDC: issuer/audience/nonce/exp	Không dùng audience=BFF để duyệt tại Backend
Access / refresh token	Access gọi API; refresh chỉ ở token endpoint	Không trả token ngân hàng cho JS
JWT_AUTH	Backend kiểm JWS + tenant/subject/AR/TXN/hash/version	Không chứa ảnh/template; không tự bảo đảm dùng một lần
APR	Hồ sơ/quyền cho phép nghiệp vụ phía TCTC	Không phải token SaaS cấp thay ngân hàng
Core reference	Theo dõi lệnh xử lý hạch toán	Không được suy thành công khi timeout

Profile kiểm chứng Pin typ/schema/alg/issuer/audience; khóa tin cậy, thời hạn, jti, context và trạng thái.

Các mã mẫu nối đúng hành trình và bằng chứng

Alias minh họa; không phải token, chứng thư hay bản tin wire hoàn chỉnh

Chặng	Tham chiếu mẫu	Dữ liệu kiểm tra
B01–B02 / Tạo và đăng ký	cus_0128 · TXN_0087 · AR_0087	H_TX / v1; 50.000.000 VND; chủ thể có quyền
B03 / Khởi chạy SDK	Launch token opaque · origin đã đăng ký	Method trong policy; consent gắn TXN/v1
B04 / Thu nhận	CH_0087 · CAP_0087 · CT_0087 · D1	Ticket, bridge, thời hạn và payload fingerprint
B05 / Kiểm chứng	JWT_AUTH_0087 · jti · APR_0087	Tenant/subject/context/consent; trạng thái mới
B06–B07 / Core và kết quả	CB_0087 · RCPT_0087	Stable reference; authoritative status; receipt khi thành công

Giá trị chính thức Core nhận account ID ngân hàng; ****0128/****8899 chỉ là thông tin hiển thị.

Yêu cầu, Capture, bằng chứng và APR có trạng thái riêng

Chuyển trạng thái có điều kiện và ghi nhận bền vững; không gom thành cờ success

Đối tượng	Vòng đời tham chiếu	Quy tắc
Yêu cầu AR	CREATED > PENDING > VERIFIED / NOT_VERIFIED / CANCELLED / EXPIRED	VERIFIED chưa cho phép hạch toán
Capture CAP	ISSUED > CAPTURING > UPLOADED > MATCHED / REJECTED	Retry khác CAP hoặc payload theo contract
Bằng chứng	PENDING > AVAILABLE / INVALIDATED	AR VERIFIED có thể cần chờ bằng chứng ký
APR phía TCTC	AUTHORIZED > RESERVED > EXECUTED / FAILED / RECONCILING	Giữ chỗ và dispatch bền vững
Lệnh / Core	DRAFT > AWAITING_AUTH > READY > DISPATCHED > kết quả	Sửa nội dung vô hiệu xác nhận phiên bản cũ

Đua trạng thái Cancel, hết hạn và hoàn tất phải được giải quyết nguyên tử theo trạng thái server.

Chưa rõ kết quả thì đối soát lệnh gốc

Stable reference do ngân hàng quản lý; cần Core contract về dedupe và status query

01

Thành công xác định

Đánh dấu EXECUTED; hoàn tất APR; phát biên nhận đúng Core reference.

02

Thất bại xác định

FAILED; trả lý do theo quyền; xử lý APR theo policy đã chốt.

03

Timeout / chưa rõ

RECONCILING; tra mã ổn định; không tạo lệnh mới hoặc release APR tùy tiện.

Điểm crash	Khôi phục đề xuất	Bằng chứng nghiệm thu
Sau reserve / trước dispatch	Khôi phục durable record; kiểm quyền và trạng thái	Không mất dấu hoặc tạo quyền mới
Sau dispatch / trước response	Query Core theo stable_ref trước resend	Không hạch toán lặp khi response bị mất
Hai worker cùng xử lý	Conditional update/lock và dispatch ownership	Một logical execution theo Core contract

Giới hạn bảo đảm Không tuyên bố exactly-once chỉ bằng JWT hoặc idempotency key.

C1, C_BANK và D1 là các danh tính khác nhau

Kho khóa, rotation, thu hồi và xử lý pending được thống nhất theo từng chủ thể

Danh tính	Chủ thể / quyền	Quản lý vòng đời
C1 / ib-bff	BFF; OIDC confidential client; certificate-bound access token theo profile	Đăng ký client/cert; khóa server; rollover không tự đổi binding token cũ
C_BANK	Backend; register/pull/cancel; ACL tenant và request	Service principal riêng; giới hạn quyền; thu hồi và audit
D1	Native bridge đã onboarding; quyền Capture giới hạn	Installer/khóa native; origin allowlist; đổi thiết bị và revoke
K_TX_01	Dịch vụ ký JWT_AUTH; issuer/JWKS được pin theo trust	Algorithm allowlist; kid cache; rotation; xử lý lộ khóa

Tin cậy khóa Không fetch jku/x5u tùy ý từ JWT; proxy phải chặn giả header và bypass ingress.

Chặn sai origin, bridge và thu nhận không hợp lệ

Đây là ca kiểm thử đề xuất; chưa phải báo cáo hệ thống đã đạt

Mã / tình huống	Kết quả mong đợi	Ánh xạ
N01 / Origin lạ hoặc token sai scope	Không khởi chạy/capture; audit theo policy	B03 / P01
N02 / Không có bridge hoặc camera bị từ chối	Thông báo rõ; không tự xác thực thành công	B04 / C01
N03 / D1 hết hạn hoặc bị thu hồi	Ingress chặn; không cấp quyền API ngân hàng	P03
N04 / CT sai AR/CAP/subject hoặc hết hạn	Từ chối upload; không tạo bằng chứng thành công	P03
N05 / Upload timeout; CAP trùng khác payload	Query trước retry; chặn thay mẫu dưới cùng CAP	P03 / P04
N06 / Replay mẫu, PAD hoặc chất lượng không đạt	Pipeline phát hiện theo khả năng đã kiểm; không cấp APR	B04

Cần đo thực tế OS/browser/model, PAD và chống injection phải có kết quả kiểm thử theo cấu hình.

Không cho phép khi sai lệnh hoặc chưa rõ bằng chứng

Kiểm chứng độc lập với callback SDK và phiên SSO đang tồn tại

Mã / tình huống	Kết quả mong đợi	Ánh xạ
N07 / JWT sai typ/alg/iss/aud/kid/chữ ký	Từ chối; không APR; không lấy khóa từ URL tùy ý	B05
N08 / Đúng chữ ký, sai tenant/subject/TXN/hash/v	Từ chối context mismatch; audit	B05
N09 / Hết hạn, jti replay hoặc chưa đủ mới	Không tạo thêm quyền; query trạng thái gốc	B05
N10 / Thiếu consent, sửa lệnh hoặc cancel thắng	Không APR; vô hiệu xác nhận cũ	B03 / B05
N11 / Callback hoàn tất, evidence còn pending	Không duyệt theo JS; bounded poll phía Backend	B05
N12 / Worker đua, Core timeout hoặc crash	Durable reserve/dispatch; query stable_ref; đối soát	B06

Bổ sung nghiệm thu Test sai C1/cnf, quyền tài khoản, refresh token, tenant isolation và thu hồi khóa.

Mỗi hồ sơ có đối tượng và phạm vi riêng

Bản hồ sơ có sẵn không tự chứng minh tình trạng duy trì hiện hành tại tổ chức cấp

Hồ sơ / đơn vị	Đối tượng / số / thời hạn	Cách sử dụng
ISO/IEC 27001:2022 / SIS	ISMS Mobile-ID · SIS351224I008 05/12/2024–04/12/2027	Hồ sơ quản trị; xác minh duy trì
PAD Level 2 / TAYLLORCOX	eIDAS eID 2.0 trong Trusted Hub; Android/iPhone PCEB 26/04/06 · 06/04/2026–05/04/2028	Không suy ra PAD Palm
eID HIGH / TAYLLORCOX	Mô-đun eIDAS eID 2.0 trong Trusted Hub QSCD PCEB 26/04/07 · 07/04/2026–06/04/2028	Không chuyển sang mọi module SaaS
OpenID Connect / OIDF	Mobile-ID SSO v1.0; các profile OP trong registry	Không phải chứng nhận FAPI SaaS
FIDO2 / công bố Mobile-ID	Trusted Hub Server / Trusted Key SDK; cần mã và phiên bản chứng nhận gốc	Phân biệt chứng nhận và membership

Tra hồ sơ Nguồn và bản PDF chứng nhận trong gói; cần xác minh trạng thái trước nghiệm thu.

Tài liệu chuẩn để đối chiếu thiết kế

Liên kết mở được từ PDF; phiên bản triển khai phải được chốt trong dự án

FAPI 2.0 Security Profile Final
OpenID Foundation · Mở tài liệu ›

OpenID Connect Core
OpenID Foundation · Mở tài liệu ›

WebAuthn Level 3
W3C · Mở tài liệu ›

SPC · Candidate Recommendation Draft
W3C · 13/10/2026 · Mở tài liệu ›

OIDC/FAPI và Client Policies
Keycloak · Mở tài liệu ›

Authentication SPI
Keycloak · Mở tài liệu ›

mTLS / certificate-bound access tokens
RFC 8705 · Mở tài liệu ›

PAR / JWT / JWT Best Practices
RFC 9126 · 7519 · 8725 · Mở tài liệu ›

Native Messaging
Chrome for Developers · Mở tài liệu ›

Camera / getUserMedia
MDN Web API · Mở tài liệu ›

Nguồn bổ sung Registry OIDF, Mobile-ID, GoPaperless và hồ sơ chứng nhận được ghi trong bảng nguồn của gói.

Đăng ký mẫu trước, xác thực 1:1 khi sử dụng

Enrollment, xác thực và hạch toán là ba quy trình khác nhau

01

Xác định danh tính

Nguồn hồ sơ tin cậy; ánh xạ subject SaaS và khách hàng ngân hàng.

02

Đăng ký mẫu

Quyền/mục đích, thu nhận và chất lượng theo thiết bị/phương thức được duyệt.

03

Kích hoạt / thu hồi

Quản lý trạng thái mẫu, thay đổi chủ thể và khả năng sử dụng theo tenant.

Trường hợp	Quy tắc	Điều kiện
Chưa có mẫu / mẫu bị thu hồi	Chuyển enrollment riêng hoặc phương thức khác	Không tự enrollment trong thanh toán
Thay thiết bị / đổi bridge	Onboarding lại theo policy	Không suy diễn D1 là danh tính khách hàng
Rút đồng ý / kết thúc dịch vụ	Chặn dùng theo quyền; xử lý lưu/xóa riêng	Retention, backup và căn cứ theo hợp đồng

Phạm vi matching 1:1 với subject đã xác định; không tìm kiếm liên ngân hàng hoặc chia sẻ mẫu mặc định.

Chọn một profile giao dịch, kiểm thử đến cùng

Profile SDK API-only là phương án chính đề xuất; step-up OIDC là phương án tùy chọn

Nội dung	SDK API-only / chính	OIDC step-up / tùy chọn
Khởi chạy	Backend cấp requestToken; Frontend gọi SDK	BFF tạo yêu cầu OIDC gắn AR; browser redirect
Điều phối xác thực	Dịch vụ yêu cầu/Capture; không bắt buộc SPI	Keycloak Authentication Flow/SPI kiểm context
Đường trả kết quả	SDK báo UX; Backend pull bằng chứng	Code về BFF; Backend pull bằng chứng riêng
Quyết định TCTC	Backend kiểm consent/context/state rồi APR	Cùng quy tắc; ID token không thay JWT_AUTH
Điều kiện duyệt	API/SDK đã có; trust, Capture và UAT được kiểm	Cộng thêm flow bắt buộc, độ mới và liên kết OIDC

Mở pilot Đủ SDK/thiết bị, Core contract, trust, dữ liệu, vận hành và người phê duyệt trước ngày 0.