GIẢI PHÁP CYBERID
CHO NGÂN HÀNG

Phiên bản 1.0

MỤC LỤC

Theo dõi tài liệu

Tên tài liệu

Tiêu đề	GIẢI PHÁP CYBERID CHO NGÂN HÀNG
Tên file tài liệu	GIẢI PHÁP CYBERID CHO NGÂN HÀNG v1.0

Các phiên bản

Phiên bản	Ngày phát hành	Các sửa đổi	Ghi chú
1.0	17-08-2018	Tất cả	Phiên bản đầu tiên

Từ viết tắt

- FIDO: Fast IDentity Online
- UAF: Universal Authentication Framework
- CA: Certificate Authority
- RA: Registration Authority
- VA: Validation Authority
- TSA: TimeStamp Authority
- CTS: chứng thư số
- CSR: Certificate Signing Request
- CSDL: Cơ sở dữ liệu
- STID: Công ty TNHH Đầu tư và Phát triển Công nghệ Thông minh (VTCSmarttech)

1. Giới thiệu

CyberID là hệ thống công nghệ theo tiêu chuẩn FIDO UAF để xác thực/định danh người dùng và được tích hợp với Core Banking ứng dụng cho hệ thống Internet/Mobile Banking hiện hành của các ngân hàng, tổ chức tín dụng hoặc cho các website thương mại điện tử, công ty chứng khoán… cần đến sự xác thực người dùng cuối. CyberID bao gồm phần xác thực và ký số trên di động (CyberID Client) và phần xử lý trung tâm là hạt nhân của hệ thống (CyberID Service) tích hợp tại Core Server của ngân hàng.

CyberID đáp ứng yêu cầu "Giao dịch loại D" theo QĐ/630-NHNN về việc xác thực và ký giao dịch bằng thiết bị U2F/UAF và bằng chứng thư số, là môi trường tích hợp cần thiết cho các ứng dụng ngân hàng, tổ chức tín dụng nhằm đem lại độ bảo mật cao nhất tại thời điểm hiện tại cho các giao dịch điện tử giữa ngân hàng và người dùng.

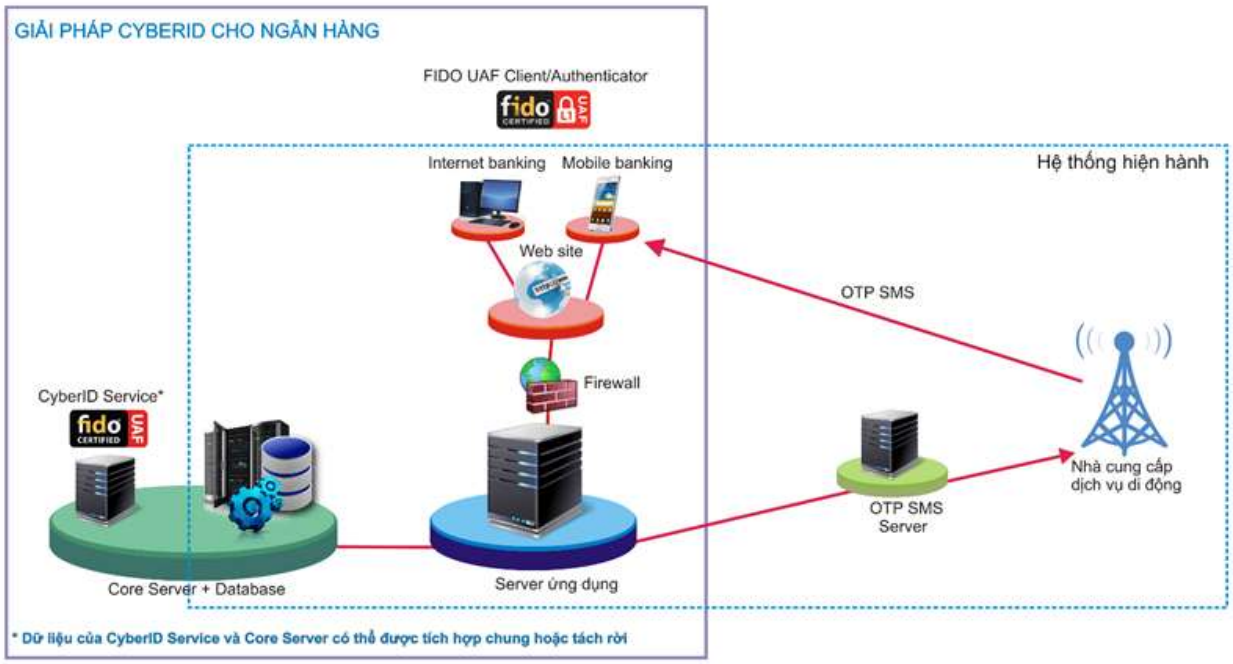
CyberID đã được cấp chứng chỉ bảo mật của liên minh FIDO, có sự tham gia của các tổ chức công nghệ hàng đầu thế giới cả về phần mềm, phần cứng lẫn ứng dụng như Google, Microsoft, Intel, ARM, Samsung, Qualcomm, LG, NXP, Facebook, Twitter, Paypal, Visa Card, Master Card, Bank of America….

Chứng chỉ FIDO UAF Server

Chứng chỉ FIDO UAF
Client/Authenticator Level 1

2. Mô hình hệ thống CyberID xác thực cho Mobile Banking

2.1 Mô hình hệ thống



Giải pháp CyberID cho ngân hàng mở rộng thêm phần xác thực thông qua tiêu chuẩn bảo mật cấp cao FIDO UAF bên cạnh các kiểu bảo mật truyền thống của hệ thống. Giải pháp CyberID bao gồm phần ứng dụng trên di động (Client) và phần CyberID Service tích hợp tại Core Server của ngân hàng. Yêu cầu đăng nhập từ phía khách hàng sẽ thông qua ***Server ứng dụng*** và tiến hành xác thực với CyberID Service.

Với mô hình này, khách hàng chỉ cần có smartphone hỗ trợ quét vân tay là đã có thể nâng cấp sử dụng dịch vụ an toàn, nhanh chóng là tiêu chí hàng đầu khi khách hàng sử dụng dịch vụ trực tuyến!

Giải pháp mang đến cho người dùng nhiều lợi điểm như:

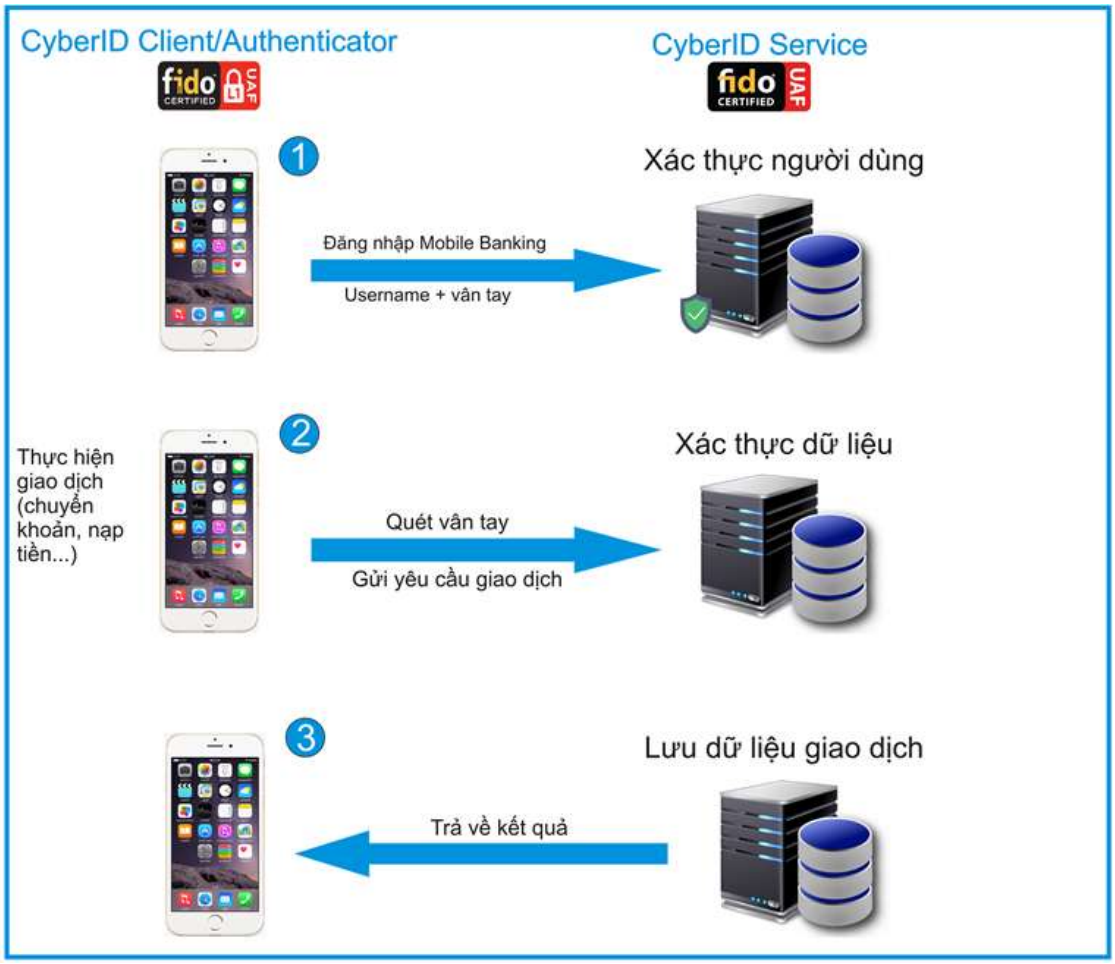
- Loại bỏ việc nhập mật khẩu phức tạp và khó nhớ cho người dùng bằng việc quét vân tay.
- Chỉ tích hợp thêm tính năng và bổ sung dữ liệu không gây ảnh hưởng đến hệ thống cũ.
- Thông tin khách hàng được đảm bảo an toàn và tin cậy theo tiêu chuẩn của liên minh FIDO.
- Không tốn chi phí đầu tư thiết bị đầu cuối phía người dùng, mọi smartphone đều có thể sử dụng được.
- Hỗ trợ đăng nhập Internet Banking trên trình duyệt bằng xác thực FIDO UAF trên di động.

2.2 Quy trình đăng ký

- Bước 0: Khách hàng đến Ngân hàng đăng ký sử dụng dịch vụ Internet/Mobile Banking để được cấp tài khoản mới bao gồm tên đăng nhập (Username) và mật khẩu (Password). Khách hàng tải hoặc cập nhật ứng dụng Mobile Banking (có tích hợp tính năng xác thực bằng FIDO) vào smartphone khách hàng.
- Bước 1: Khách hàng thực hiện đăng nhập ứng dụng Mobile Banking bằng tài khoản [Username + Password] được cung cấp ở Bước 0.
- Bước 2: Khách hàng đăng ký UAF bằng cách chọn chức năng "xác thực UAF" bên trong ứng dụng Mobile Banking. Ứng dụng sẽ yêu cầu khách hàng quét vân tay để định danh người dùng với tài khoản đăng nhập được cấp ở Bước 0.
- Bước 3: Nếu đăng ký thông tin thành công, một cặp khóa public + private sẽ được tạo ra và được cập nhập bổ sung vào dữ liệu [Username + Password] của ngân hàng đã tạo trước đó hoặc dữ liệu này có thể được quản lý riêng bởi hệ thống CyberID tùy yêu cầu của Ngân hàng. Nếu người dùng chọn kiểu xác thực cấp cao bằng UAF này làm mặc định thì cứ mỗi lần đăng nhập sau, ứng dụng sẽ yêu cầu quét vân tay.

  Khóa private, dùng cho quá trình xác thực và ký giao dịch, tạo ra ở Bước 3 được lưu trữ trên phần cứng bảo mật của điện thoại và không thể được truy xuất ra bên ngoài. Tất cả các thao tác của khách hàng về sau trên ứng dụng Mobile Banking (kiểm tra tài khoản, chuyển khoản, đặt vé máy bay, xem sao kê giao dịch,…) đều phải qua bước xác thực với UAF bằng việc quét vân tay.

2.2 Quy trình sử dụng



- Bước 1: Khách hàng đăng nhập vào tài khoản Mobilbe Banking xác thực bằng vân tay UAF.
- Bước 2: mỗi khi thực hiện giao dịch (chuyển khoản, nạp tiền điện thoại, thanh toán hóa đơn…) nào đó, người dùng đều phải quét vân tay UAF xác thực/ký cho giao dịch thực hiện trước khi gởi tới Server ứng dụng để kiểm tra.
- Bước 3: Sau khi Server ứng dụng kiểm tra thành công sẽ lưu dữ liệu giao dịch vào hệ thống và trả kết quả thông báo qua giao diện người dùng Mobile Banking.

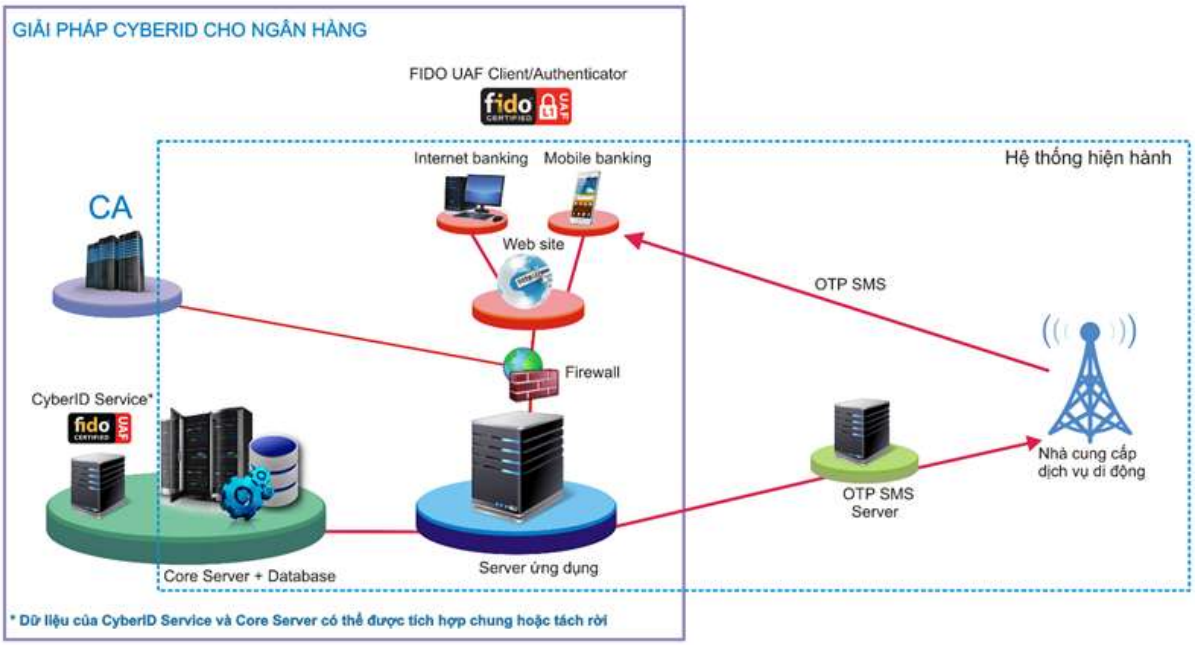
Bước 2 và Bước 3 sẽ được lặp lại mỗi khi Khách hàng thực hiện các giao dịch khác.

Chú ý:

- *Khi thay thế hoặc làm thất lạc smartphone trong quá trình sử dụng, người dùng cần phải đăng ký lại dịch vụ quét vân tay UAF này trên smartphone mới để vô hiệu hóa tính năng xác thực bằng UAF trên smartphone cũ.*

3. Mô hình CyberID xác thực và ký giao dịch thông qua CA cho Mobile Banking

3.1 Mô hình hệ thống

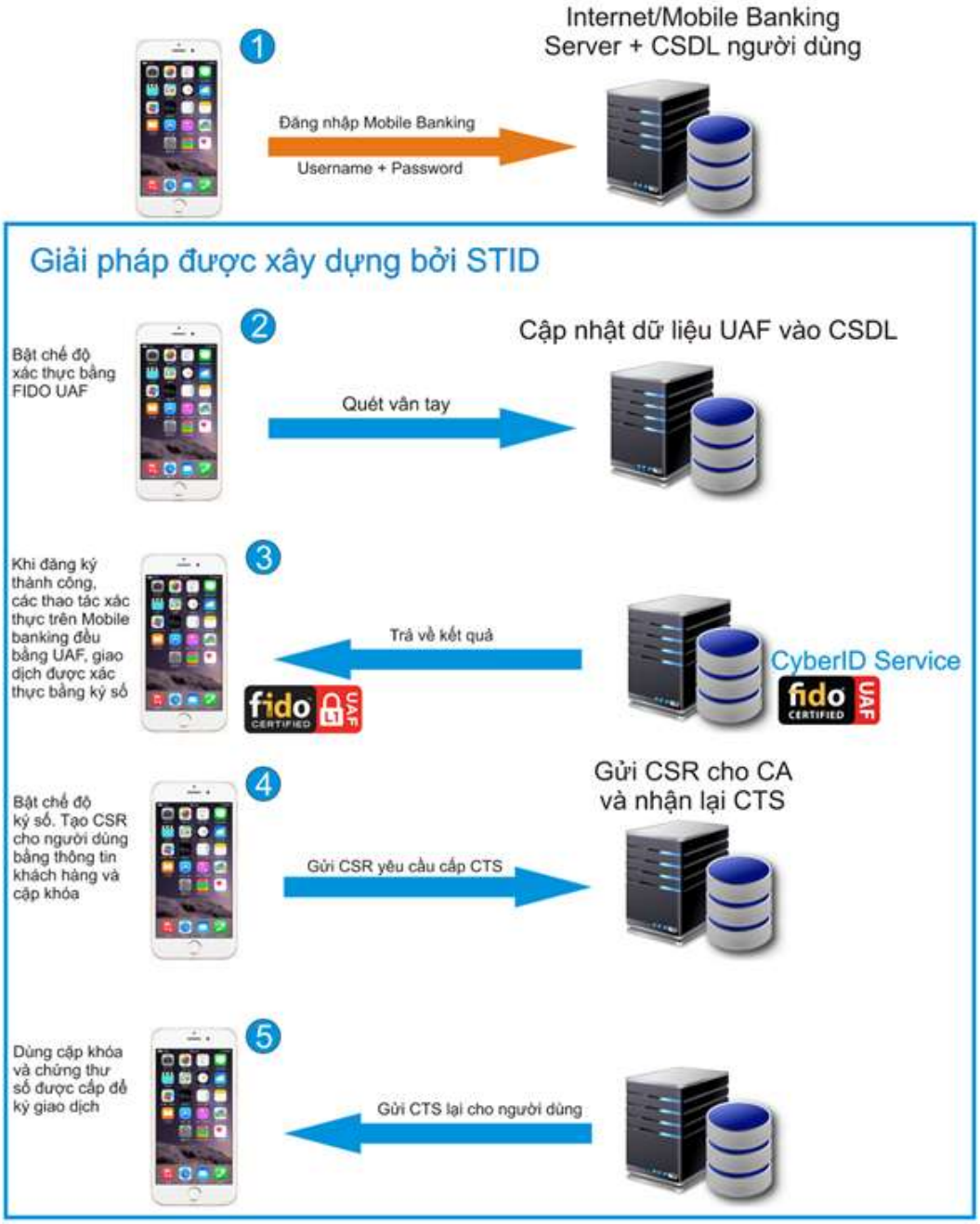


Giải pháp CyberID xác thực và ký giao dịch cho ngân hàng được xây dựng trên nền hệ thống hiện hành bổ sung thêm module xác thực FIDO UAF Client/Authenticator phía Client và CyberID Service phía Core Server. Mô hình này cần CA (công cộng hoặc dùng riêng) cấp phát chứng thư số dùng cho quá trình ký số các giao dịch cần thiết của ngân hàng. Quá trình xin cấp phát và nhận chứng thư số sẽ được kết nối trực tiếp tới module giao tiếp của hệ thống CA qua giao diện ứng dụng Mobile Banking.

Với mô hình này, khách hàng cuối phải đầu tư chi phí chứng thư số mua từ các nhà cung cấp dịch vụ CA hoặc ngân hàng cũng có thể tự đầu tư xây dựng hệ thống CA dùng riêng này.

Nếu ngân hàng không dùng chứng thư số của CA cung cấp mà vẫn muốn có chức năng ký giao dịch thì có thể sử dụng luôn cặp khóa phát sinh trong quá trình đăng ký FIDO UAF để ký cho các giao dịch. Tuy nhiên, các giao dịch ký số này chỉ có giá trị trong nội tại ngân hàng triển khai hệ thống này mà thôi.

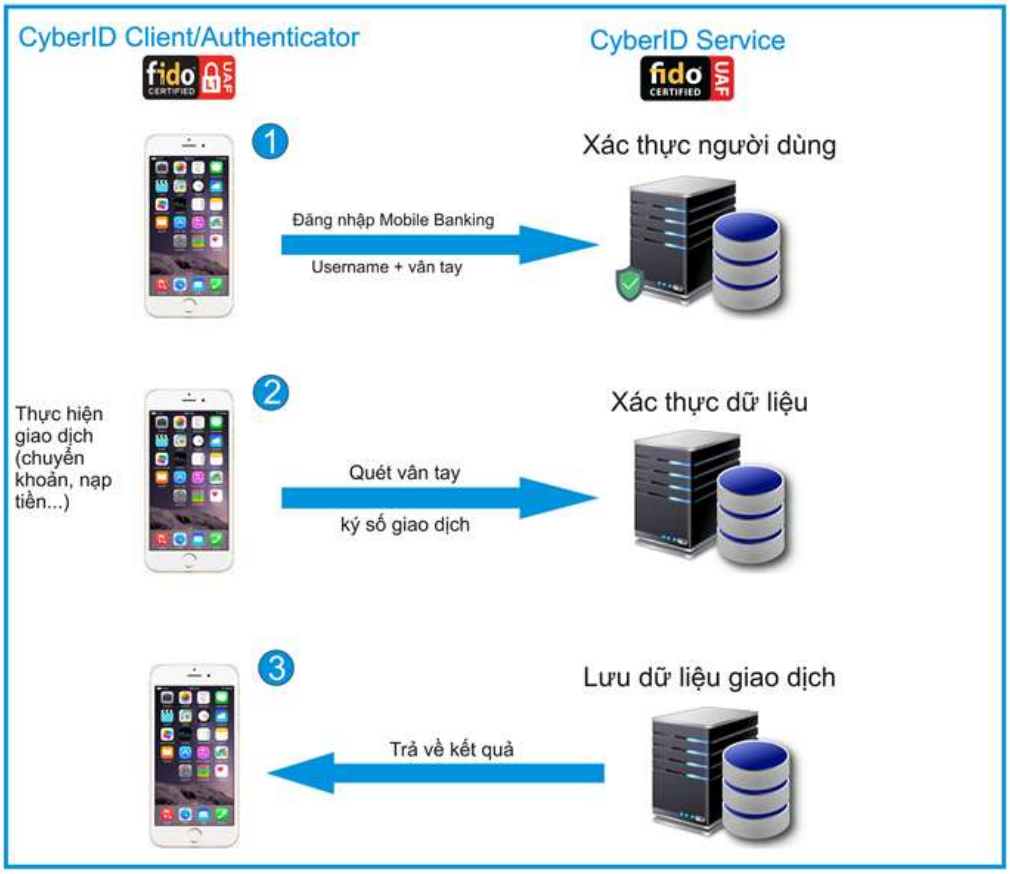
3.2 Quy trình đăng ký



- Bước 0 đến Bước 3: tương tự các bước trong mục 2.2
- Bước 4: Người dùng bật chế độ ký số (có thể được thực hiện tự động sau quá trình xác thực) trên ứng dụng Mobile Banking. Ứng dụng sẽ khởi tạo cặp khóa public và private, sau đó tạo chuỗi CSR (Certificate Signing Request) yêu cầu cấp chứng thư số đến CA từ giao diện ứng dụng Mobile Banking thông qua ***Server ứng dụng*** của ngân hàng.
- Bước 5: CA sau khi nhận CSR sẽ kiểm tra, phê duyệt và cấp phát chứng thư số dựa vào thông tin có trong CSR này rồi gửi lại cho ***Server ứng dụng***. Chứng thư số sau đó được ***Server ứng dụng*** gửi đến ứng dụng Mobile Banking để lưu trữ vào vùng

nhớ bảo mật của smartphone khách hàng. Kể từ lúc này, với chứng thư số và cặp khóa đã khởi tạo, khách hàng có thể ký số mọi giao dịch sau quá trình xác thực với UAF trước đó.

3.3 Quy trình sử dụng



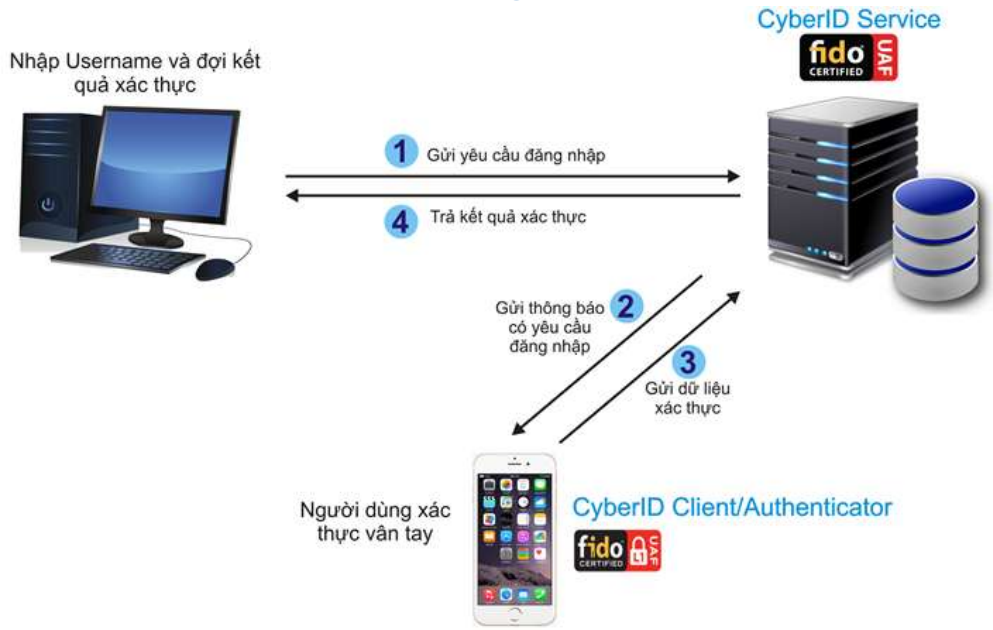
- Bước 1: Khách hàng đăng nhập vào tài khoản Mobilbe Banking xác thực bằng vân tay UAF.
- Bước 2: mỗi khi thực hiện giao dịch (chuyển khoản, nạp tiền điện thoại, thanh toán hóa đơn…) nào đó, người dùng đều phải quét vân tay UAF để ký số cho giao dịch thực hiện trước khi gởi tới Server ứng dụng để kiểm tra. Quá trình ký số ở giai đoạn này sẽ sử dụng chứng thư số được cấp từ CA trong giai đoạn đăng ký trước đó.
- Bước 3: Sau khi Server ứng dụng kiểm tra thành công sẽ lưu dữ liệu giao dịch vào hệ thống và trả kết quả thông báo trên giao diện người dùng.

Bước 2 và Bước 3 sẽ được lặp lại mỗi khi Khách hàng thực hiện các giao dịch khác.

Chú ý:

- *Khi thay thế hoặc làm thất lạc smartphone trong quá trình sử dụng, người dùng cần phải đăng ký lại dịch vụ quét vân tay UAF này trên smartphone mới để vô hiệu hóa tính năng xác thực bằng UAF trên smartphone cũ.*

4 CyberID xác thực cho Internet Banking



Với cả hai mô hình ở mục 2 và 3, khách hàng cuối cũng có thể sử dụng chức năng xác thực người dùng khi đăng nhập Internet Banking trên máy tính PC bằng việc tận dụng quá trình xác thực UAF trên smartphone để tăng tính bảo mật.

Để đáp ứng được điều này, phía ứng dụng Internet Banking của ngân hàng sẽ tích hợp thêm module đăng nhập bằng UAF.

Cách thực hiện:

- Người dùng cài đặt ứng dụng Mobile Banking và đăng ký chức năng xác thực web bằng FIDO UAF trên ứng dụng Mobile Banking.
- Tại bước đăng nhập Internet Banking, thay vì phải nhập mật khẩu và OTP SMS (nếu có), người dùng được yêu cầu quét vân tay trên smartphone để xác thực việc đăng nhập.
- Nếu xác thực thành công bởi hệ thống CyberID thì người dùng mới được phép thực hiện các tác vụ khác của ứng dụng.

5 Tích hợp hệ thống CyberID với hệ thống hiện tại

Việc tích hợp giải pháp CyberID với hệ thống hiện tại có thể được thực hiện theo trình tự tích hợp sau:

5.1 CyberID Service

CyberID Service là hạt nhân của cả giải pháp được triển khai trên nền tảng web service dùng để tiếp nhận và kiểm tra yêu cầu xác thực từ CyberID Client gửi đến tới hệ thống Core Banking của ngân hàng tùy vào yêu cầu đưa ra.

CyberID Service sẽ được STID triển khai và cung cấp API cho ngân hàng kết nối tới hệ thống xác thực. CyberID Service này đã được cấp chứng chỉ chứng nhận UAF Server từ liên minh FIDO.

5.2 CyberID Client/Authenticator

CyberID Client/Authenticator là gói thư viện trên di động hỗ trợ cả hệ điều hành Android và iOS phục vụ cho nhiệm vụ xác thực người dùng Mobile Banking. Nhóm phát triển ứng dụng Mobile Banking của ngân hàng chỉ cần gọi các hàm kết nối tới CyberID Client/Authenticator để thực hiện quá trình xác thực. Gói giải pháp cũng đã được chứng nhận UAF Client/Authenticator Level 1 từ liên minh FIDO.

5.3 CyberID CA (dùng cho mô hình xác thực và ký số giao dịch)

- CyberID CA là giải pháp tổng thể về chữ ký số bao gồm CA server, RA server, VA server và TSA server. Ngân hàng cần triển khai cân nhắc lựa chọn phát triển CA dùng riêng hoặc CA công cộng:
  - CA dùng riêng: STID sẽ tư vấn và phát triển hệ thống này cho ngân hàng do đã có kinh nghiệm triển khai hệ thống CA dùng riêng tại ngân hàng SeAbank trước đây cùng đối tác.
  - CA công cộng: STID sẽ cung cấp module kết nối tới CA (chẳng hạn NewCA, VNPT-CA, Viettel-CA) để gởi yêu cầu cấp phát và cập nhật chứng thư số từ giao diện ứng dụng Mobile Banking cho khách hàng.
- STID cũng sẽ cung cấp thư viện API để ngân hàng có thể tích hợp vào hệ thống ký số giao dịch, ký số tài liệu (Microsoft Office, PDF, XML, plaintext…) trên cả smartphone lẫn máy tính để bàn PC/Laptop.
- Tham khảo hệ thống CA do STID phát triển tại: https://cybersecurity.com.vn/

Tài liệu tham khảo

1. Chứng chỉ UAF server và UAF Client/Authenticator của STID tại: https://vtcsmarttech.com.vn//wp-content/uploads/fido-certified-products.html

2. Thông tin cặp khóa được lưu trữ trong vùng nhớ bảo mật của thiết bị iOS và Android:
   - iOS: https://spr.com/ios-security-protecting-the-ios-keychain/ https://developer.apple.com/documentation/security/certificate_key_and_trust_services/keys/storing_keys_in_the_secure_enclave
   - Android: https://fidoalliance.org/wp-content/uploads/Hardware-backed_Keystore_White_Paper_June2018.pdf