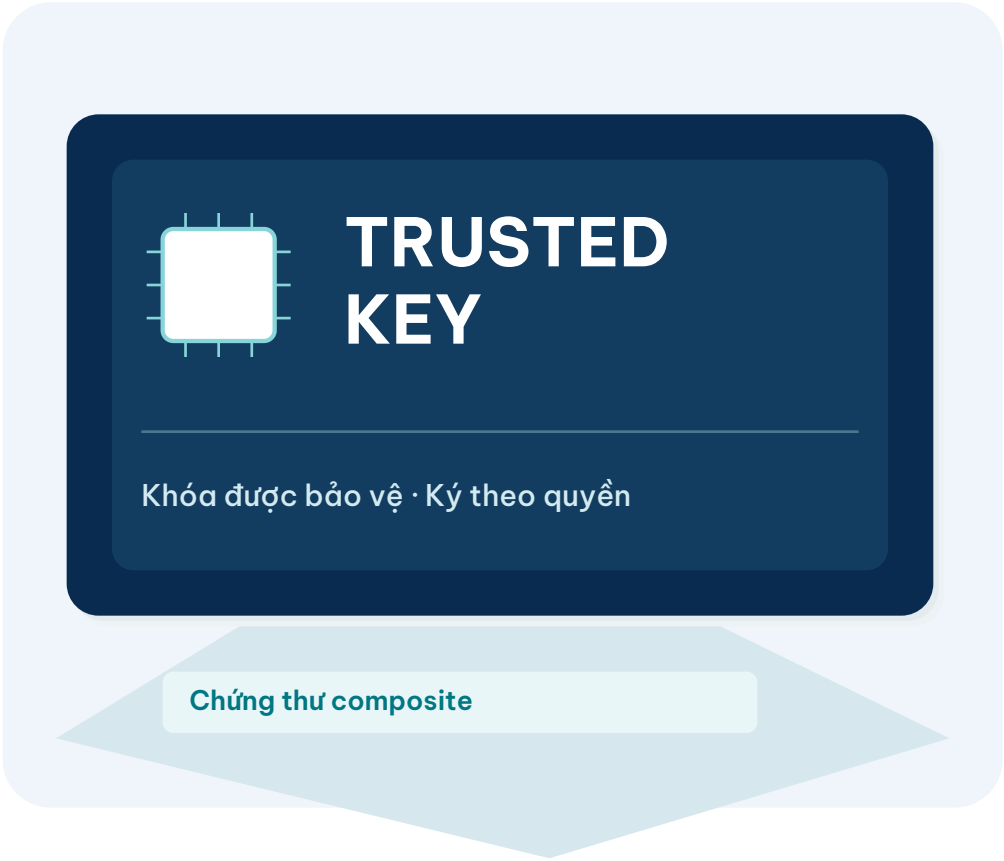
HẠ TẦNG TIN CẬY SỐ HẬU LƯỢNG TỬ

MOBILE-ID QUANTUMSAFE ECOSYSTEM

Niềm tin số.
Sẵn sàng chuyển đổi.

Hệ sinh thái quản lý chứng thư composite, bảo vệ khóa phần cứng và ký–xác minh PQC.

CA / TSP · KHỐI CƠ YẾU · CƠ QUAN QUẢN LÝ



Minh họa chức năng · Không phải ảnh sản phẩm

Một nền tảng chung. Một lộ trình có thể triển khai.

Mật mã hậu lượng tử (PQC) được đưa vào các dịch vụ tin cậy theo từng phạm vi được kiểm chứng.

Bảo vệ khóa. Chuyển đổi dịch vụ. Duy trì bằng chứng.

Trusted Key cho tuyến ký cục bộ. HSM cho khóa hạ tầng và tuyến ký máy chủ.

Bảo toàn đầu tư

Kết nối hạ tầng khóa công khai (PKI) hiện hữu với lớp mật mã mới; duy trì nghiệp vụ trong quá trình chuyển đổi.

Khởi đầu trong sáu tháng

Ưu tiên một tuyến cấp chứng thư–ký–xác minh trên Windows, cùng thiết bị và phân hệ quản trị đã chọn.

Mở rộng đến 2029

Kết nối ký từ xa, dấu thời gian, chuyển phát và bảo quản bằng chứng theo các cổng nghiệm thu.

Phạm vi · 3	Kiến trúc · 10	Triển khai · 37	Hợp tác · 44

Quyết định khởi đầu: chọn chủ trì, nghiệp vụ ưu tiên, phạm vi pilot và tiêu chí chấp nhận.

Nhận được gì sau một dự án QuantumSafe?

Phạm vi đề xuất được chốt theo cấu hình, quyền sử dụng và tiêu chí nghiệm thu.

Mobile-ID cung cấp

Trusted Key; phần mềm tích hợp; Wrapper, Agent và bộ mẫu theo quyền được cấp.

Khách hàng chuẩn bị

Chính sách, hạ tầng, license, chủ nghiệp vụ, người dùng và dữ liệu thử được phép.

Hai bên phối hợp

Thiết kế, tích hợp CA/VA và quản trị; kiểm thử, đào tạo, nghiệm thu và chuyển giao.

Phụ thuộc bên ngoài

HSM, Card OS, hệ điều hành và ứng dụng đích; hỗ trợ theo phiên bản/cấu hình.

Đầu ra: thiết kế + bộ cài/cấu hình + mẫu chứng thư/hồ sơ + kết quả kiểm thử + tài liệu vận hành.

Bắt đầu từ tài sản có vòng đời tin cậy dài.

Chuyển đổi mật mã cần đi trước thời điểm tổ chức phải thay đổi đồng loạt.



Chứng thư và khóa

Hạ tầng cấp phát, thiết bị và bên sử dụng có thời gian thay thế khác nhau.



Hồ sơ và bằng chứng

Tài liệu cần được kiểm tra qua nhiều vòng đời thuật toán, chứng thư và phần mềm.



Kết nối và dữ liệu

Kênh truyền, giao diện dịch vụ và dữ liệu lưu trữ cần chính sách bảo vệ riêng.

Ưu tiên theo giá trị tài sản, thời gian bảo vệ và độ khó chuyển đổi; không dự báo thời điểm máy tính lượng tử phá vỡ hệ thống.

Mobile-ID · Hệ sinh thái QuantumSafe · Danh mục năng lực

Mỗi tổ chức có một mục tiêu chuyển đổi rõ ràng.

Kiến trúc dùng chung; chính sách vận hành và quyền quyết định thuộc từng tổ chức.



Tổ chức chứng thực

Mở tuyến chứng thư và ký số mới; quản lý vòng đời, thiết bị và khả năng liên thông.



Cơ quan quản lý / khối cơ yếu

Có kiến trúc tham chiếu, ranh giới khóa, phạm vi đánh giá và cơ sở xem xét từng cấu hình.



Tổ chức sử dụng

Tích hợp nghiệp vụ từng bước; xác minh được hồ sơ và kiểm soát chi phí chuyển đổi.

Phạm vi chấp nhận và yêu cầu thẩm định được xác định theo từng hệ thống và nghiệp vụ.

PQC trở thành năng lực xuyên suốt hạ tầng số.

Các sản phẩm dùng chung lớp khóa, chứng thư, chính sách và bằng chứng; mức sẵn sàng được quản lý riêng.

Danh tính & quyền
CheckID · TrustedID · SSO · Passkey

Chứng thư & vòng đời
CA cấp · VA trạng thái · RA đăng ký · TMS thiết bị

Khóa & tích hợp
Trusted Key · HSM · Provider · SDK

Ký & tài liệu
GoPaperless · Trusted SIC · Agent

Thời gian & chuyển phát
Trusted TSA · Trusted Delivery

Xác minh & bảo quản
Verifier · Trusted LTANS · Records

XUYÊN SUỐT — **Kiểm kê mật mã · Chính sách · Giám sát · Thay thuật toán · Bằng chứng**

Mobile-ID · Hệ sinh thái QuantumSafe · Danh mục năng lực

Chọn đường chuyển đổi phù hợp với bên nhận.

Bảo toàn nghiệp vụ hiện tại trong khi bổ sung năng lực mật mã mới.

01

Hạ tầng hiện hữu

Kiểm kê khóa, chứng thư, ứng dụng và nơi xác minh. Giữ đường kiểm tra hồ sơ cũ.

→

02

Giai đoạn chuyển tiếp

Chọn composite, chữ ký độc lập hoặc bằng chứng bổ sung theo khả năng các bên.

→

03

Phạm vi hậu lượng tử

Mở vận hành trên tổ hợp đã nghiệm thu; giảm thuật toán cũ theo chính sách.

Composite là một cấu trúc mật mã kết hợp; hai chữ ký độc lập hoặc bằng chứng PQC bổ sung là các phương án khác.

Mỗi phân hệ có trạng thái và điều kiện mở dịch vụ.

Nguồn công bố và thông tin Mobile-ID được tách khỏi kết quả nghiệm thu của dự án.

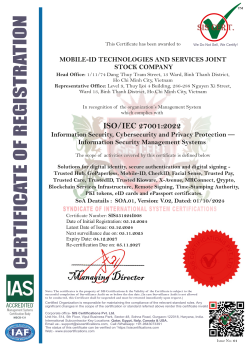
Phân hệ	Cơ sở / mức sẵn sàng	Điều kiện chấp nhận
EJBCA / HSM / Windows	Nền tảng có tài liệu hãng	Chốt release, firmware, build và thuật toán
Trusted Key / Wrapper	Mobile-ID xác nhận; chốt tổ hợp	BOM, Card OS, applet, build và bộ thử
Provider / .NET SDK	Công bố thí điểm trên QuantumSafe	Ma trận API, dữ liệu ký và lỗi
CA/VA / Agent / hồ sơ	Thí điểm / tích hợp theo dự án	Cấp–ký–xác minh và vòng đời đạt UAT
Dịch vụ / nền tảng mới	Thí điểm hoặc roadmap riêng	TSA/SIC theo tổ hợp; macOS mục tiêu 2028

Hồ sơ chứng nhận, năng lực PQC và khả năng tương thích là ba phạm vi được công bố riêng.

QuantumSafe · Danh mục năng lực EJBCA · Chứng thư composite Microsoft · Windows PQC

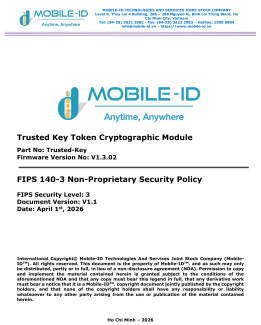
Ba hồ sơ bảo đảm. Ba phạm vi được xác định.

Hệ thống quản lý an toàn, mô-đun mật mã và thiết bị ký máy chủ có hồ sơ riêng.



ISO/IEC 27001:2022

Hệ thống quản lý an toàn



FIPS 140-3 Level 3

Module Trusted Key Token



QSCD / SAM

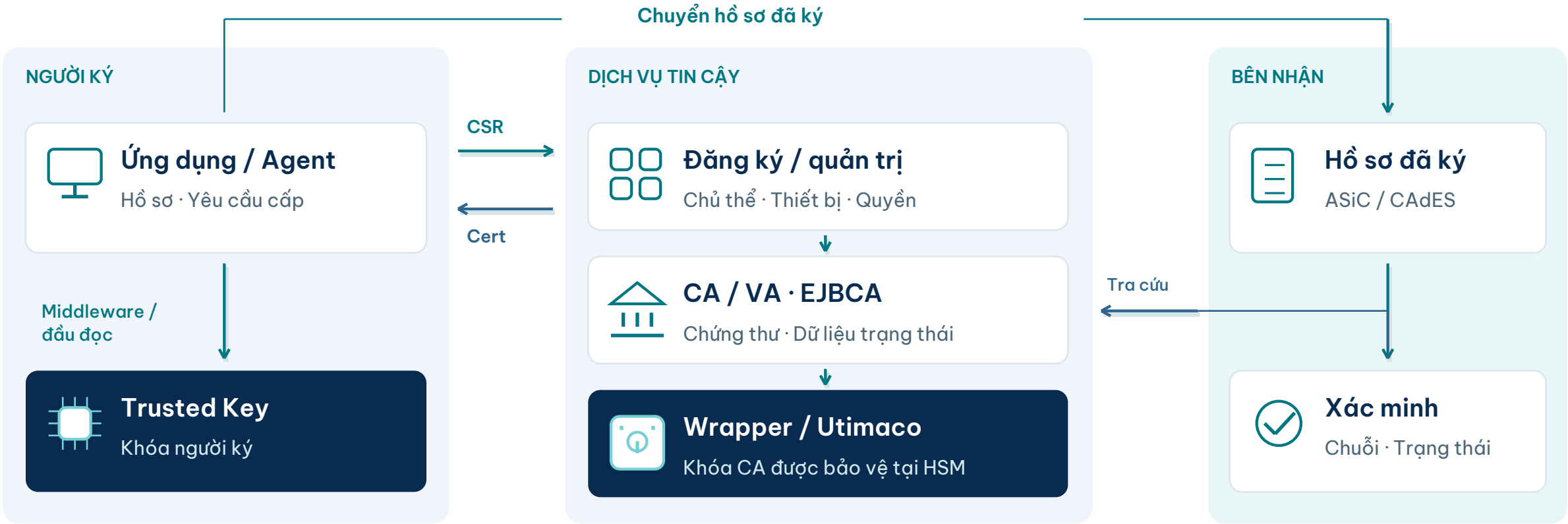
Hạ tầng ký máy chủ theo hồ sơ

Chứng nhận gắn đúng chủ thể, module và cấu hình; năng lực PQC mới cần bằng chứng riêng.

NIST · Hồ sơ 5331 ISO · Hồ sơ Mobile-ID SAM/QSCD · Hồ sơ Mobile-ID

Ba miền tin cậy. Hai tuyến xử lý độc lập.

Luồng cấp chứng thư và luồng chuyển hồ sơ ký được tách để thấy rõ trách nhiệm.



EJBCA · Chứng thư composite Mobile-ID · Kiến trúc JavaCard Utimaco · Quantum Protect

Khóa ở đúng nơi. Quyền sử dụng được phân định.

Mô-đun bảo mật phần cứng (HSM) bảo vệ khóa hạ tầng; Trusted Key bảo vệ khóa người ký cục bộ.

Khóa cấp chứng thư

Khóa được bảo vệ

Nằm tại HSM trong miền quản trị của tổ chức chứng thực; quản lý bằng nghi thức khóa và phân quyền.

Khóa ký cục bộ

Khóa được bảo vệ

Nằm trong Trusted Key theo cấu hình; được sử dụng qua applet và phần mềm tích hợp.

Khóa ký từ xa

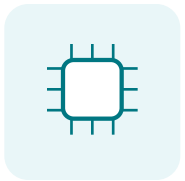
Khóa được bảo vệ

Nằm ở hạ tầng ký máy chủ theo thiết kế riêng; kích hoạt bằng quyền gắn giao dịch.

Ứng dụng nhận kết quả phép ký; khóa bí mật không đi vào gói hồ sơ. Log hỗ trợ phải loại bí mật.

Composite xuất hiện ở ba lớp cấu hình riêng.

Khóa chủ thể, chữ ký CA và chữ ký hồ sơ là các lựa chọn cần kiểm tra độc lập.



Khóa chủ thể

Khóa công khai trong chứng thư; khóa bí mật tương ứng được bảo vệ tại thiết bị.



Chữ ký của CA

CA ký chứng thư bằng khóa trong HSM; thuật toán được cấu hình theo chuỗi tin cậy.



Chữ ký hồ sơ

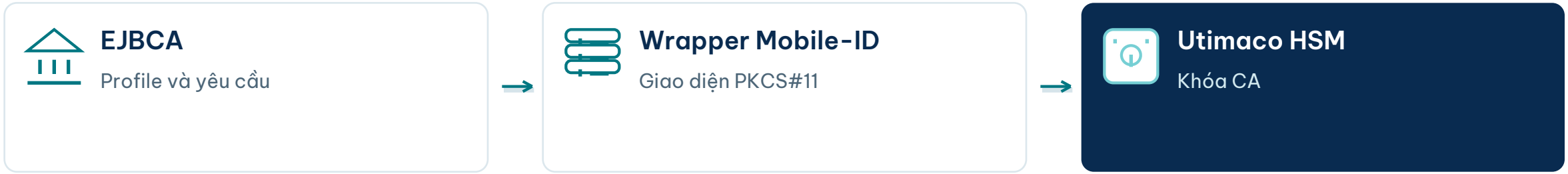
Ứng dụng tạo chữ ký theo profile; bên nhận phải hiểu thuật toán và định dạng.

Chứng thư composite không tự làm cho CMS/CAdES, PDF/Office hoặc mọi bên nhận hỗ trợ PQC.

EJBCA · Chứng thư composite RFC 10073 · Composite ML-DSA Microsoft · .NET 10

EJBCA kết nối HSM qua lớp tích hợp của Mobile-ID.

Wrapper PKCS#11 ánh xạ giao diện, cơ chế mật mã và vòng đời phiên trên cấu hình được chọn.



Chính sách cấp

EJBCA quản lý profile, yêu cầu cấp và trạng thái chứng thư.

Tích hợp mật mã

Wrapper điều phối object, mechanism, session và kết quả/lỗi từ HSM.

Bảo vệ khóa CA

HSM thực hiện phép ký trong miền khóa của tổ chức chứng thực.

Wrapper được Mobile-ID xác nhận đã xây dựng; phạm vi cung cấp gắn với bản build và báo cáo kiểm thử dự án.

EJBCA · Chứng thư composite Utimaco · Quantum Protect Keyfactor · Utimaco

Cấp đúng chứng thư. Cung cấp đúng trạng thái.

Hai dịch vụ phối hợp nhưng có trách nhiệm riêng.



Cấp chứng thư số (CA)

Nhận yêu cầu đã duyệt; cấp, gia hạn và thu hồi theo profile. Đầu ra gồm chứng thư, danh sách thu hồi và nhật ký.



Kiểm tra trạng thái (VA)

Cung cấp dữ liệu trạng thái và hỗ trợ chính sách xác minh. Kiểm thử phản hồi CRL/OCSP trên chuỗi và thuật toán đã chọn.

Bộ xác minh hồ sơ kết hợp trạng thái với chuỗi tin cậy, thời điểm kiểm tra và chính sách bên nhận.

EJBCA · Chứng thư composite RFC 10073 · Composite ML-DSA

Gắn thiết bị với chủ thể và quyền cấp chứng thư.

Quản lý thiết bị (TMS) kết nối đăng ký/phê duyệt (RA) trong một chuỗi có dấu vết.

QUẢN LÝ THIẾT BỊ VÀ ĐĂNG KÝ · MINH HỌA

Chủ thể	Nguyễn Minh An	Đã xác lập
Hồ sơ	HS-PQC-26001	Chờ phê duyệt
Thiết bị	Trusted Key · serial mẫu	Đã liên kết
Chứng thư	Composite · profile dự án	Chờ cấp

01 **Thiết bị**

Nhập kho, cấp phát, kích hoạt, thay thế và kết thúc sử dụng.

02 **Đăng ký**

Xác lập chủ thể, quyền ký, mục đích và phê duyệt yêu cầu.

03 **Truy vết**

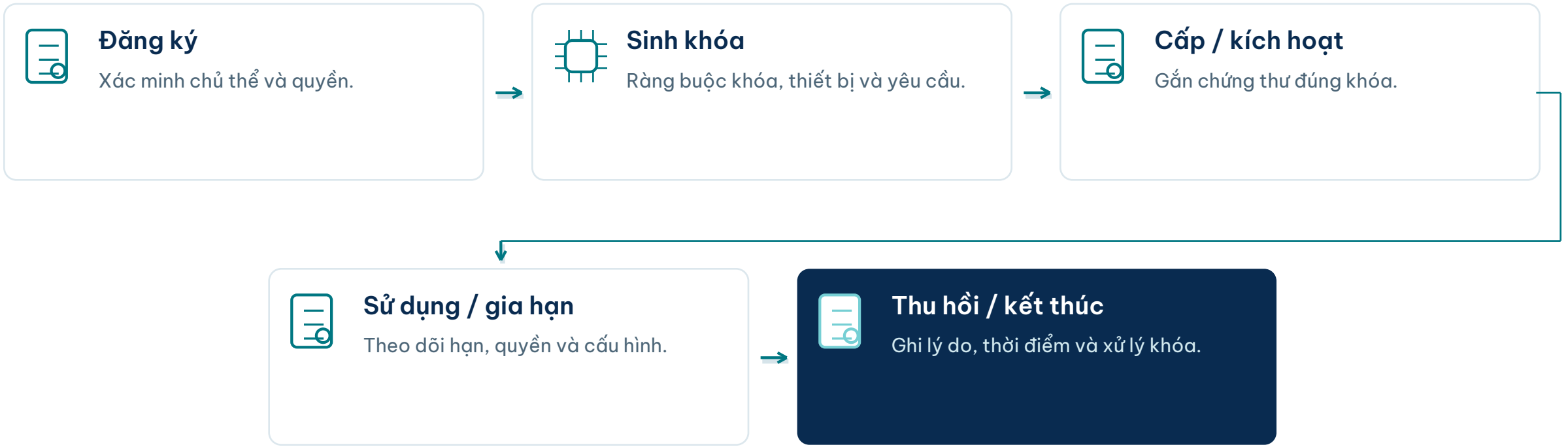
Gắn người nhận, serial, khóa và chứng thư với sự kiện vòng đời.

Giao diện minh họa. Chức năng và tích hợp được chốt theo phạm vi dự án.

Mobile-ID · Hệ sinh thái Mobile-ID · Kiến trúc JavaCard

Mỗi thay đổi có chủ thể, quyền duyệt và bằng chứng.

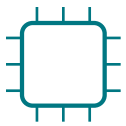
Từ đăng ký ban đầu đến thu hồi hoặc kết thúc sử dụng.



Mất token, đổi quyền hoặc sự cố kích hoạt quy trình khóa quyền, thu hồi và cấp lại theo chính sách.

Sinh khóa trong thiết bị, liên kết chứng thư đúng khóa.

Luồng ưu tiên cho người ký cục bộ; tổ chức phê duyệt theo chính sách đăng ký.



Trusted Key

Applet sinh khóa; phần mềm tạo yêu cầu cấp chứng thư (CSR).



Đăng ký / phê duyệt

Kiểm tra danh tính, quyền và bằng chứng sở hữu khóa.



CA / HSM

EJBCA cấp chứng thư theo profile; HSM bảo vệ khóa CA.



Agent / thiết bị

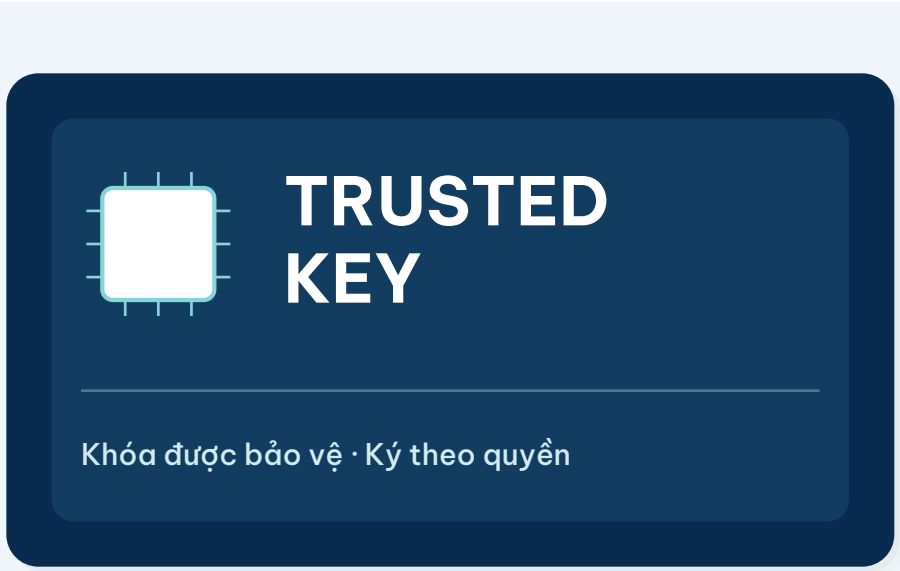
Nhận chứng thư, liên kết đúng khóa và ký thử để kiểm tra.

Nghiệm thu cả yêu cầu sai, gắn sai khóa và yêu cầu lặp; khóa bí mật người ký không nằm trong hồ sơ cấp phát.

EJBCA · Chứng thư composite Mobile-ID · Kiến trúc JavaCard

Trusted Key: bảo vệ khóa, kết nối nghiệp vụ.

Thương hiệu thiết bị thống nhất; đầu đọc, secure element và phần mềm là các lớp cấu thành.



TRUSTED KEY

01 Bảo vệ khóa

Sinh và sử dụng khóa tại nền tảng bảo mật theo cấu hình được xác nhận.

02 Kết nối ứng dụng

Đầu đọc, middleware và PQC Agent đưa yêu cầu ký đến đúng khóa.

03 Quản trị vòng đời

Gắn thiết bị với chủ thể, chứng thư, quyền và sự kiện sử dụng.

Minh họa chức năng Trusted Key; không mô tả kiểu dáng công nghiệp, model hoặc chứng nhận của cấu hình mới.

AB Circle · CIR115B AB Circle · Datasheet Infineon · SLC27

Trusted Key: lớp kết nối tiêu chuẩn với máy tính.

AB Circle CIR115B là thành phần đầu đọc tham chiếu; không phải thương hiệu đại diện của giải pháp.

Trusted Key



Thành phần: AB Circle CIR115B
Ảnh tham chiếu đã xử lý nền

Giao tiếp	ISO/IEC 7816; Class A/B/C; T=0/T=1
Truyền dữ liệu	Extended APDU; CCID; PC/SC
Kết nối	CIR115B-01: USB-A; CIR115B-02: USB-C theo điều kiện hãng
Liên thông	Kiểm tra đồng thời driver, hệ điều hành, thẻ và middleware

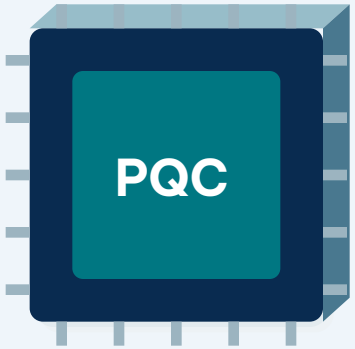
CIR115B-01 USB-A; -02 USB-C theo điều kiện hãng. Xuất xứ Japan chỉ xác nhận bằng CO đúng model/lô.

AB Circle · CIR115B AB Circle · Datasheet

Trusted Key: nền tảng bảo vệ khóa phần cứng.

Thành phần tham chiếu: Infineon SLC27, kết hợp Card OS, applet và giao diện mật mã phù hợp.

Trusted Key



Secure element

Thành phần: Infineon SLC27
Minh họa chức năng, không phải ảnh chip

01 **Nền tảng được công bố**

Infineon nêu thư viện mật mã được chứng nhận Common Criteria.

02 **Tổ hợp cần xác nhận**

Mã chip, Card OS, giao diện mật mã, applet và bộ tham số phải khớp.

03 **Bằng chứng tích hợp**

Sinh khóa, yêu cầu chứng thư, ký mẫu và xác minh chéo trên đúng tổ hợp.

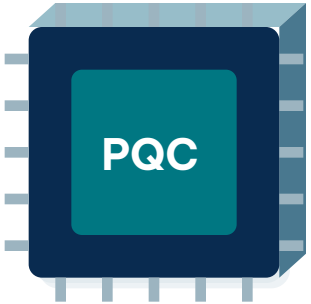
Hình cấu trúc minh họa. Xuất xứ Germany/Taiwan cần chứng từ theo lô; chứng nhận thư viện không tự bao phủ toàn sản phẩm.

Infineon · SLC27 Mobile-ID · Kiến trúc JavaCard

Trusted Key: năm lớp tích hợp, một ranh giới khóa.

Mỗi lớp có giao diện, chính sách và bằng chứng nghiệm thu riêng.

ỨNG DỤNG	Agent · Hồ sơ · Xác minh
MIDDLEWARE	KSP / PKCS#11 · Phiên · Dữ liệu ký
TRUYỀN TẢI	Reader · PC/SC · APDU
APPLET MOBILE-ID	Đối tượng khóa · Quyền · Trạng thái
CARD OS + SILICON	JavaCard / native PQC · SLC27



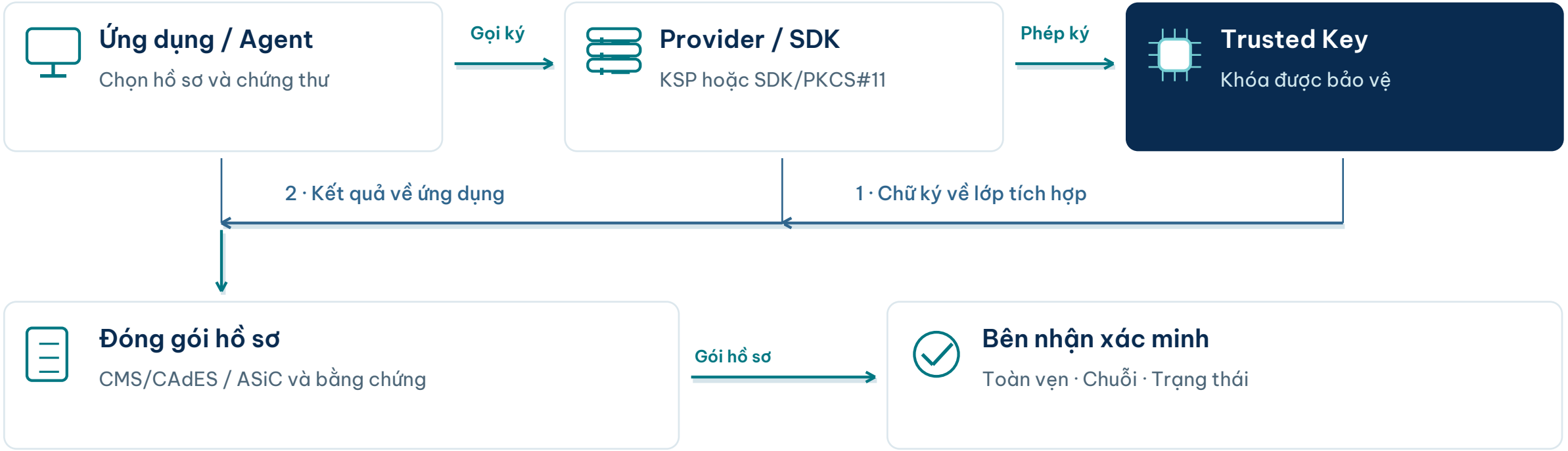
Khóa được bảo vệ tại nền tảng phần cứng.

Năng lực thuật toán phụ thuộc silicon và Card OS; applet gọi dịch vụ được nền tảng cung cấp.

Mobile-ID · Kiến trúc JavaCard Infineon · SLC27

Ứng dụng điều phối. Thiết bị thực hiện phép ký.

PQC Agent kết nối hồ sơ với khóa người dùng trên Trusted Key.



Mẫu luồng tham chiếu; dữ liệu đầu vào phép ký và cơ chế chia khối phải khớp profile đã chọn.

Microsoft · Windows PQC Microsoft · .NET 10 Mobile-ID · Kiến trúc JavaCard

Từ API mật mã đến hồ sơ có thể xác minh.

Windows CNG là nền tảng mật mã; KSP là lớp cung cấp khóa; .NET và SDK xử lý logic ứng dụng.



Chọn tuyến theo cấu hình

Hệ điều hành

Windows 11 24H2/25H2 với bản cập nhật phù hợp; chốt OS build khi triển khai.

Khóa phần cứng

KSP hoặc SDK/PKCS#11 phải tương thích thuật toán, đối tượng khóa và hợp đồng API.

Hồ sơ nghiệp vụ

Mobile-ID bổ sung profile CAdES, đóng gói ASiC và báo cáo xác minh.

API PQC native không tự chứng minh hỗ trợ composite hoặc CAdES đầy đủ; .NET hiện đại khác .NET Framework.

Microsoft · Windows PQC Microsoft · .NET 10 Microsoft · Tích hợp PQC

Một điểm thao tác cho thiết bị, chứng thư và hồ sơ.

Người dùng hiểu rõ nội dung và phạm vi trước khi xác nhận sử dụng khóa.

PQC AGENT · GIAO DIỆN MINH HỌA

Người ký	Nguyễn Minh An · HS-PQC-26001
Thiết bị	Trusted Key · Đã nhận diện
Chứng thư	Composite · Profile dự án
Tài liệu	Đăng ký dịch vụ.pdf

Xem phạm vi ký và xác nhận sử dụng khóa

01 · Chuẩn bị

Thiết bị, chứng thư và hồ sơ.

02 · Xác nhận

Xem tài liệu, chọn phạm vi và nhập PIN.

03 · Hoàn tất

Đóng gói, tự kiểm tra và xuất kết quả.

Giao diện minh họa · Nguyễn Minh An · HS-PQC-26001. Chức năng cung cấp theo bản phát hành và cấu hình được duyệt.

Giữ nguyên tài liệu, bổ sung chuỗi bằng chứng.

ASiC là gói hồ sơ liên kết tài liệu, chữ ký và bằng chứng theo profile được chọn.

Tài liệu gốc	Hợp đồng · Phụ lục · Dữ liệu nghiệp vụ
Liên kết được ký	Manifest / tham chiếu theo profile
Chữ ký và chứng thư	CMS/CAdES detached · Chuỗi tin cậy
Bằng chứng	Timestamp · Trạng thái · Báo cáo

Một bộ hồ sơ. Nhiều lớp kiểm chứng.

Bên nhận kiểm tra tài liệu, chữ ký và dữ liệu tin cậy bằng công cụ phù hợp.

Chọn ASiC-S hoặc ASiC-E theo số đối tượng và quy trình; báo cáo bổ sung cần được ràng buộc nếu yêu cầu bảo vệ toàn vẹn.

Mobile-ID · Hồ sơ ASiC ETSI · ASiC ETSI · CAdES

Ba lớp kỹ thuật phục vụ một kết quả nghiệp vụ.

Tách thông điệp chữ ký, profile bằng chứng và cấu trúc đóng gói.

CMS

Cấu trúc thông điệp chữ ký: thông tin người ký, thuộc tính và giá trị chữ ký.

CAdES

Profile mở rộng cho chữ ký CMS và dữ liệu xác minh theo mức được chọn.

ASiC

Container liên kết tài liệu với chữ ký và bằng chứng liên quan.

Dùng API CMS hoặc container ASiC không tự tạo chứng nhận tuân thủ ETSI hay bảo đảm lưu trữ dài hạn.

ETSI · ASiC ETSI · CAdES Microsoft · Tích hợp PQC

Bên nhận thấy kết quả và biết bước tiếp theo.

Báo cáo gắn kết quả từng lớp với cấu hình, dữ liệu kiểm tra và bước xử lý tiếp theo.

BÁO CÁO XÁC MINH · MINH HỌA

HS-PQC-26001 · Nguyễn Minh An

Profile: theo dự án · Thời điểm kiểm tra: ghi trong báo cáo

Cấu trúc / tài liệu	Đủ dữ liệu kiểm tra
Chữ ký / thuật toán	Đạt theo profile mẫu
Chuỗi / trạng thái	Chưa đủ dữ liệu trạng thái
Hành động tiếp theo	Bổ sung bằng chứng rồi kiểm tra lại

Kết luận có căn cứ. Hành động rõ ràng.

- Hợp lệ
- Không hợp lệ
- Chưa đủ cơ sở kết luận
- Không hỗ trợ cấu hình

Giao diện và dữ liệu minh họa. Kết quả phải kèm thời điểm, cấu hình và dữ liệu đã dùng; thiếu bằng chứng không tự đồng nghĩa chữ ký sai.

Trải nghiệm thống nhất, khóa ký trong miền bảo vệ.

Trusted SIC điều phối trải nghiệm, quyền kích hoạt và tuyến ký theo chính sách nhà cung cấp.



Hướng PQC trên Trusted SIC được công bố là thí điểm có kiểm soát; cung cấp theo bản phát hành và tổ hợp CA/HSM đã xác nhận.

Trusted SIC · Ký từ xa

Passkey gắn người ký với giao dịch được duyệt.

Người dùng xem hồ sơ, phê duyệt giao dịch; dịch vụ kiểm tra quyền trước khi gọi khóa ký.

XÁC NHẬN PHẠM VI KÝ

Nguyễn Minh An

Đăng ký dịch vụ.pdf · 01 tài liệu

Mục đích: đăng ký dịch vụ

Danh tính ký: theo chứng thư đã chọn

Giao dịch: HS-PQC-26001 · Còn 02:00

Xem hồ sơ · Phê duyệt bằng Passkey

Dữ liệu và giao diện minh họa

01 **Xem và xác nhận**

Hiển thị đúng tài liệu, mục đích, danh tính và ngữ cảnh giao dịch.

02 **Cấp quyền kích hoạt**

Xác minh Passkey; ràng buộc quyền với hash, người ký, khóa, giao dịch và thời hạn.

03 **Thực thi ký**

Dịch vụ ký kiểm tra quyền, gọi HSM/QSCD và trả kết quả có dấu vết.

Khóa Passkey khác khóa ký tài liệu. Thuật toán của Passkey không tự trở thành PQC khi chữ ký hồ sơ dùng PQC.

Trusted SIC · Ký từ xa

Bổ sung thời gian tin cậy cho vòng đời hồ sơ.

Dịch vụ dấu thời gian (TSA) ký xác nhận trên dấu vết dữ liệu theo chính sách và nguồn thời gian được quản trị.



TSA hậu lượng tử là hướng thí điểm; thuật toán ký, hash, chứng thư và bên xác minh phải được kiểm thử đồng bộ.

Trusted TSA · Tích hợp QuantumSafe · Dấu thời gian

Mỗi sự kiện chuyển phát có bằng chứng đối chiếu.

Trusted Delivery liên kết danh tính, dấu tổ chức, thời gian và hồ sơ giao nhận.



Tiếp nhận

Ràng buộc người gửi với nội dung và quyền.



Tạo bằng chứng

Liên kết giao dịch, dấu vết nội dung, dấu tổ chức và thời gian.



Chuyển giao

Ghi nhận sự kiện tại miền và ứng dụng nhận.



Bảo quản

Lưu biên nhận, chứng thư, trạng thái và log theo chính sách.

Đến miền nhận, chuyển giao ứng dụng, đã đọc và chấp thuận là các sự kiện khác nhau; PQC mở theo cấu hình dự án.

Trusted Delivery · Bằng chứng

Duy trì khả năng kiểm tra qua nhiều vòng đời thuật toán.

Trusted LTANS và Trusted Records là các điểm tích hợp bảo quản trong hệ sinh thái đề xuất.



Tài liệu, chữ ký, chứng thư, trạng thái và bằng chứng thời gian.

Theo dõi chính sách, độ mới dữ liệu và thay đổi thuật toán.

Tạo lần bảo vệ tiếp theo trước khi điều kiện tin cậy suy giảm.

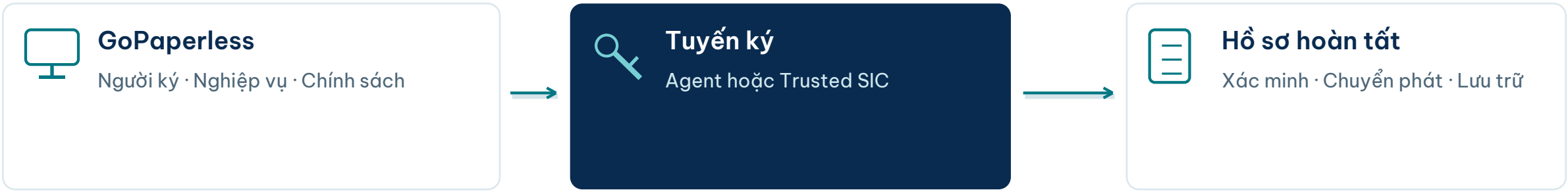
Chuyển giao gói bằng chứng cùng lịch sử xử lý.

Năng lực tích hợp và lịch gia hạn được chốt theo dự án. Bổ sung PQC không tự phục hồi bằng chứng đã mất độ tin cậy.

Mobile-ID · Hệ sinh thái QuantumSafe · Dấu thời gian Mobile-ID · Hồ sơ ASiC

Đưa PQC vào hành trình tài liệu đang vận hành.

Lớp điều phối nghiệp vụ chọn tuyến ký và sử dụng dịch vụ tin cậy dùng chung.



Chọn chính sách

Nghiệp vụ xác định người ký, phạm vi và mức bằng chứng.

Điều phối

Gọi Agent cục bộ hoặc dịch vụ ký từ xa qua giao diện tích hợp.

Hoàn tất hồ sơ

Đóng gói, xác minh, chuyển phát và lưu trữ theo chính sách.

Mô hình tích hợp đề xuất; không mặc định toàn bộ tính năng hiện hữu của GoPaperless đã dùng PQC.

Mobile-ID · Hệ sinh thái Trusted SIC · Ký từ xa

Ưu tiên dịch vụ gần nghiệp vụ, mở rộng theo rủi ro.

Một lớp mật mã dùng chung hỗ trợ nhiều ứng dụng sau khi được kiểm thử.



Danh tính và quyền

CheckID / TrustedID / SSO hỗ trợ đầu vào đăng ký và kích hoạt ký; danh tính không thay thế chữ ký.



Giao dịch và thiết bị

Billing / Pay / ThingID là điểm tích hợp hồ sơ, thông điệp và danh tính thiết bị theo dự án.



Mã phần mềm và kênh truyền

Ký mã/firmware, bảo vệ API và kênh truyền là các luồng chuyển đổi riêng.

QKD và Web3 là hướng nghiên cứu/đối tác theo nhu cầu; không thuộc phạm vi ký số cốt lõi mặc định.

Mobile-ID · Hệ sinh thái QuantumSafe · Danh mục năng lực

Từ tuyến ký đầu tiên đến hạ tầng chuyển đổi mật mã.

Định hướng phát triển đề xuất của Mobile-ID; mỗi mốc mở theo nguồn lực, tiêu chuẩn và nghiệm thu.

CUỐI 2026



Nền móng

Kiểm kê · Profile · Thiết bị · Sandbox

2027



Tuyến lõi

Cấp–ký–xác minh · Windows · Pilot

2028



Liên thông

macOS · Dịch vụ tin cậy · Ứng dụng

2029



Nhân rộng

Theo ngành · Quản trị thay mật mã

macOS 2028 là mục tiêu Mobile-ID. Roadmap không phải cam kết phát hành của Apple hay cam kết hoàn tất PQC toàn hệ sinh thái.

Các phân hệ cùng lộ trình, có cổng mở riêng.

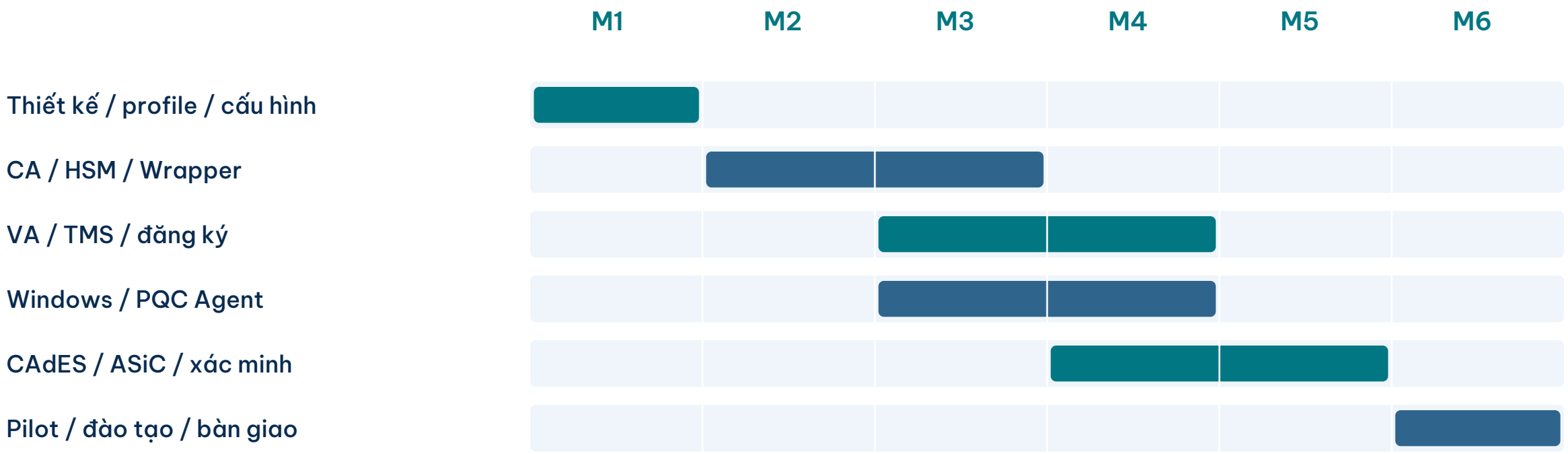
Định hướng Mobile-ID: chữ ký/chứng thư, kênh truyền và bằng chứng có phụ thuộc khác nhau.

	2026	2027	2028	2029
CA / VA / quản trị	Profile / thiết kế	Tuyến lõi / UAT	Liên thông	Nhân rộng
Trusted Key / Agent	Cấu hình thử	Windows / pilot	Ứng dụng mới	Quản trị thay đổi
Ký từ xa / Passkey	Chọn phạm vi	Thí điểm	Mở theo tổ hợp	Mở theo ngành
TSA / Delivery / LTANS	Policy / mẫu	TSA thí điểm	Delivery / lưu giữ	Gia hạn / vận hành
GoPaperless / PDF / Office	Chọn nghiệp vụ	ASiC / CAdES	Adapter có điều kiện	Mở theo tương thích
macOS / kênh truyền	Kiểm kê / khảo sát	Thiết kế tuyến	macOS mục tiêu	Mở theo nghiệm thu

Mốc là mục tiêu theo dự án. PDF/Office, macOS và dịch vụ mới chỉ mở sau kiểm thử tương thích; xem phụ lục phụ thuộc.

Một phạm vi pilot, nhiều phân hệ cùng tiến độ.

Kế hoạch mục tiêu bắt đầu sau khi thống nhất đầu vào, thiết bị và quyền sử dụng.



M2: tích hợp CA/HSM sơ bộ · M3: hoàn tất lõi CA/HSM · M4–M5: kiểm thử liên thông · M6: nghiệm thu pilot

Sáu mốc thống nhất giữa thiết kế, tích hợp và vận hành.

Kết quả sơ bộ và kết quả nghiệm thu được nhận diện riêng.

Mốc	Đầu ra	Điều kiện chuyển bước
M1 / Thiết kế	Kiến trúc, cấu hình, profile, phân công	Hai bên duyệt phạm vi và kế hoạch
M2 / Tích hợp sơ bộ	CA/HSM/Wrapper cấp chứng thư mẫu	Chạy mẫu và ghi nhận khoảng trống
M3 / Lõi tin cậy	Hoàn tất CA/HSM; tích hợp VA và TMS/RA	Chuỗi, thu hồi, quyền và vòng đời đúng
M4 / Tuyến Windows	Agent, thiết bị và enrollment được kiểm thử	Dữ liệu ký và phiên thiết bị ổn định
M5 / Hồ sơ toàn trình	CAdES/ASiC, xác minh, lỗi và phục hồi	Liên thông đúng trên bộ thử được duyệt
M6 / Pilot / bàn giao	UAT, đào tạo, runbook, vận hành thử	Chủ trì phê duyệt theo phạm vi

Lịch thương mại được chốt sau khảo sát; dịch vụ mở rộng và macOS có cổng riêng.

Chọn nơi vận hành theo quyền kiểm soát và dữ liệu.

Kiến trúc có thể tổ chức theo môi trường của từng đơn vị.



Tại hạ tầng tổ chức

Tổ chức quản lý CA/HSM, dữ liệu và miền vận hành theo phân quyền.



Đám mây riêng

Phân vùng mạng, khóa, tenant và dịch vụ; thống nhất ranh giới trách nhiệm.



Môi trường cô lập

Phân phối trust anchor, danh sách thu hồi và gói cập nhật theo chính sách.

Chốt dữ liệu đi ra ngoài, dịch vụ online và cách xử lý khi thiếu kết nối trước khi thiết kế chi tiết.

Quản lý cấu hình cùng bằng chứng và khả năng phục hồi.

Đưa chuyển đổi mật mã vào quy trình vận hành thường xuyên.

Kiểm kê

Theo dõi thiết bị, applet, khóa, chứng thư, provider và profile của từng tuyến.

Giám sát

Hết hạn, thu hồi, lỗi ký và support bundle không chứa bí mật.

Thay đổi

Gói cập nhật được ký số, kiểm thử hồi quy và rollback có chính sách.

Phục hồi

Sao lưu khóa CA theo chính sách, khôi phục cấu hình và diễn tập sự cố.

Chốt mức dịch vụ, mục tiêu khôi phục và quyền quản trị trong hợp đồng; không mặc định sao lưu/xuất khóa người dùng từ token.

Nghiệm thu cả kết quả đúng và tình huống sai.

Mỗi ca thử có cấu hình, dữ liệu, kết quả kỳ vọng và người phê duyệt.

Nhóm kiểm thử	Tình huống	Bằng chứng
Đăng ký / cấp chứng thư	Đúng/sai CSR, sở hữu khóa, gắn sai thiết bị	Yêu cầu, chứng thư và trace
Composite / hồ sơ	Sai thành phần, sai OID, đổi/xóa tài liệu	Mẫu lỗi và báo cáo từng lớp
Chứng thư / thời gian	Hết hạn, thu hồi, thiếu trạng thái, chain không tin	Chính sách và dữ liệu đã dùng
Thiết bị / phục hồi	Sai PIN, rút token, timeout, cập nhật/rollback	Log đã lọc và biên bản
Remote / Passkey nếu chọn	Replay, sai giao dịch, quyền hết hạn	Kết quả kiểm tra và dấu vết

Kết quả benchmark được công bố theo cấu hình và phương pháp đo; không đưa chỉ tiêu chưa đo thành cam kết.

Một tuyến tham chiếu, ba cách tạo giá trị.

Chọn phạm vi nhỏ có khả năng chứng minh trước khi nhân rộng.



Tổ chức chứng thực

Một issuing CA, tập profile, model token và tuyến ký. Đầu ra: vòng đời, hồ sơ và khả năng liên thông.



Khối cơ yếu / quản lý

Miền tin cậy, chính sách và kiến trúc kiểm soát khóa. Đầu ra: hồ sơ để xem xét đánh giá theo yêu cầu.



Doanh nghiệp / cơ quan

Một bộ hồ sơ nghiệp vụ tích hợp vào quy trình hiện hữu. Đầu ra: thao tác ký và khả năng tra soát rõ.

Chủ nghiệp vụ quyết định điều kiện chấp nhận và lưu giữ; tài liệu không xác lập phê duyệt của cơ quan nhà nước.

Đầu tư theo phạm vi, duy trì theo mức sử dụng.

Báo giá sau khi chốt cấu hình, quy mô và mô hình vận hành.

Nhóm	Cấu phần	Đơn vị xác định quy mô
Hạ tầng	CA/license, HSM, dự phòng, môi trường	CA, site, phân vùng và tải
Thiết bị	Trusted Key, reader, dự phòng và cấp phát	Người dùng / thiết bị
Phần mềm	Wrapper, provider, Agent, SDK và verifier	Môi trường / ứng dụng / quyền dùng
Triển khai / đào tạo	Khảo sát, tích hợp, kiểm thử và chuyển giao	Phạm vi và đầu ra nghiệm thu
Duy trì	Hỗ trợ, cập nhật, vận hành và bằng chứng	Mức dịch vụ, thời hạn, dung lượng

Không áp dụng đơn giá hoặc chỉ tiêu sản lượng mặc định trong proposal này.

Chọn phạm vi hợp tác theo đầu ra cần đạt.

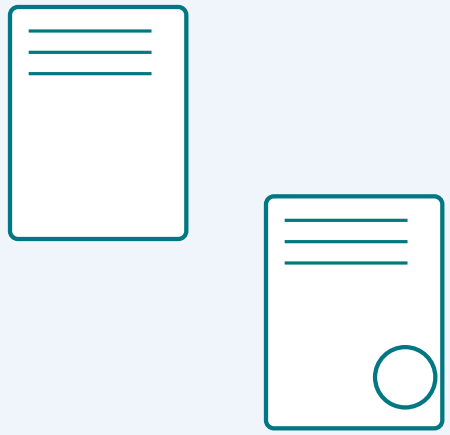
Ba mức tiếp cận; thời gian, quyền sử dụng và hỗ trợ được chốt trong hợp đồng.

Mức hợp tác	Phạm vi và đầu ra	Điều kiện / chưa bao gồm
Đánh giá / trải nghiệm	Chọn nghiệp vụ; demo; phương án và phạm vi pilot	Dữ liệu thử, cấu hình và lịch được thống nhất
Pilot khoảng sáu tháng	Tuyến cấp–ký–xác minh; quản trị; bộ bằng chứng UAT	License, thiết bị và nhân sự; chưa mở mọi dịch vụ
Triển khai / mở rộng	Môi trường vận hành; đào tạo; dịch vụ mở rộng theo phạm vi	SLA, quy mô và quyền mã nguồn thỏa thuận riêng

Không có đơn giá mặc định. Hạ tầng, bản quyền bên thứ ba và đánh giá độc lập chỉ bao gồm khi hợp đồng quy định.

Bàn giao năng lực có thể tiếp nhận và vận hành.

Phần mềm, cấu hình, tài liệu và bằng chứng được tổ chức thành một bộ thống nhất.



Thiết kế + Phần mềm + Bằng chứng vận hành

01

Thiết kế

Kiến trúc, profile, signing contract, phân quyền và ma trận cấu hình.

02

Phần mềm và mẫu

Bộ cài, SDK/API, Wrapper và mẫu CSR/chứng thư/hồ sơ theo quyền được cấp.

03

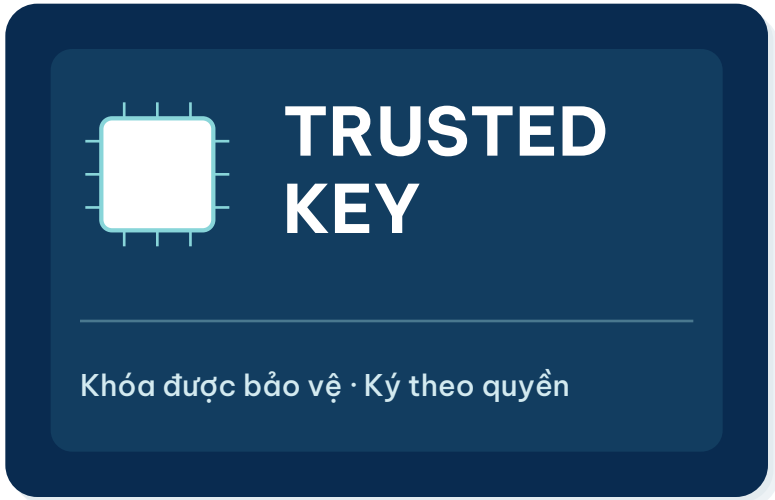
Vận hành

Kiểm thử, phương pháp đo, hướng dẫn sự cố, đào tạo và chính sách hỗ trợ.

Quyền sở hữu, quyền sử dụng, mã nguồn và tài nguyên bên thứ ba được thỏa thuận riêng.

Trải nghiệm Trusted Key trên một hồ sơ xuyên suốt.

Theo xác nhận Mobile-ID: có sandbox, thiết bị và đội kỹ thuật hỗ trợ; lịch và cấu hình cần thống nhất.



Minh họa chức năng Trusted Key

01

Nguồn lực

Sandbox, thiết bị và đội kỹ thuật theo xác nhận Mobile-ID.

02

Cần cấu hình trước

Nghiệp vụ, profile, thiết bị, bộ dữ liệu và lịch demo.

03

Trải nghiệm / đầu ra

Cấp–ký–xác minh; mẫu chứng thư, hồ sơ và báo cáo theo phạm vi.

Phạm vi, cấu hình và kết quả được ghi trong biên bản demo/pilot. Giao diện minh họa không thay bằng chứng nghiệm thu.

Trao đổi kiến trúc. Trải nghiệm Trusted Key.

Xác định nghiệp vụ ưu tiên và kế hoạch chuyển đổi PQC phù hợp tổ chức.

Trao đổi kiến trúc.
Trải nghiệm sandbox.
Chuyển đổi có kiểm chứng.

Tổ chức · Nghiệp vụ · Quy mô · Môi trường
Bốn đầu vào cho buổi làm việc đầu tiên.

Website
www.mobile-id.vn

Giải pháp
quantumsafe.mobile-id.vn

Email
info@mobile-id.vn

Điện thoại
1900 6884 · +84 28 3622 2982

Kết nối đội Mobile-ID
Trusted Key · QuantumSafe Ecosystem

Chốt tổ hợp mật mã, định dạng và chính sách kiểm tra.

Profile là cấu hình được quản lý; không mở mọi thuật toán cùng lúc.

Thành phần	Quyết định cần chốt	Đầu ra
Thuật toán	Tổ hợp ML-DSA và thuật toán truyền thống	Danh mục, tham số và bằng chứng an toàn
Định dạng	Định danh thuật toán (OID), public key, encoding	Mẫu DER/PEM và bộ thử
Chứng thư	Key Usage, EKU, thời hạn và policy identifier	Profile chứng thư và chủ thể
Phép ký	Message/prehash/context/signed attributes	Hợp đồng dữ liệu ký
Xác minh	Đúng cấu trúc, thành phần và trust policy	Báo cáo liên thông, sai cấu hình bị từ chối

RFC 10073 là Proposed Standard về Composite ML-DSA cho X.509 PKI; mỗi ứng dụng vẫn cần kiểm tra triển khai.

EJBCA · Chứng thư composite RFC 10073 · Composite ML-DSA Microsoft · .NET 10

Mỗi lớp phải hiểu đúng đối tượng được ký.

Áp dụng cho KSP, PKCS#11, applet và bộ tạo CMS/CAdES.

Câu hỏi	Quyết định cần kiểm tra
Ký gì?	Tài liệu, manifest hoặc DER signed attributes theo profile
API nhận gì?	Message, prehash hoặc giá trị chuyên biệt được hỗ trợ
Lớp nào xử lý?	Băm, context, domain separation và kết hợp chữ ký
Mã hóa thế nào?	OID, AlgorithmIdentifier, encoding, thứ tự thành phần
Chứng minh đúng?	Test vectors, kiểm tra chéo và từ chối profile không khớp

Loại bỏ băm hai lần, sai context, sai draft và xác minh thiếu thành phần composite.

RFC 10073 · Composite ML-DSA Microsoft · .NET 10 Microsoft · Tích hợp PQC

Truyền dữ liệu lớn với trạng thái phiên rõ ràng.

APDU là đơn vị lệnh/phản hồi giữa máy tính và thẻ; giới hạn theo tổ hợp thực tế.

Khối 01 → Khối 02 → Khối 03 → Khối 04 → Khối 05

Applet / Card OS

Chia / ráp khối

Chốt kích thước, thứ tự, độ dài; phát hiện thiếu hoặc lặp dữ liệu.

Phiên / phục hồi

Rút thẻ, timeout và hủy ký kết thúc về trạng thái xác định.

Bộ nhớ / tốc độ

Đo buffer, đối tượng bền vững/tạm thời, số lượt trao đổi và thời gian.

Kiểm thử dữ liệu biên, lỗi giữa phiên, reader và tải lặp trên đúng cấu hình; không tái sử dụng phiên lỗi.

Mobile-ID · Kiến trúc JavaCard

Card OS, applet và middleware có nhiệm vụ riêng.

Năng lực native được nền tảng cung cấp; ứng dụng sử dụng qua lớp tích hợp.

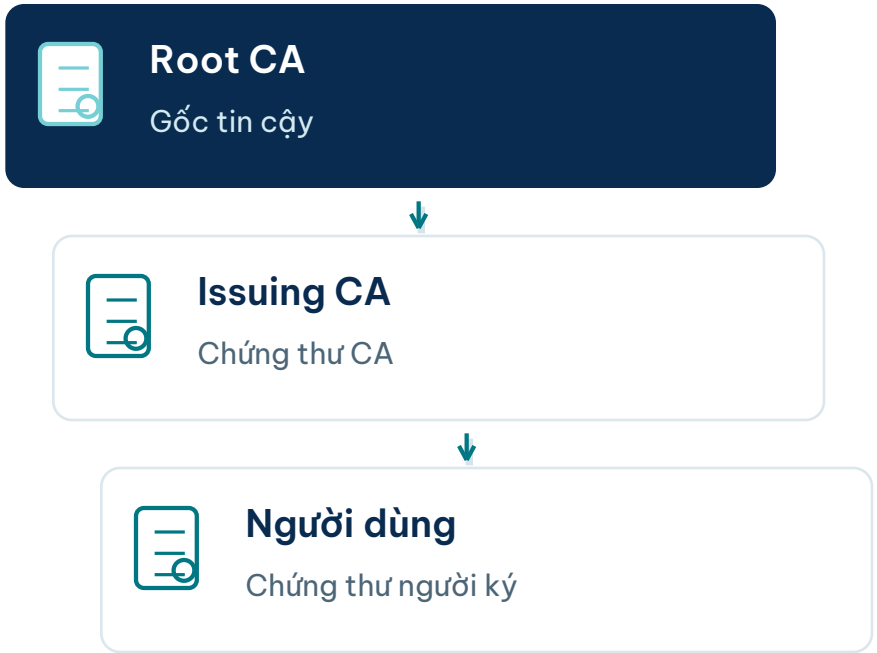
Card OS / silicon	Applet Mobile-ID	Middleware
Mật mã và nguồn ngẫu nhiên	Định danh khóa, thuật toán và quyền	Ánh xạ KSP / PKCS#11
Lưu khóa và đối tượng	PIN, phiên và lệnh nghiệp vụ	Phiên người dùng, retry và thông báo
Giới hạn bộ nhớ/API	Quản lý khe khóa, gọi dịch vụ OS	Chia khối, truyền và ráp APDU
Tự kiểm tra / bảo vệ nền	Mã lỗi và trạng thái kết thúc	Log hỗ trợ không chứa bí mật

Applet không tự bổ sung thuật toán native khi Card OS thiếu giao diện cần thiết.

Mobile-ID · Kiến trúc JavaCard

Đánh giá cả chuỗi, không chỉ chứng thư người ký.

Chính sách gốc tin cậy quyết định cách bên nhận chấp nhận hồ sơ.



01 **Root / Issuing CA**

Chọn hierarchy, thuật toán, thời hạn và vùng thử/vận hành.

02 **Trạng thái**

Kiểm tra CRL/OCSP, chữ ký phản hồi và độ mới dữ liệu.

03 **Bên nhận**

Phân phối trust anchor; xác định private trust và phạm vi sử dụng.

Xác minh được trên một môi trường không tự tạo public trust hoặc sự chấp nhận cho mọi nghiệp vụ.

EJBCA · Chứng thư composite RFC 10073 · Composite ML-DSA

Công bố hỗ trợ theo tổ hợp đã được kiểm thử.

.NET 10: API chữ ký PQC experimental; composite tại GA dựa draft 8, cần kiểm tra với RFC 10073.

Tuyến	Điều kiện cần chốt	Cổng công bố
Windows / .NET	OS build, KB, provider, package, profile	Ký–xác minh và lỗi trên tổ hợp
CMS/CAdES / ASiC	OID, encoding, container và policy	Bộ mẫu đúng/sai, verifier độc lập
Adobe PDF	Adapter, signature profile, version và bên nhận	Báo cáo tương thích trước công bố
Microsoft Office	Ứng dụng, định dạng và bộ xác minh	Báo cáo tương thích trước công bố
macOS	CryptoTokenKit/SDK, cài đặt và ứng dụng	Roadmap 2028; cổng phát hành riêng

Adobe/Office là hướng chuẩn bị mở rộng; không hạ cấp ngầm sang chữ ký truyền thống khi PQC chưa hỗ trợ.

Microsoft · Windows PQC Microsoft · .NET 10 Apple · CryptoTokenKit

Ghi đúng model, bản build và lô hàng.

Thông tin thương hiệu, nơi chế tạo wafer, đóng gói và xuất xứ hàng hóa được phân biệt.

Cấu phần	Hồ sơ cần chốt	Điều kiện
Đầu đọc trong Trusted Key	AB Circle CIR115B-01/02, revision, serial, CO	Japan: cần chứng từ đúng model/lô
Secure element trong Trusted Key	Infineon SLC27; mã linh kiện, lot, CO/COQ	Germany/Taiwan: cần chứng từ
Card OS / applet	Nhà cung cấp, API, version, checksum	Đúng tổ hợp đã xác nhận
Backend / máy người dùng	EJBCA, HSM, Wrapper, OS, .NET, KSP	Manifest cấu hình và kiểm thử liên thông

Các chứng từ xuất xứ và cấu hình được xác nhận trong hồ sơ mua sắm/triển khai; không suy từ trụ sở nhà cung cấp.

AB Circle · CIR115B AB Circle · Datasheet Infineon · SLC27

Đo trên cấu hình thật, báo cáo có thể tái lập.

Thời gian nhập PIN và xử lý kỹ thuật được tách khi cần đánh giá.

Chỉ tiêu	Phương pháp	Cách báo cáo
Sinh khóa / cấp chứng thư	Tách thời gian token, CSR, RA và CA	Trung vị/P95; số lần và cấu hình
Ký toàn trình	Theo kích thước file, profile và tuyến ký	Độ trễ; loại trừ/thể hiện thời gian người dùng
Xác minh	Cold/warm cache; trạng thái online và chuỗi	Độ trễ, tỷ lệ lỗi và dữ liệu
Dung lượng	Public key, chứng thư, chữ ký và ASiC	Byte, chi phí truyền/lưu trữ
Tải / ổn định	Đồng thời, lặp, timeout và phục hồi	Thông lượng, bão hòa và lỗi

Ghi reader, chip/OS, applet, CPU, Windows, .NET, provider, mạng và bộ dữ liệu; không có benchmark thương mại mặc định.

Rõ chủ trì, rõ quyền duyệt và trách nhiệm hỗ trợ.

Phân công đề xuất được chốt trong phạm vi dự án.

Hạng mục	Tổ chức / CA	Mobile-ID	Hãng / đánh giá
Chính sách / trust	Chủ trì và phê duyệt	Tư vấn kiến trúc	Tham vấn theo scope
CA/HSM/Wrapper	Quản trị và phối hợp	Tích hợp theo hợp đồng	Hỗ trợ nền tảng
Thiết bị / middleware	Cấp phát, quản trị người dùng	Cung cấp và tích hợp	Chip/Card OS theo cấu hình
Ứng dụng / hồ sơ	Chủ nghiệp vụ và dữ liệu	Agent, SDK, verifier	Đối tác ứng dụng
Nghiệm thu / vận hành	Phê duyệt và vận hành	Thực hiện, sửa lỗi, đào tạo	Độc lập nếu yêu cầu

ISO/IEC 27001:2022 cho hệ thống quản lý an toàn.

SIS3512241008 · Mobile-ID Technologies And Services Joint Stock Company.


CERTIFICATE OF REGISTRATION

IAS ACCREDITED Management Systems Certification Body MSCB-131

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 certificate 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

01 **Phạm vi**

Hệ thống quản lý an toàn thông tin theo nội dung in trên chứng chỉ.

02 **Thời hạn in**

Cấp 05/12/2024; hết hạn 04/12/2027.

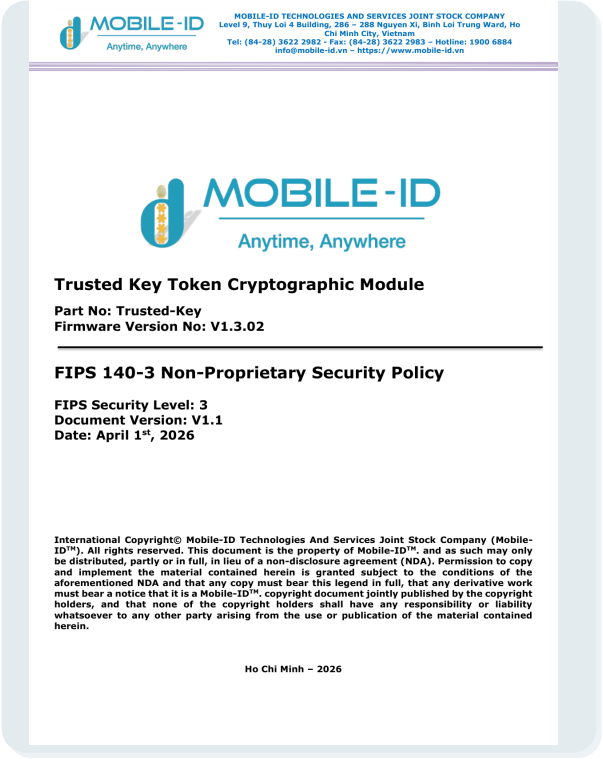
03 **Điều kiện sử dụng**

Đối chiếu tình trạng duy trì với tổ chức cấp khi dùng cho quyết định. Đây không phải chứng nhận thuật toán PQC.

ISO · Hồ sơ Mobile-ID

Trusted Key Token: FIPS 140-3 Level 3.

Hồ sơ NIST CMVP số 5331 và Security Policy xác định ranh giới được thẩm định.



MOBILE-ID Anytime, Anywhere

MOBILE-ID TECHNOLOGIES AND SERVICES JOINT STOCK COMPANY
Level 9, Thuy Loi 4 Building, 286 – 288 Nguyen Xi, Binh Loi Trung Ward, Ho Chi Minh City, Vietnam
Tel: (84-28) 3622 2982 - Fax: (84-28) 3622 2983 – Hotline: 1900 6884
info@mobile-id.vn – https://www.mobile-id.vn

MOBILE-ID Anytime, Anywhere

Trusted Key Token Cryptographic Module

Part No: Trusted-Key
Firmware Version No: V1.3.02

FIPS 140-3 Non-Proprietary Security Policy

FIPS Security Level: 3
Document Version: V1.1
Date: April 1st, 2026

International Copyright© Mobile-ID Technologies And Services Joint Stock Company (Mobile-ID™). All rights reserved. This document is the property of Mobile-ID™, and as such may only be distributed, partly or in full, in lieu of a non-disclosure agreement (NDA). Permission to copy and implement the material contained herein is granted subject to the conditions of the aforementioned NDA and that any copy must bear this legend in full, that any derivative work must bear a notice that it is a Mobile-ID™ copyright document jointly published by the copyright holders, and that none of the copyright holders shall have any responsibility or liability whatsoever to any other party arising from the use or publication of the material contained herein.

Ho Chi Minh – 2026

01 Module

Trusted Key Token Cryptographic Module; Overall Level 3.

02 Cấu hình

Part No. Trusted-Key; firmware V1.3.02 theo Security Policy V1.1.

03 Giới hạn

Không tự áp dụng #5331 cho SLC27, ML-DSA hoặc composite mới. Hình là trang đầu Security Policy, không phải ảnh chứng chỉ NIST.

NIST · Hồ sơ 5331 NIST · Security Policy

Thiết bị ký máy chủ: hồ sơ QSCD và mức đánh giá.

Theo hồ sơ Mobile-ID công bố: TAYLLORCOX PCEB 26/04/09; đối tượng và cấu hình phải được đối chiếu.


Certificate No.: PCEB 26/04/09

tayllorcox.com
ensure your certification

Certificate

Certification body TAYLLORCOX PCEB established by TAYLLORCOX s.r.o. auditing, inspection and testing institute hereby awards this certificate to the company

Mobile-ID Technologies And Services Joint Stock Company

ID No.: 0313994173
1/11/74 Dang Thuy Tram Street, Binh Loi Trung Ward, Ho Chi Minh City, Viet Nam

to confirm that its qualified electronic signature creation device

Trusted Hub Service Provider Appliance QSCD

is in accordance with:

eIDAS Common Criteria Standards EAL 4+ augmented (AVA_VAN.5, ALC_FLR.3) by EN 419221-5:2018, EN 419241-2:2019 and ISO/IEC 15408 (Common Criteria) Version 3.1 Revision 5

This certificate is issued in accordance with certification scheme requirements defined by standards EN 419221-5:2018 (following Cryptographic Module: CryptoServer CP5 Se52 PCIe, CryptoServer CP5 Se500 PCIe, CryptoServer CP5 Se1500 PCIe), EN 419241-2:2019 and ISO/IEC 15408 (Common Criteria) Version 3.1 Revision 5. Security target version 1.2.260313.

Date of the certification: 2026-04-09
This certificate is valid until: 2028-04-08

Radek Nedvěd
Head of Certification Body
Place and date of issue of the certificate: Prague, 2026-04-09

The certificate was issued by TAYLLORCOX s.r.o., TAYLLORCOX PCEB
Na Florenci 1859/35, Nové Město - Praha 1, CZ 110 00, audit@tayllorcox.com, www.tayllorcox.cz
To check this certificate validity please call the phone number: +420 222 563 101
Member of: TAYLLORCOX UK Ltd. 75 King William St., EC4N, London, United Kingdom, audit@tayllorcox.com

01 Mức đánh giá

EAL4+ augmented AVA_VAN.5 và ALC_FLR.3; Security Target 1.2.260313.

02 Cấu hình / thời hạn in

CryptoServer CP5 Se52/Se500/Se1500 PCIe; 09/04/2026–08/04/2028.

03 Điều kiện sử dụng

Đối chiếu duy trì với tổ chức cấp; không suy rộng sang cấu hình PQC mới hoặc tư cách EU QTSP.

SAM/QSCD · Hồ sơ Mobile-ID

macOS 2028: dùng chung lõi, phát triển lớp tích hợp.

Mục tiêu phát triển Mobile-ID theo khả năng API và ứng dụng đích.

2028

macOS

Mục tiêu phát triển
theo cổng nghiệm thu

01 **Lõi dùng chung**

Profile, vòng đời, applet, định dạng hồ sơ và bộ xác minh.

02 **Tích hợp macOS**

Khảo sát CryptoTokenKit, Keychain, PKCS#11/SDK và khả năng thuật toán.

03 **Cổng phát hành**

Bộ cài signed/notarized, enrollment, ký–xác minh và ma trận phiên bản.

Không phải cam kết hỗ trợ PQC của Apple; nếu API native chưa phù hợp, đánh giá tuyến SDK được kiểm thử riêng.

Apple · CryptoTokenKit

Chức năng đi cùng nơi chạy và quyền vận hành.

Danh mục tham chiếu được chốt trong thiết kế và hợp đồng.

Phân hệ	Nơi chạy / chủ quản	Giao diện / đầu ra	Nghiệm thu
CA / RA / VA	Backend PKI / tổ chức chứng thực	Enrollment, cert, CRL/OCSP, audit	Profile, quyền và vòng đời
HSM / Wrapper	Vùng mật mã / CA và Mobile-ID	PKCS#11; yêu cầu / chữ ký/lỗi	Vectors, session, HA/DR
TMS / quản trị	Backend tổ chức / chủ tài sản	Agent/API; cấp phát, định danh, quyền	Mất/thay thiết bị, trace
TSA / bảo quản	Dịch vụ chọn / đơn vị vận hành	Timestamp, gói bằng chứng, lưu giữ	Trust, thời gian và phục hồi

Các phân hệ được cung cấp theo cấu hình và phạm vi; tích hợp TSA/bảo quản có cổng riêng.

Giao diện, dữ liệu và bằng chứng có ranh giới rõ.

Các phân hệ dùng chung chính sách nhưng có tiêu chí chấp nhận riêng.

Phân hệ	Nơi chạy / chủ quản	Vào / ra	Nghiệm thu
Trusted Key	Thiết bị / người dùng và tổ chức	APDU, PIN / public key/chữ ký	KeyGen/Sign, PIN, buffer, phiên
PQC Agent	Windows / đơn vị sử dụng	Hồ sơ, cert / yêu cầu ký/gói kết quả	Cài, cập nhật, lỗi và rollback
Định dạng / verifier	Ứng dụng/backend / chủ nghiệp vụ	Tài liệu, cert / ASiC/CAdES/báo cáo	Toàn vẹn, chain, trạng thái, thiếu dữ liệu
Giám sát / audit	Control plane / tổ chức	Sự kiện / log/cảnh báo/báo cáo	Quyền, thời gian, lưu giữ; không bí mật

Hiện hữu, tích hợp và roadmap được công bố riêng.

Danh mục sản phẩm là cơ sở định hướng; năng lực PQC được nghiệm thu theo từng module.

Nhóm sản phẩm	Vai trò mở rộng PQC	Trạng thái đề xuất
GoPaperless / Sign / Trusted Hub	Điều phối ký và chính sách hồ sơ	Tích hợp dự án; Trusted SIC PQC thí điểm
Trusted TSA / LTANS / Records	Thời gian, gia hạn và lưu bằng chứng	TSA PQC thí điểm; bảo quản theo scope
Trusted Delivery	Dấu tổ chức, biên nhận và bằng chứng	Mở rộng theo cấu hình và hồ sơ dịch vụ
CheckID / TrustedID / FIDO2	Danh tính, xác thực và quyền kích hoạt	Tích hợp đầu vào; không mặc định PQC
Billing / Pay / ThingID	Thông điệp, chứng từ, danh tính thiết bị	Hướng mở rộng theo nghiệp vụ

Không dùng dữ liệu demo, giấy phép mẫu hoặc tên đối tác minh họa trên website như bằng chứng production.

Mobile-ID · Hệ sinh thái QuantumSafe · Danh mục năng lực Trusted SIC · Ký từ xa

Mở từng mốc khi điều kiện kỹ thuật và vận hành đủ.

Định hướng phải chuyển thành phạm vi, chủ trì và bằng chứng cụ thể.

Mốc	Chủ trì đề xuất	Phụ thuộc / cổng
Cuối 2026 / nền móng	Mobile-ID + kiến trúc tổ chức	Inventory, BOM, profile; mẫu chạy tham chiếu
2027 / tuyến lõi và pilot	CA + Mobile-ID + chủ ứng dụng	License, thiết bị, build; UAT theo cấu hình
2028 / liên thông mở rộng	Mobile-ID + đơn vị dịch vụ + đối tác	API/ứng dụng, trust, bằng chứng; cổng riêng
2029 / nhân rộng quản trị	Chủ chương trình + vận hành	Tải, hỗ trợ, thay thuật toán, báo cáo và DR

Chữ ký/chứng thư, kênh truyền và bằng chứng có thể tiến khác nhau; không ấn định ngày dừng thuật toán cũ khi chưa phê duyệt.

Tiêu chuẩn định hướng thiết kế và cách kiểm tra.

Phân biệt đặc tả, kiểm thử phù hợp, thẩm định module và chấp nhận nghiệp vụ.

Tham chiếu	Phạm vi	Điều kiện áp dụng
RFC 10073	Composite ML-DSA cho X.509 PKI	Chốt OID, encoding và triển khai
NIST FIPS 203 / 204 / 205	ML-KEM / ML-DSA / SLH-DSA	Phân biệt thiết lập khóa và chữ ký
ETSI EN 319 122-1	Cấu trúc/profile CAdES	Chọn bản và mức profile
ETSI EN 319 162-1	Container ASiC	Liên kết, cấu trúc và xác minh
RFC 3161 / hồ sơ TSA	Giao thức dấu thời gian	Cấu hình dịch vụ, policy và trust

Việc chấp nhận cho hệ thống chuyên dùng hoặc nghiệp vụ được xem xét riêng; proposal không xác lập phê duyệt.

RFC 10073 · Composite ML-DSA ETSI · ASiC ETSI · CAdES

Đọc thuật ngữ qua vai trò trong hệ thống.

Tên viết tắt chỉ dùng khi giúp trao đổi chính xác.

Thuật ngữ	Ý nghĩa sử dụng
PQC / PKI	Mật mã hậu lượng tử / hạ tầng khóa công khai
CA / RA / VA / TMS	Cấp chứng thư / đăng ký và phê duyệt / trạng thái / quản lý thiết bị
HSM / QSCD / SAM	Bảo vệ khóa phần cứng / thiết bị tạo chữ ký đủ điều kiện / module kích hoạt chữ ký theo hồ sơ áp dụng
CMS / CAdES / ASiC	Thông điệp chữ ký / profile CMS mở rộng / container hồ sơ
Provider / SDK / API	Lớp cung cấp mật mã / bộ công cụ phát triển / giao diện lập trình
Crypto-agility	Khả năng thay đổi mật mã theo chính sách, kiểm thử và quản lý cấu hình

Nền tảng, chuẩn composite và Windows.

Chọn tên tài liệu để mở nguồn chính thức; phạm vi hỗ trợ được ghi dưới từng mục.

EJBCA · Chứng thư composite

Cấu hình CA, profile và cấp chứng thư composite

RFC 10073 · Composite ML-DSA

Đặc tả composite; không tự chứng minh tương thích sản phẩm

Microsoft · Windows PQC

API ML-DSA / ML-KEM qua CNG và .NET

Microsoft · .NET 10

API và giới hạn phiên bản; cần đối chiếu RFC 10073

Microsoft · Tích hợp PQC

Điểm tích hợp chứng thư, CNG và CMS; không mặc định đủ CAdES

NIST · Hồ sơ 5331

Trusted Key Token Cryptographic Module trong phạm vi công bố

Hồ sơ ký, bảo đảm và thiết bị.

Chọn tên tài liệu để mở nguồn chính thức; phạm vi hỗ trợ được ghi dưới từng mục.

Mobile-ID · Hồ sơ ASiC

Kiến trúc ASiC-CAdES và quản trị hồ sơ; không phải kết quả UAT

Mobile-ID · Kiến trúc JavaCard

Ranh giới Card OS, applet, APDU và middleware

ETSI · ASiC

Building blocks và baseline container ASiC

ETSI · CAdES

Building blocks và baseline CAdES

AB Circle · CIR115B

Giao tiếp, APDU, model USB-A/USB-C; không chứng minh CO

Phần cứng và tích hợp nền tảng.

Chọn tên tài liệu để mở nguồn chính thức; phạm vi hỗ trợ được ghi dưới từng mục.

AB Circle · Datasheet

Thông số reader; cần xác nhận tổ hợp triển khai

Infineon · SLC27

Công bố SLC27 với thư viện ML-DSA/ML-KEM; không xác định CO theo lô

Utimaco · Quantum Protect

PQC và PKCS#11 vendor mechanisms; không thay báo cáo composite

Keyfactor · Utimaco

Tuyến tích hợp PQC qua PKCS#11

ISO · Hồ sơ Mobile-ID

ISMS trong phạm vi chứng chỉ; chưa xác minh duy trì với tổ chức cấp

Bảo đảm và hệ sinh thái.

Chọn tên tài liệu để mở nguồn chính thức; phạm vi hỗ trợ được ghi dưới từng mục.

SAM/QSCD · Hồ sơ Mobile-ID

TOE và cấu hình in trên hồ sơ; chưa xác minh duy trì với tổ chức cấp

Apple · CryptoTokenKit

Tích hợp token và tài sản mật mã; không cam kết PQC năm 2028

NIST · Security Policy

Ranh giới module và dịch vụ trong policy; không tự mở rộng sang SLC27

Mobile-ID · Hệ sinh thái

Danh mục nền tảng; không xác nhận PQC toàn bộ

QuantumSafe · Danh mục năng lực

Trạng thái công bố theo module; không thay nghiệm thu

Dịch vụ tin cậy và tiêu chuẩn hậu lượng tử.

Chọn tên tài liệu để mở nguồn chính thức; phạm vi hỗ trợ được ghi dưới từng mục.

Trusted SIC · Ký từ xa

Thí điểm có kiểm soát; lớp trải nghiệm, kích hoạt và thực thi

QuantumSafe · Dấu thời gian

Thí điểm có kiểm soát

Trusted TSA · Tích hợp

Hồ sơ chuẩn và demo; không dùng giấy phép mẫu

Trusted Delivery · Bằng chứng

Mô hình dịch vụ; không dùng đối tác/giấy phép demo

NIST · Tiêu chuẩn PQC

FIPS 203/204/205 và chuyển đổi mật mã