XÁC THỰC NHANH FIDO

Ver 2.3

vtcsmarttech
STID nâng cánh giá trị

CÔNG TY CỔ PHẦN ĐẦU TƯ VÀ PHÁT TRIỂN CÔNG NGHỆ THÔNG MINH

www.vtcsmarttech.com.vn

Nội dung

1. CÁC VẤN ĐỀ XÁC THỰC HIỆN NAY
2. TIÊU CHUẨN XÁC THỰC FIDO/FIDO2
3. HỢP TÁC STID – FIDO ALLIANCE
4. TÍCH HỢP HỆ THỐNG

CÁC VẤN ĐỀ CỦA XÁC THỰC HIỆN NAY

XÁC THỰC ĐANG LÀ VẤN ĐỀ LỚN CỦA CHÚNG TA

AUTHENTICATION IS OUR BIGGEST PROBLEM

fido ALLIANCE

WIRED

SO, UH, THAT BILLION-ACCOUNT YAHOO BREACH WAS ACTUALLY 3 BILLION

The New York Times

Target to Pay $18.5 Million to 47 States in Security Breach Settlement

The Register

Sensitive client emails, usernames, passwords exposed in Deloitte hack

Fortune

LinkedIn Lost 167 Million Account Credentials in Data Breach

Mashable

Someone is selling 33 million Twitter passwords on the dark web

ars technica

Cluster of "megabreaches" compromises a whopping 642 million passwords

The New York Times

Russian Hackers Amass Over a Billion Internet Passwords

By Nicole Perlroth and David Gelles

Aug. 5, 2014

473

A Russian crime ring has amassed the largest known collection of stolen Internet credentials, including 1.2 billion user name and password combinations and more than 500 million email addresses, security researchers say.

HELPNETSECURITY

Help Net Security

December 5, 2012

Share

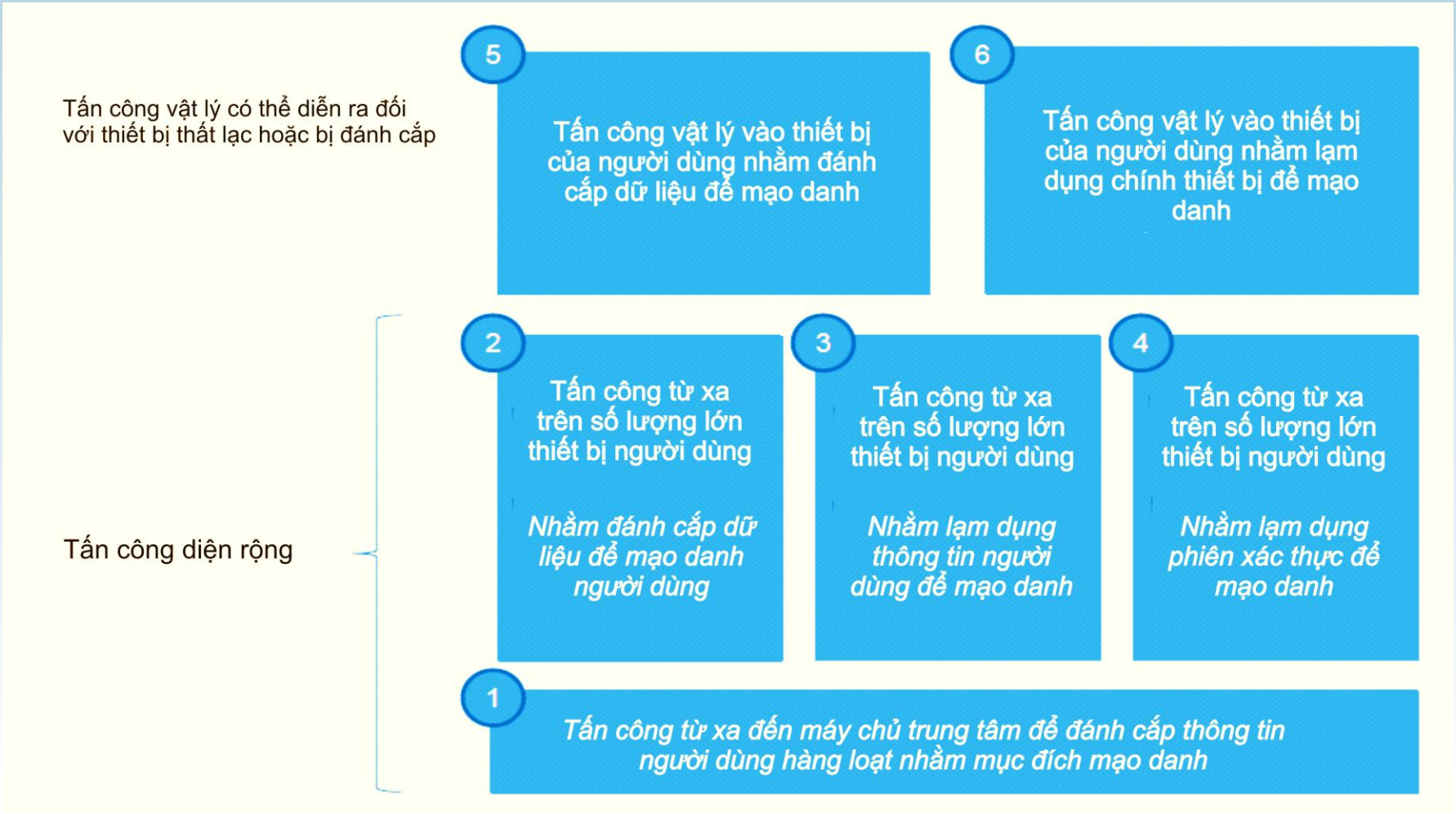
How the Eurograbber attack stole 36 million euros

Check Point has revealed how a sophisticated malware attack was used to steal an estimated Ã¢â€šÂ¬36 million from over 30,000 customers of over 30 banks in Italy, Spain, Germany and Holland over summer this year.

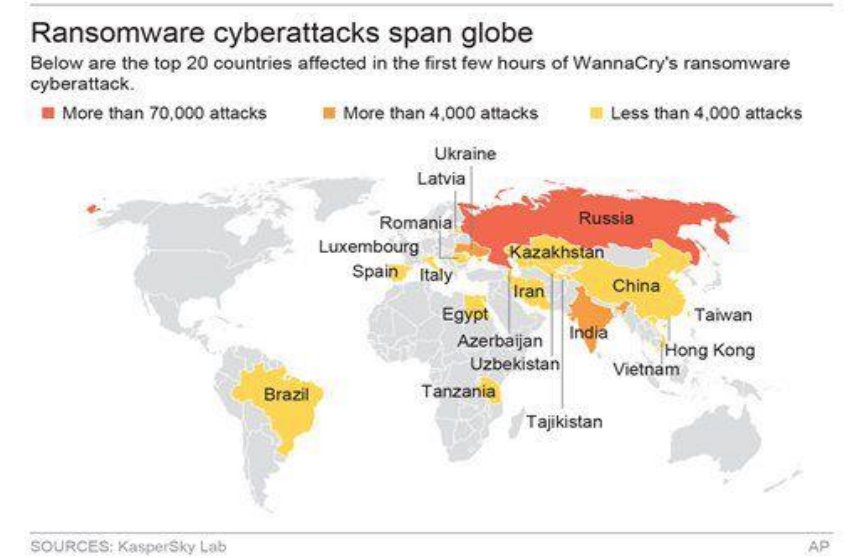
The theft used malware to target the PCs and mobile devices of banking customers. The attack also took advantage of SMS messages used by banks as part of customers' secure login and authentication process.

CÁC VẤN ĐỀ CỦA XÁC THỰC HIỆN NAY

NHỮNG NGUY CƠ TIỀM ẨN ĐỐI VỚI XÁC THỰC GIAO DỊCH



CÁC VẤN ĐỀ CỦA XÁC THỰC HIỆN NAY



An toàn an ninh thông tin tại Việt Nam vẫn đang là vấn đề nhức nhối!!!

CÁC VẤN ĐỀ CỦA XÁC THỰC HIỆN NAY

"Lâu nay, chúng ta nói nhiều đến tuyên truyền, song tôi nghĩ vấn đề an ninh mạng cần phải cụ thể hóa, phải luật hóa rõ ràng thì mới mong cải thiện được tình hình"

Nguyễn Thanh Hải,
Cục trưởng cục An toàn Thông tin

"Một nghiên cứu mới của hãng bảo mật Kaspersky tại Việt Nam cho thấy, có tới ¾ người dùng không biết tự bảo vệ mình trên mạng"

Thiếu tướng Nguyễn Viết Thế, nguyên Cục trưởng cục Tin học-Nghiệp vụ Công an (bộ Công an)

Chỉ số an ninh mạng Việt Nam thấp giật mình so với thế giới

Người Đưa Tin ☆ 04/11/17 13:38 GMT+7 3 liên quan Gốc

Lượng người dùng internet ở Việt Nam đang tăng với tốc độ rất nhanh. Tuy nhiên, vấn đề bảo mật an ninh mạng lại tỷ lệ nghịch với sự phát triển, gây nên nhiều lo ngại.

Thông tin vừa được chia sẻ tại buổi tọa đàm Chia sẻ nghiên cứu sáng kiến về CNTT cơ bản và an toàn internet tại Việt Nam.

Theo cục Viễn thông (bộ Thông tin và Truyền thông), tỷ lệ người dùng internet tại Việt Nam đã đạt 53% trên tổng dân số. Việt Nam đứng vị trí thứ 16 trong top 20 quốc gia có số người sử dụng internet nhiều nhất tại Châu Á và độ tuổi người sử dụng đa phần là người trẻ, chiếm hơn 50% so với tổng dân số.

Myanmar	0.263	100
Viet Nam	0.245	101
Afghanistan	0.245	101
Syrian Arab Republic	0.237	102

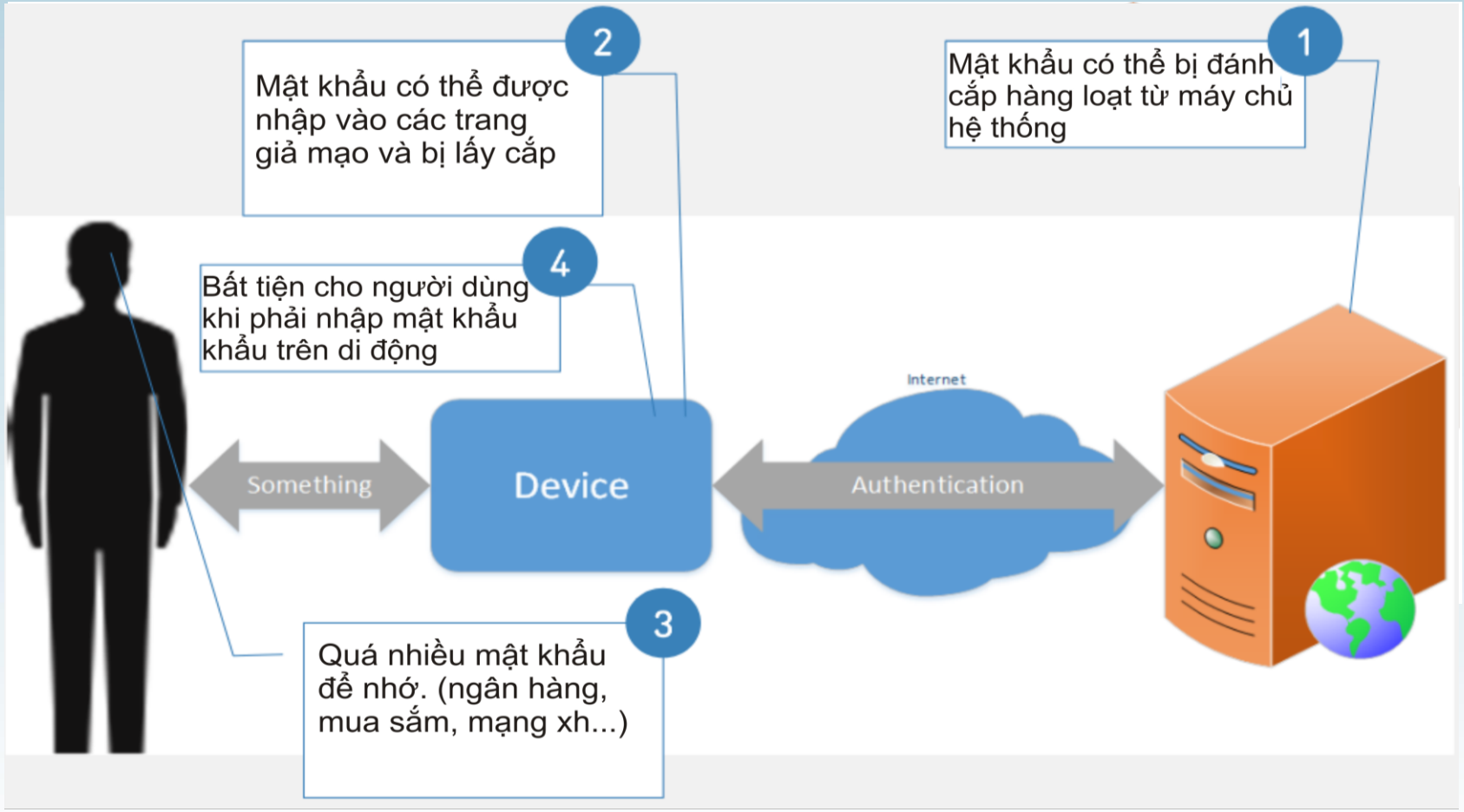
" Xếp hạng an toàn an ninh thông tin một số quốc gia - Trích báo cáo an ninh mạng toàn cầu – ITU 2017"

vtcsmarttech STID nâng cánh giá trị

fido alliance simpler stronger authentication

CÁC VẤN ĐỀ CỦA XÁC THỰC HIỆN NAY

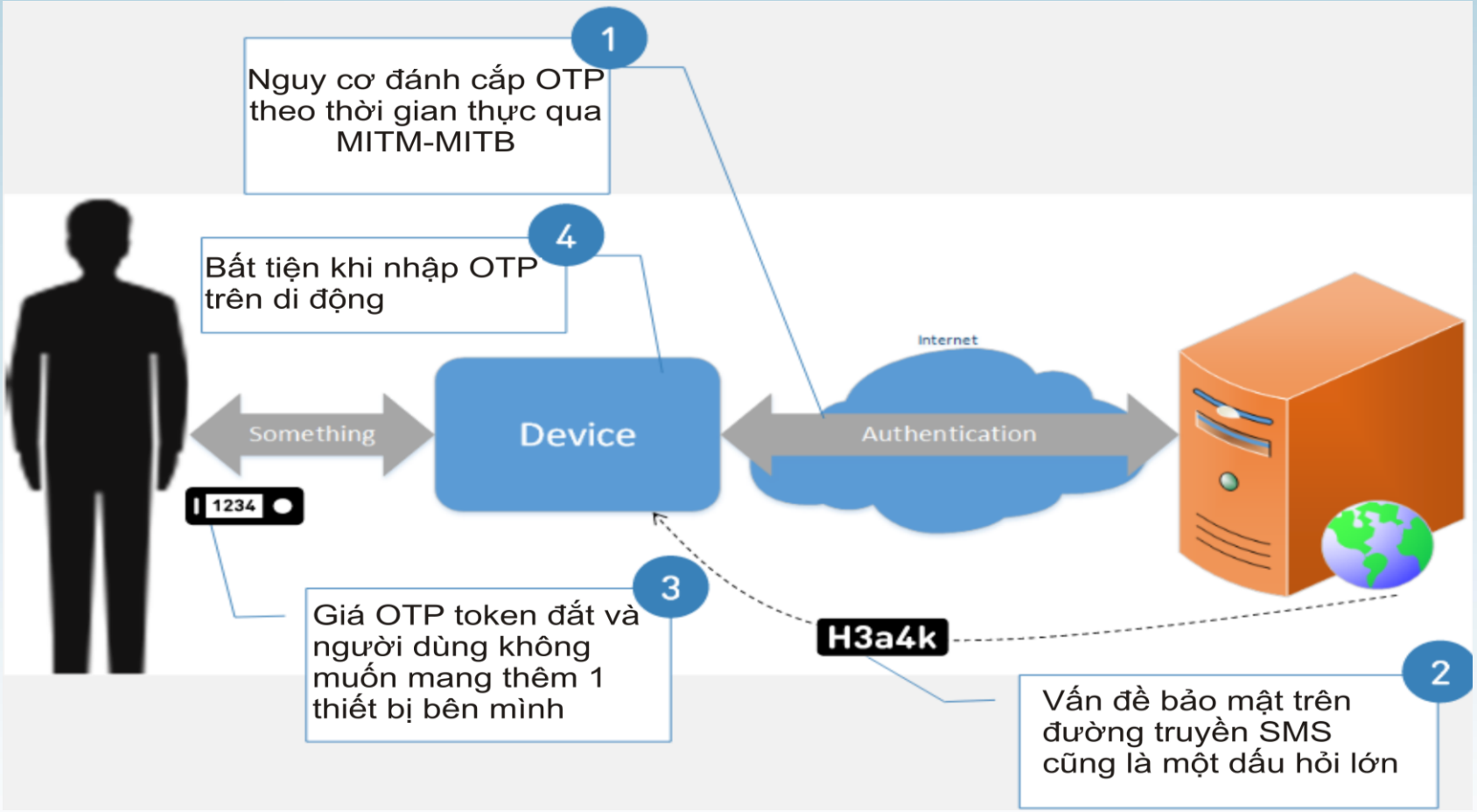
NHỮNG VẤN ĐỀ ĐỐI VỚI LƯU TRỮ VÀ XÁC THỰC TRUYỀN THỐNG



Xác thực truyền thống bằng mật khẩu

CÁC VẤN ĐỀ CỦA XÁC THỰC HIỆN NAY

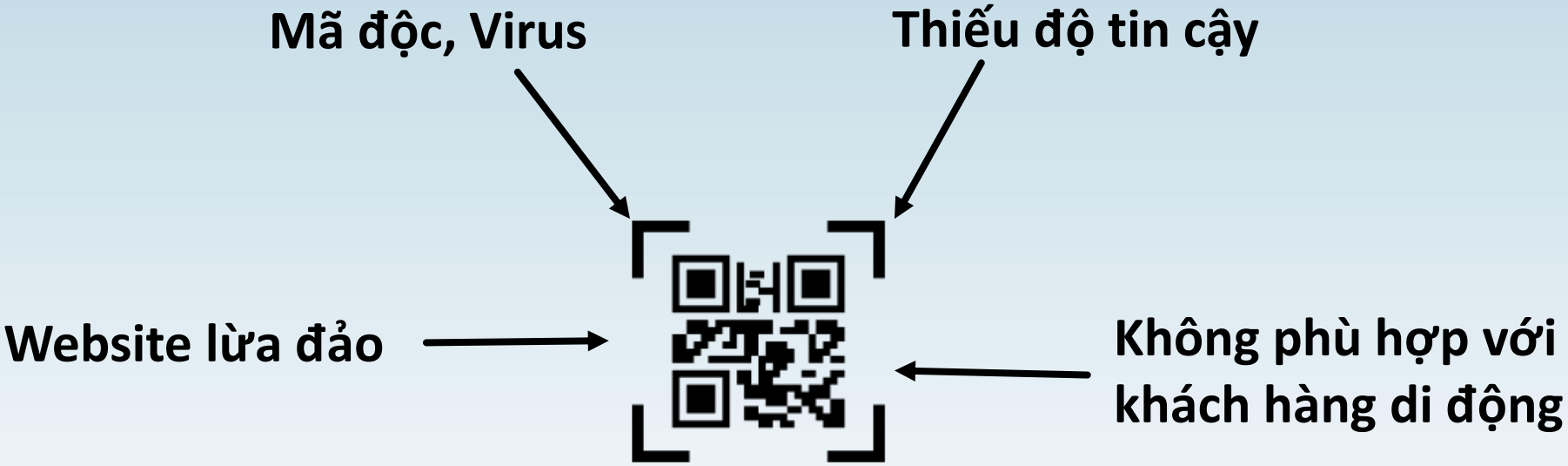
NHỮNG VẤN ĐỀ ĐỐI VỚI LƯU TRỮ VÀ XÁC THỰC TRUYỀN THỐNG



Xác thực bằng OTP (Token/SMS)

CÁC VẤN ĐỀ CỦA XÁC THỰC HIỆN NAY

NHỮNG VẤN ĐỀ ĐỐI VỚI LƯU TRỮ VÀ XÁC THỰC TRUYỀN THỐNG



Xác thực bằng QR Code

CÁC VẤN ĐỀ CỦA XÁC THỰC HIỆN NAY

NHỮNG VẤN ĐỀ CẦN ĐẾN XÁC THỰC HẰNG NGÀY

- Quá nhiều mật khẩu phải nhớ cho tất cả dịch vụ.
- Dễ bị đánh mất mọi tài khoản cá nhân nếu dùng mật khẩu dễ nhớ, đơn giản hoặc được dùng chung.
- Mật khẩu không gắn liền với người dùng khi xảy ra sự cố, gây ra nhiều bất tiện.

=> Nhu cầu về 1 mật khẩu duy nhất và an toàn được đặt ra

CÁC VẤN ĐỀ CỦA XÁC THỰC HIỆN NAY

NHỮNG VẤN ĐỀ CHUNG

1. Mật khẩu vừa không an toàn, vừa bất tiện, đặc biệt trên thiết bị di động.

2. Các phương thức xác thực thay thế phổ biến chỉ là OTP nhưng khó khăn khi triển khai với quy mô lớn (SMS OTP, OTP Token chi phí cao và bất tiện,…)

3. Mức độ bảo mật yêu cầu phụ thuộc vào nhu cầu sử dụng, đôi khi cần kết hợp 2-3 phương thức xác thực cho 1 nhu cầu và gây bất tiện cho người dùng.

4. Các phương tiện phân tích rủi ro cần thông tin đảm bảo xác thực để đánh giá và đưa ra quyết định chính xác cho các vấn đề.

CÁC VẤN ĐỀ CỦA XÁC THỰC HIỆN NAY

Chúng ta cần một mô hình mới!

Tiêu chuẩn xác thực Fast IDentity Online

https://fidoalliance.org/

vtcsmarttech
STID nâng cánh giá trị

fido alliance | simpler stronger authentication

TIÊU CHUẨN XÁC THỰC FIDO/FIDO2

XÁC THỰC FIDO LÀ GÌ?

- FIDO là một tiêu chuẩn xác thực người dùng độc lập khả dụng trên toàn cầu, được phát triển bởi liên minh công nghệ FIDO Alliance do các công ty/tổ chức hàng đầu thế giới sáng lập nên vào năm 2014 như Google, Apple, Microsoft, Fujitsu, Yubico, MasterCard, Paypal…

- FIDO sử dụng công nghệ xác thực khuôn mặt, vân tay trên thiết bị di động hoặc mật mã số để xác thực người dùng mà không cần mật khẩu. Điều này giúp tăng cường bảo mật và giảm rủi ro bị hack mật khẩu, đồng thời cũng giúp người dùng tránh việc phải nhớ quá nhiều mật khẩu khác nhau cho các tài khoản khác nhau.

- FIDO đang dần được sử dụng rộng rãi trên các nền tảng và dịch vụ trực tuyến hỗ trợ hầu hết các thiết bị như máy tính, thiết bị di động và máy tính bảng.

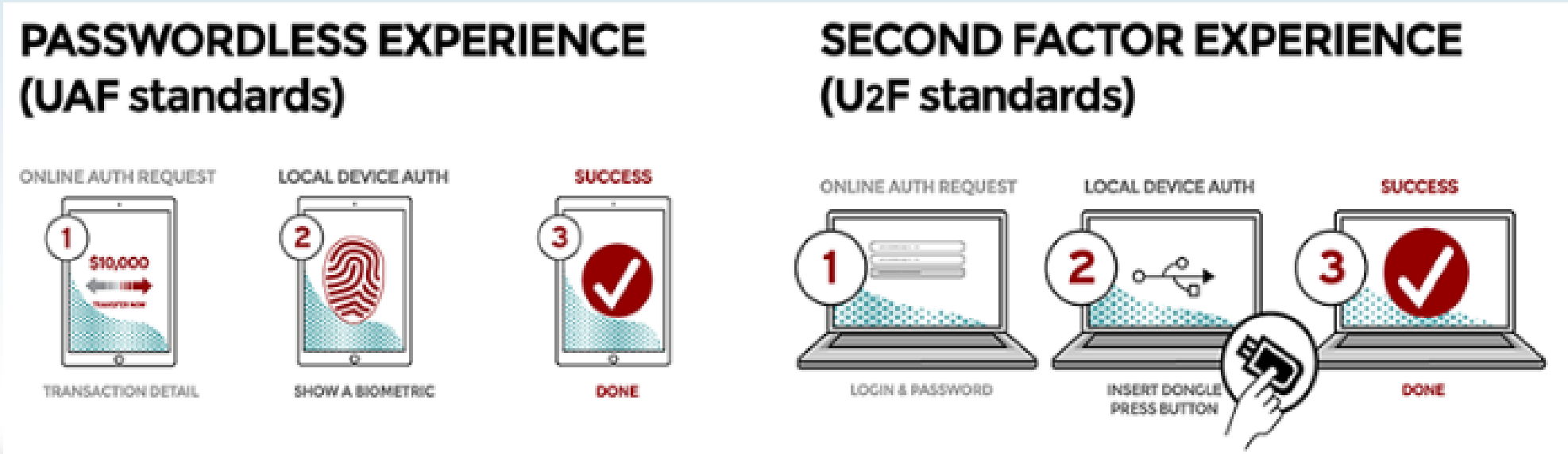
TIÊU CHUẨN XÁC THỰC FIDO/FIDO2

XÁC THỰC FIDO LÀ GÌ?

- FIDO phân ra 2 loại xác thực chính: UAF và U2F

  - ❑ UAF là một tiêu chuẩn đăng nhập hai yếu tố (2FA) bằng sinh trắc học như cảm biến vân tay, cảm biến khuôn mặt hoặc bằng giọng nói.

  - ❑ U2F là một tiêu chuẩn đăng nhập hai yếu tố sử dụng phương tiện xác thực như chìa khóa bảo mật USB.



TIÊU CHUẨN XÁC THỰC FIDO/FIDO2

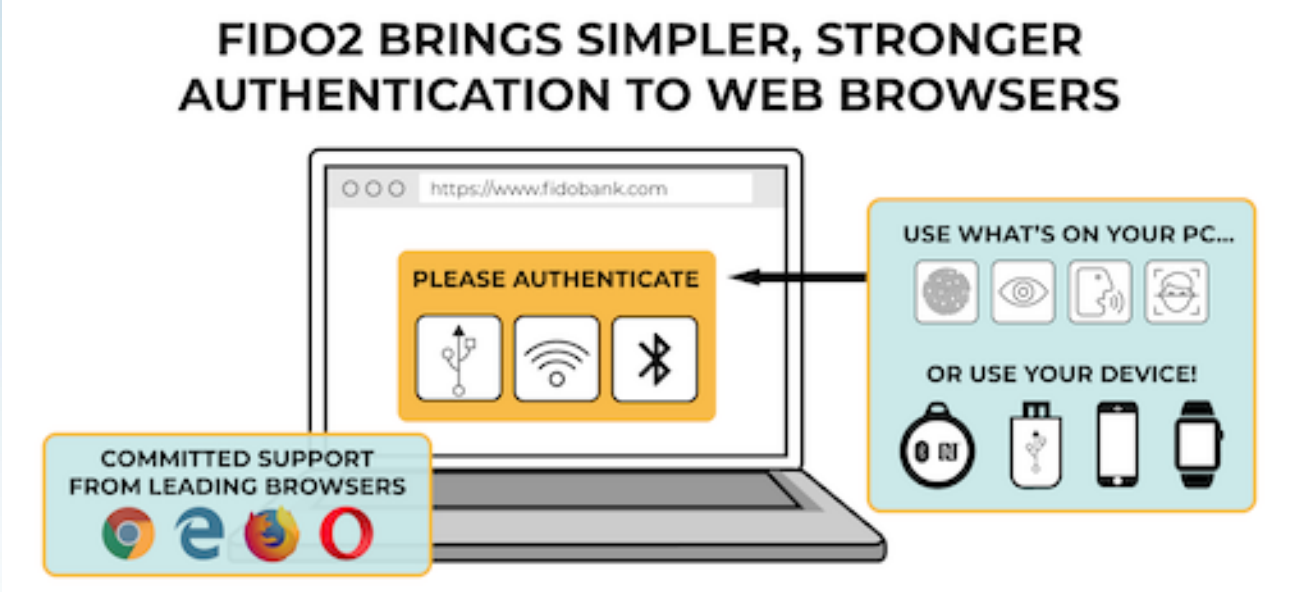
XÁC THỰC FIDO2 LÀ GÌ?

- FIDO2 là tiêu chuẩn đăng nhập hai yếu tố mới nhất được FIDO phát triển năm 2018.

- FIDO2 bao gồm hai tiêu chuẩn mới là WebAuthn và CTAP:

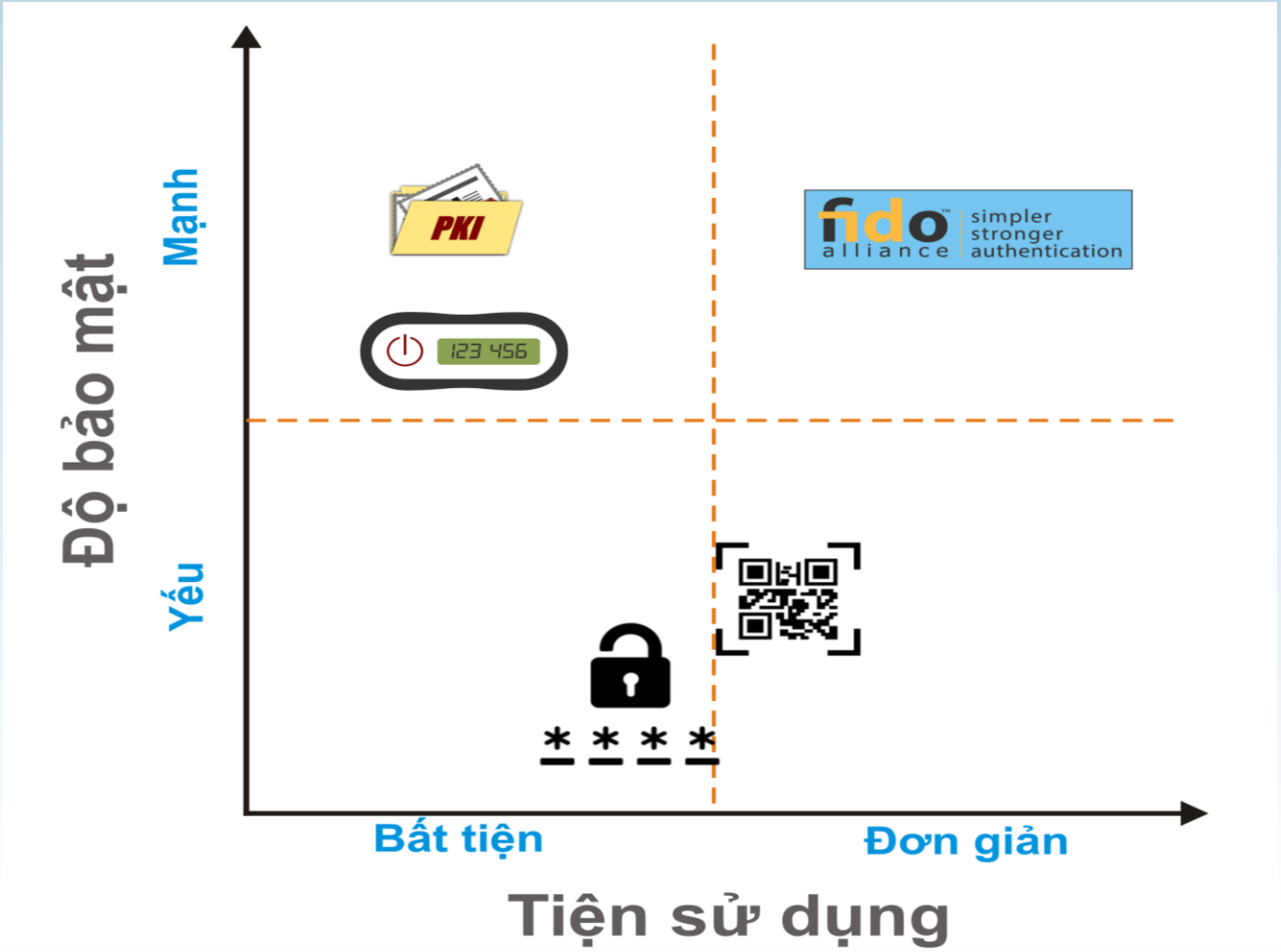
  - ❑ WebAuthn là một chuẩn đăng nhập dựa trên trình duyệt, cho phép người dùng đăng nhập vào các trang web một cách an toàn và dễ dàng.

  - ❑ CTAP là một giao thức giữa trình duyệt và phương tiện xác thực, cho phép phương tiện xác thực giao tiếp an toàn với trình duyệt.



TIÊU CHUẨN XÁC THỰC FIDO/FIDO2

MỤC TIÊU CỦA FIDO/FIDO2



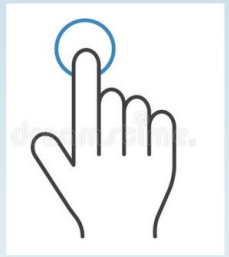
TIÊU CHUẨN XÁC THỰC FIDO/FIDO2

XÁC THỰC ĐƠN GIẢN HƠN

1

Loại bỏ mật khẩu gây bất tiện

2



Chỉ với một tương tác duy nhất với người dùng

3

Hoạt động với nhiều thiết bị phổ biến

4

Xác thực tương tự với nhiều loại thiết bị khác nhau

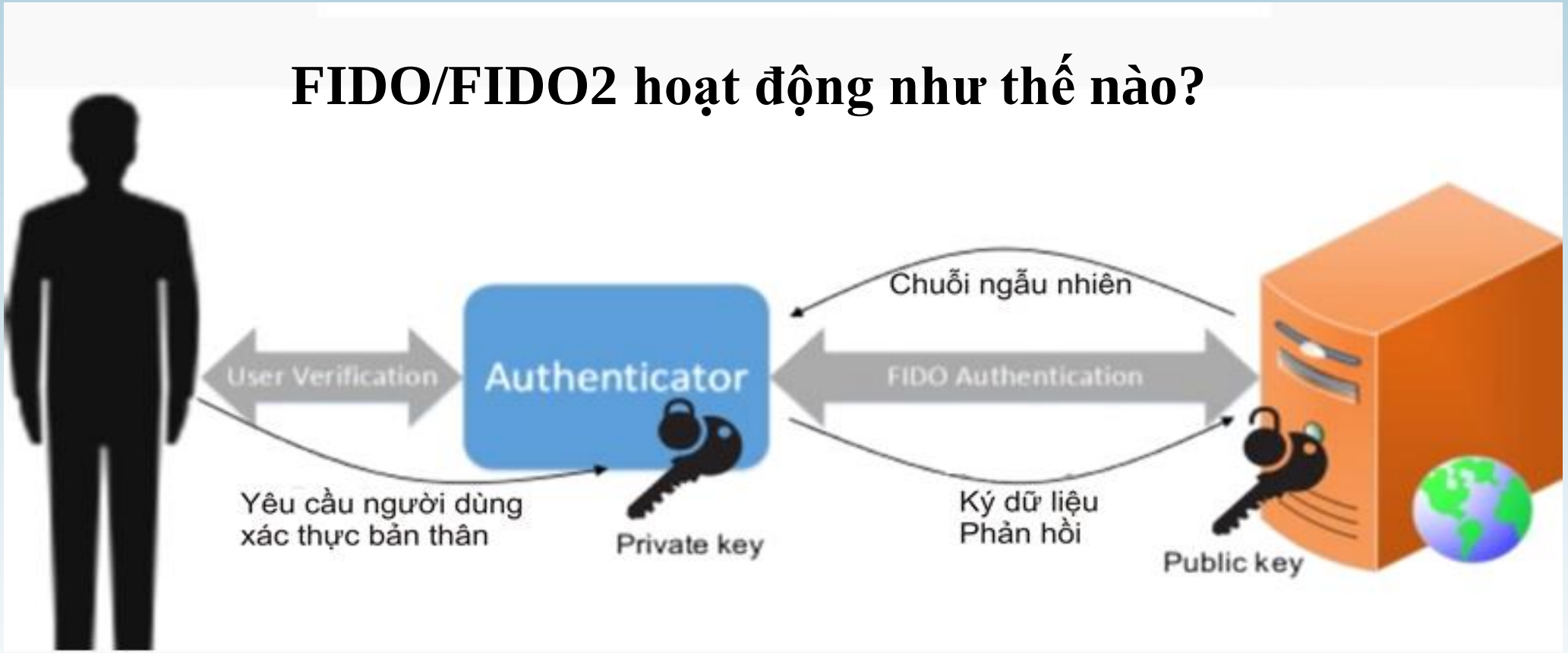
5

Nhanh chóng và tiện lợi

TIÊU CHUẨN XÁC THỰC FIDO/FIDO2

XÁC THỰC AN TOÀN HƠN

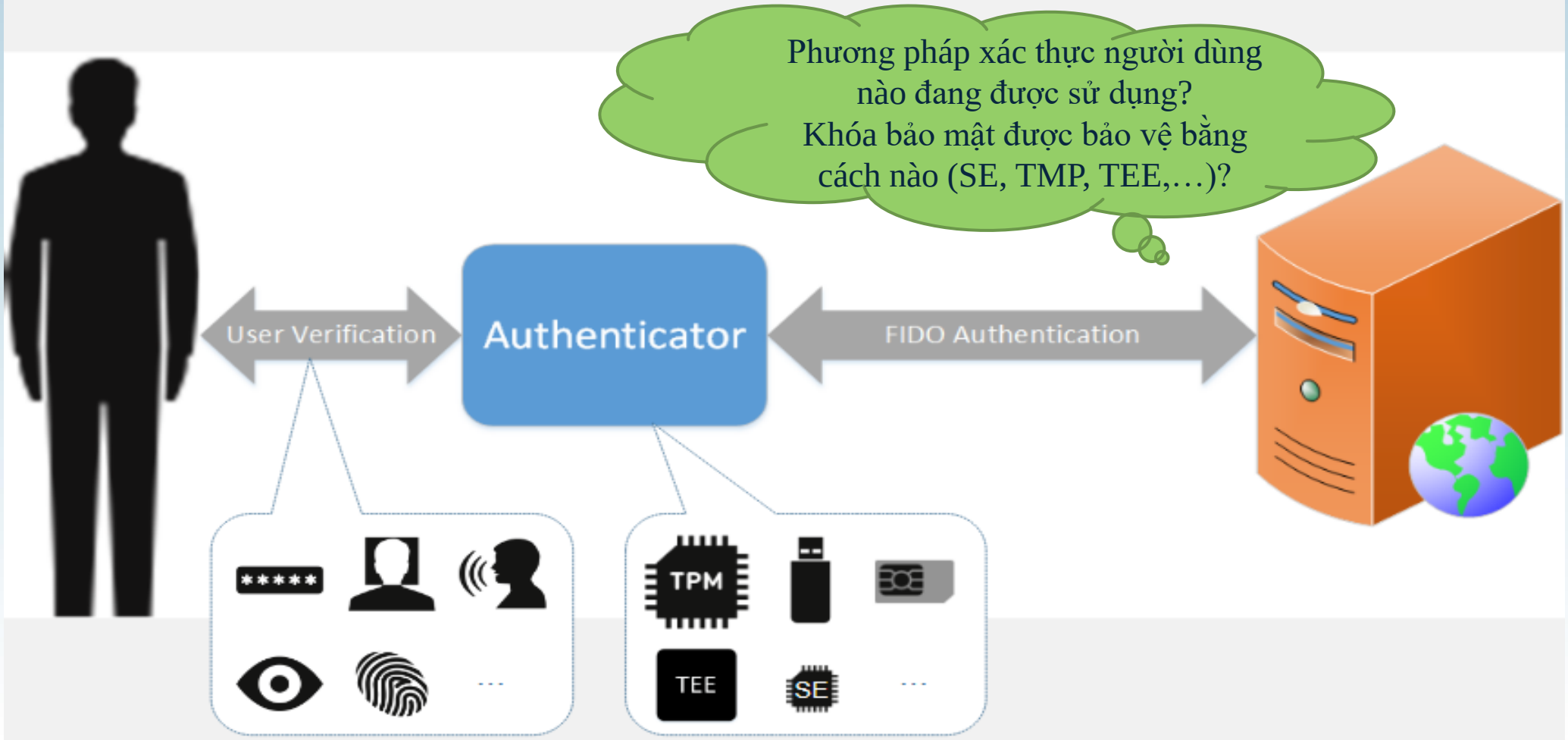
TIÊU CHUẨN XÁC THỰC FIDO/FIDO2



FIDO hoạt động dựa trên việc **xác thực người dùng với thiết bị** thông qua việc kiểm tra sinh trắc học/mã PIN và **xác thực thiết bị với dịch vụ** sử dụng thông qua FIDO server.

TIÊU CHUẨN XÁC THỰC FIDO/FIDO2

FIDO/FIDO2 hoạt động như thế nào?



TIÊU CHUẨN XÁC THỰC FIDO/FIDO2

KHOÁ BẢO MẬT ĐƯỢC LƯU Ở ĐÂU?

- Khoá bảo mật được mã hoá và lưu ở vùng nhớ độc lập với hệ điều hành của thiết bị di động, trên Secure Enclave cho chip Apple hay trên TrustZone cho chip ARM hay trên Titan M cho chip Google.
  → Cho dù thiết bị di động bị dính malware, malware có thể chiếm quyền kiểm soát toàn hệ điều hành iOS hay Android, truy xuất mọi thông tin hay dữ liệu nó muốn nhưng nó sẽ không thể truy xuất vào những thứ nằm trong vùng bảo mật!

- Khi người dùng mở khoá điện thoại bằng mã PIN, FaceID hay TouchID thì vi xử lý bên trong vùng bảo mật sẽ xác thực người dùng và sử dụng khoá xác thực này để giải mã dữ liệu trong bộ nhớ.

TIÊU CHUẨN XÁC THỰC FIDO/FIDO2

KHOÁ BẢO MẬT ĐƯỢC LƯU Ở ĐÂU?

TrustZone của ARM hoạt động tương tự Secure Enclave, nó cũng tạo ra một vùng an toàn để lưu khoá bảo mật. Chẳng hạn như phần mềm Samsung KNOX chạy trên vùng bảo mật TrustZone nhờ đó nó tách biệt hoàn toàn với phần còn lại của hệ thống. Dịch vụ Samsung Pay cũng sử dụng TrustZone để bảo mật thông tin thẻ thanh toán.

Apple Pay hay Samsung Pay sử dụng vùng nhớ bảo mật Secure Enclave hay TrustZone để bảo mật thông tin thẻ thanh toán.

TIÊU CHUẨN XÁC THỰC FIDO/FIDO2

FIDO/FIDO2 BẢO MẬT NHƯ NÀO?

FIDO sử dụng thuật toán bảo mật **ECDSA** mạnh và nhanh hơn so với thuật toán bảo mật **RSA** đang được ứng dụng rộng rãi trong lĩnh vực Hạ tầng khoá công khai (ứng dụng trong Chữ ký số).

Độ dài khóa RSA (bit)	Độ dài khóa ECDSA (bit)
1024	160-223
2048	224-225
3072	256-383
7680	384-511
15360	512+

Bảng 3. *Thực nghiệm cài đặt các lược đồ trên PC và thiết bị USB PKI Token.*

Lược đồ / Môi trường	RSA		ECDSA	
	Sinh chữ ký	Kiểm tra chữ ký	Sinh chữ ký	Kiểm tra chữ ký
PC	62ms	47ms	15ms	16ms
USB PKI Token	2,5s	2s	1s	1s

TIÊU CHUẨN XÁC THỰC FIDO/FIDO2

FIDO/FIDO2 ĐƯỢC ỨNG DỤNG VÀO ĐÂU?

- Trong các hệ thống đăng nhập hiện có như Single Sign-On (SSO) và hệ thống quản lý danh sách người dùng.

- Trong các ứng dụng di động, để cung cấp tính năng xác thực bằng vân tay hoặc nhận dạng khuôn mặt cho người dùng.

- Trong các dịch vụ trực tuyến như các nền tảng mua sắm điện tử, dịch vụ ngân hàng trực tuyến, truy cập nội dung độc quyền...

- Trong các thiết bị IoT…

TIÊU CHUẨN XÁC THỰC FIDO/FIDO2

CÁC TẬP ĐOÀN CÔNG NGHỆ TRÊN THẾ GIỚI ỨNG DỤNG FIDO2:

- Tháng 1/2019, hệ điều hành Android đạt chuẩn FIDO2, hỗ trợ hơn 1 tỷ thiết bị di động.

- Tháng 7/2019, Google kết hợp với Yubico để ra mắt sản phẩm khóa xác thực vân tay chuẩn FIDO2, và hỗ trợ xác thực các dịch vụ của Google.

- Tháng 9/2019, Apple cập nhật trình duyệt Safari, hệ điều hành iOS 13.3 và hệ điều hành MacOS Catalina hỗ trợ khóa bảo mật chuẩn FIDO2 để cải thiện quy trình xác thực cho hệ sinh thái của Apple.

- Tháng 10/2019, Microsoft cũng ứng dụng chuẩn xác thực FIDO2 vào phần mềm Windows Hello, Microsoft Azure AD và sẽ sớm hỗ trợ FIDO2 trong các phiên bản tiếp theo của hệ điều hành Windows.

TIÊU CHUẨN XÁC THỰC FIDO/FIDO2

HỖ TRỢ ĐA NỀN TẢNG

- Win 10+, MAC OS 10.15+, iOS 13.3+, Android 7+
- Browsers: Google Chrome, Microsoft Edge, Mozilla Firefox, Apple Safari

TIÊU CHUẨN XÁC THỰC FIDO/FIDO2

BẢNG SO SÁNH XÁC THỰC FIDO VỚI CÁC XÁC THỰC TRUYỀN THỐNG

	Mật khẩu	Email	OTP	Chữ ký số - PKI	FIDO
Xác thực 2 yếu tố	Không	Có	Có	Có	Có
Phương thức xác thực	Nhập mật khẩu	Xác nhận qua link	Nhập mã số gửi từ SMS hoặc email	Vân tay Khuôn mặt	Vân tay Khuôn mặt
Tính chính xác	Phụ thuộc người dùng	Trung bình	Cao	Cao	Cao
Tính tiện lợi	Thấp nếu sử dụng mật khẩu phức tạp	Trung bình	Trung bình	Thấp	Cao
Tính phổ biến	Có	Có	Có	Có	Đang phổ cập
Độ bảo mật	Phụ thuộc độ phức tạp của mật khẩu	Phụ thuộc phương pháp bảo vệ	Trung bình	Cao	Cao
Khoá bí mật	Không	Không	Không	Có	Có
Tốc độ xác thực	Trung bình	Trung bình	Trung bình	Trung bình	Nhanh
Yêu cầu phần cứng	Không	Không	Không	PKI token	Không

vtcsmarttech
STID nâng cánh giá trị

fido alliance simpler stronger authentication

HỢP TÁC STID – FIDO ALLIANCE

STID là thành viên của liên minh công nghệ FIDO Alliance từ năm 2017

HỢP TÁC STID – FIDO ALLIANCE

Certification

In recognition of SMART TECHNOLOGIES INVESTMENT & DEVELOPMENT JOINT STOCK COMPANY's achievement of FIDO® U2F Certification

Company: SMART TECHNOLOGIES INVESTMENT & DEVELOPMENT JOINT STOCK COMPANY
Product: STID NFC U2F
Specification: Universal Second Factor (U2F)
Specification Version: 1.0 (2014-12-09)
Implementation Class: Authenticator
Transport: NFC
Policy Version: 1.2.5
Interoperability Date: March 9, 2017
Conformance Self-Validation Date: February 23, 2017
Derivative: No
Source Certificate(s): N/A

fido CERTIFIED U2F

Certificate No.
U2F100020170404001

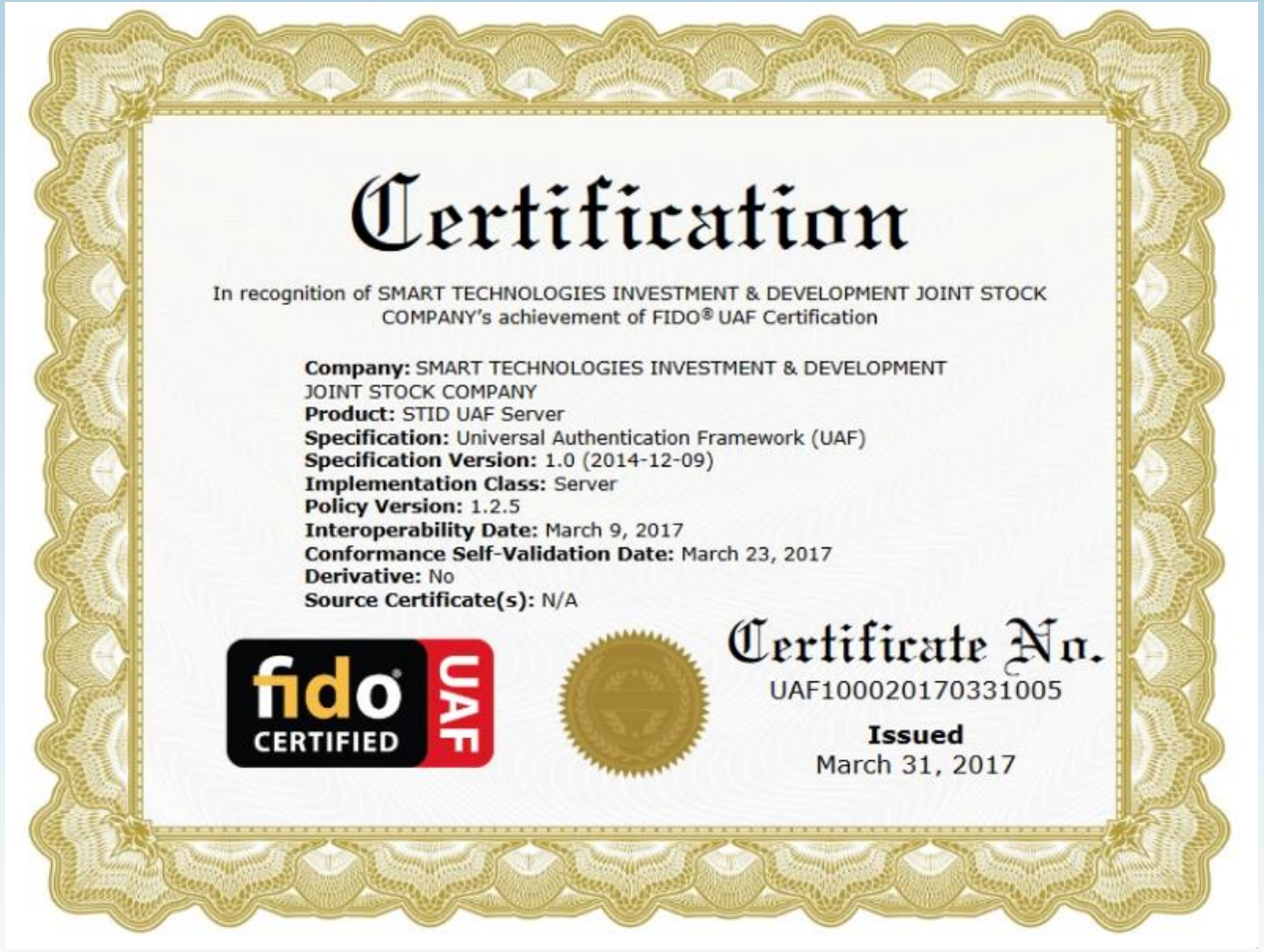
Issued
April 4, 2017

STID đã được FIDO Alliance cấp chứng chỉ cho thiết bị U2F Authenticator (tháng 4 năm 2017)

vtcsmarttech
STID nâng cánh giá trị

fido alliance simpler stronger authentication

HỢP TÁC STID – FIDO ALLIANCE



Certification

In recognition of SMART TECHNOLOGIES INVESTMENT & DEVELOPMENT JOINT STOCK COMPANY's achievement of FIDO® UAF Certification

Company: SMART TECHNOLOGIES INVESTMENT & DEVELOPMENT JOINT STOCK COMPANY
Product: STID UAF Server
Specification: Universal Authentication Framework (UAF)
Specification Version: 1.0 (2014-12-09)
Implementation Class: Server
Policy Version: 1.2.5
Interoperability Date: March 9, 2017
Conformance Self-Validation Date: March 23, 2017
Derivative: No
Source Certificate(s): N/A

fido CERTIFIED UAF

Certificate No.
UAF100020170331005

Issued
March 31, 2017

STID đã được FIDO Alliance cấp chứng chỉ cho UAF Server (tháng 3 năm 2017)

HỢP TÁC STID – FIDO ALLIANCE

Certification

In recognition of Smart Technologies Investment & Development Co., Ltd's achievement of FIDO® Level 1 Certification

Company: Smart Technologies Investment & Development Co., Ltd
Product: STID UAF Client/Authenticator for iOS
Specification: Universal Authentication Framework (UAF)
Specification Version: 1.0 (2014-12-09)
Implementation Class: Client/Authenticator Combo
Level: L1
AAID: 0063#0002
Operating System: iOS
Functional Policy Version: 1.3.3
Authenticator Policy Version: 1.0.0
Security Requirements Version: 1.0.0
Interoperability Date: May 3rd, 2018
Conformance Self-Validation Date: April 13th, 2018
Vendor Questionnaire Approval Date: July 30th, 2018

fido CERTIFIED L1 UAF

Certificate No.
UAF100020180801001
Issued
August 1st, 2018

STID đã được FIDO Alliance cấp chứng chỉ cho iOS UAF Client/Authenticator L1 (tháng 8 năm 2018)

HỢP TÁC STID – FIDO ALLIANCE

Certification

In recognition of SMART TECHNOLOGIES INVESTMENT & DEVELOPMENT JOINT STOCK COMPANY's achievement of FIDO® Level 1 Certification

Company: SMART TECHNOLOGIES INVESTMENT & DEVELOPMENT JOINT STOCK COMPANY
Product: STID UAF Client/Authenticator for Android
Specification: Universal Authentication Framework (UAF)
Specification Version: 1.0 (2014-12-09)
Implementation Class: Client / Authenticator Combo
Level: L1
AAID: 0063#0001
Operating System: Android
Functional Policy Version: 1.3.3
Authenticator Policy Version: 1.0.0
Security Requirements Version: 1.0.0
Interoperability Date: May 3rd, 2018
Conformance Self-Validation Date: April 13th, 2018
Vendor Questionnaire Approval Date: October 22nd, 2018

fido CERTIFIED UAF L1

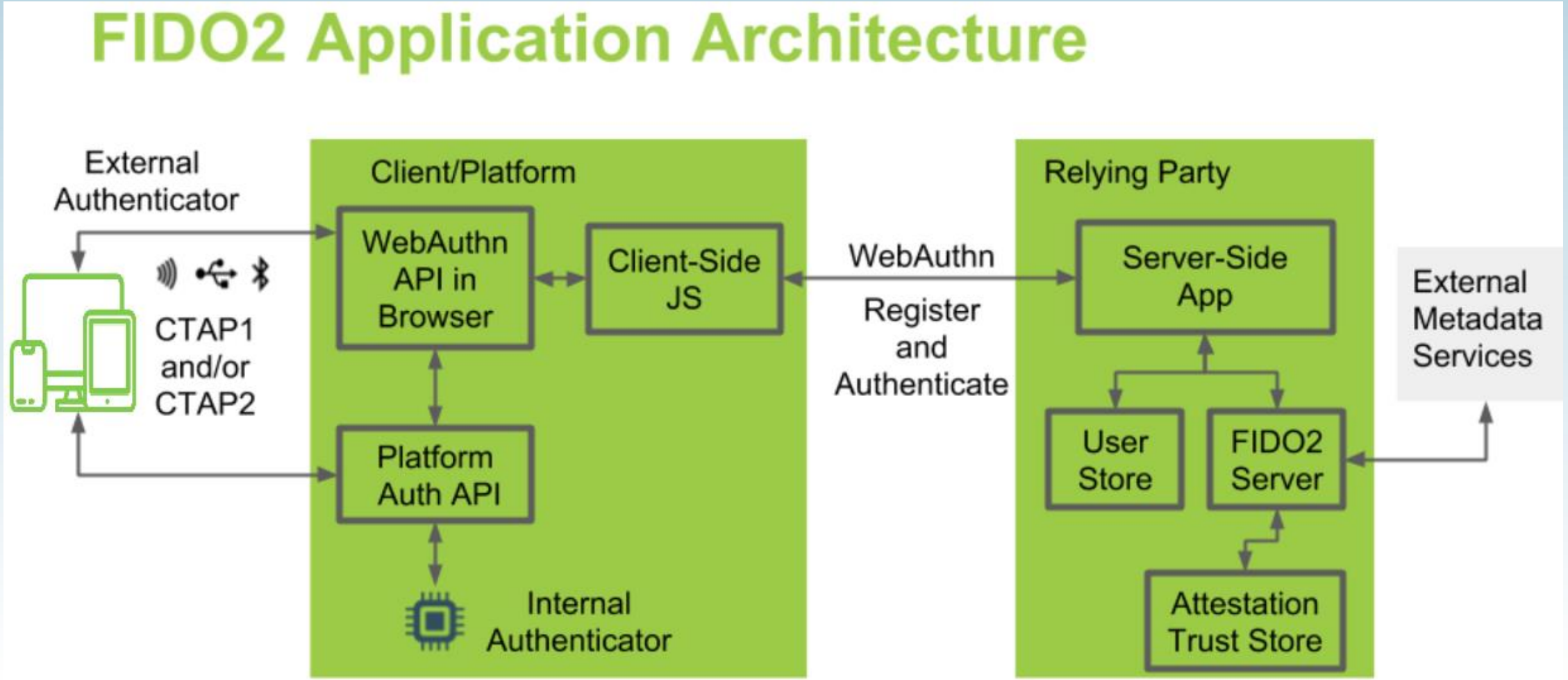
Certificate No.
UAF100020181024001
Issued
October 24th, 2018

STID đã được FIDO Alliance cấp chứng chỉ cho Android UAF Client/Authenticator L1 (tháng 10 năm 2018)

https://fidoalliance.org/certification/fido-certified-products/

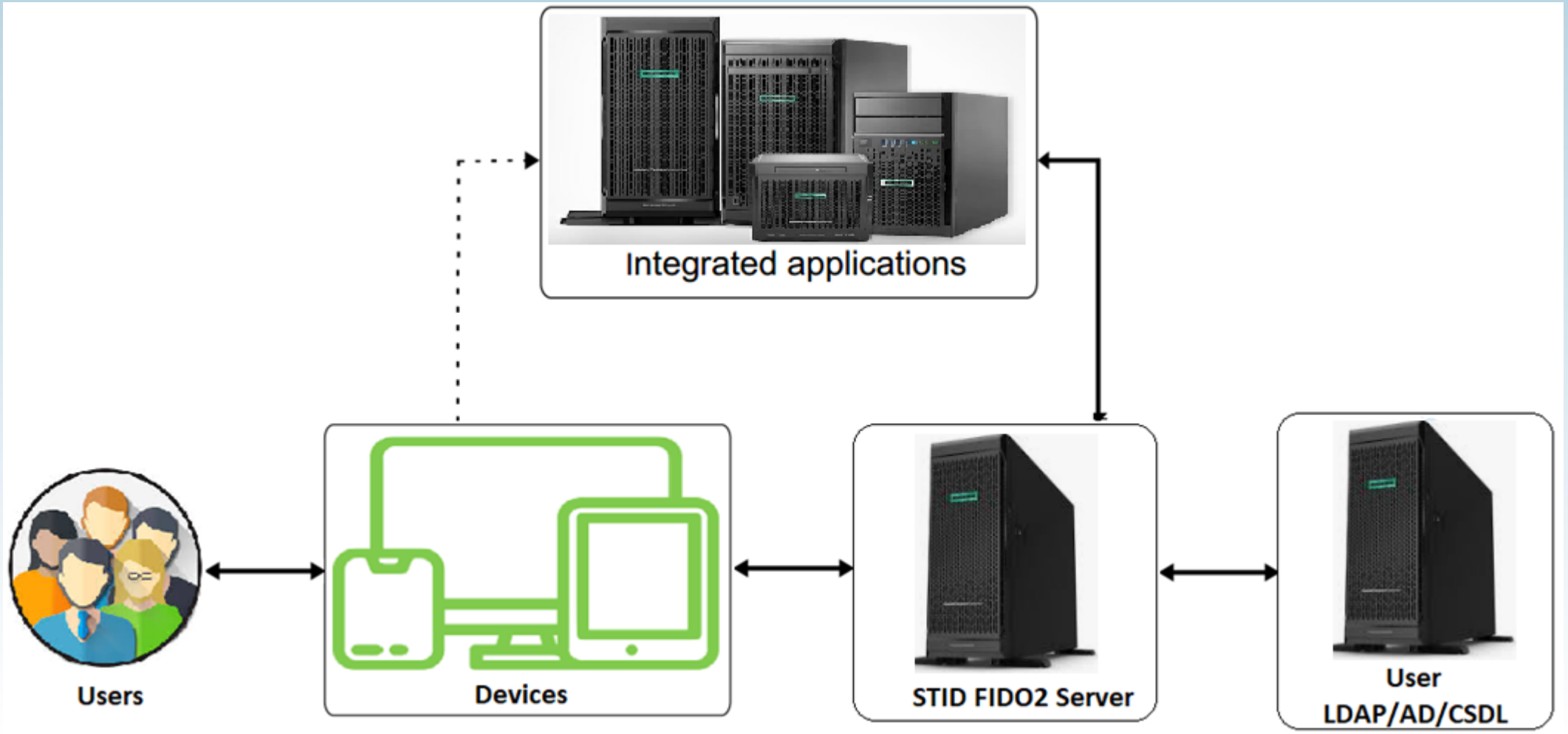
TÍCH HỢP HỆ THỐNG

MÔ HÌNH KIẾN TRÚC



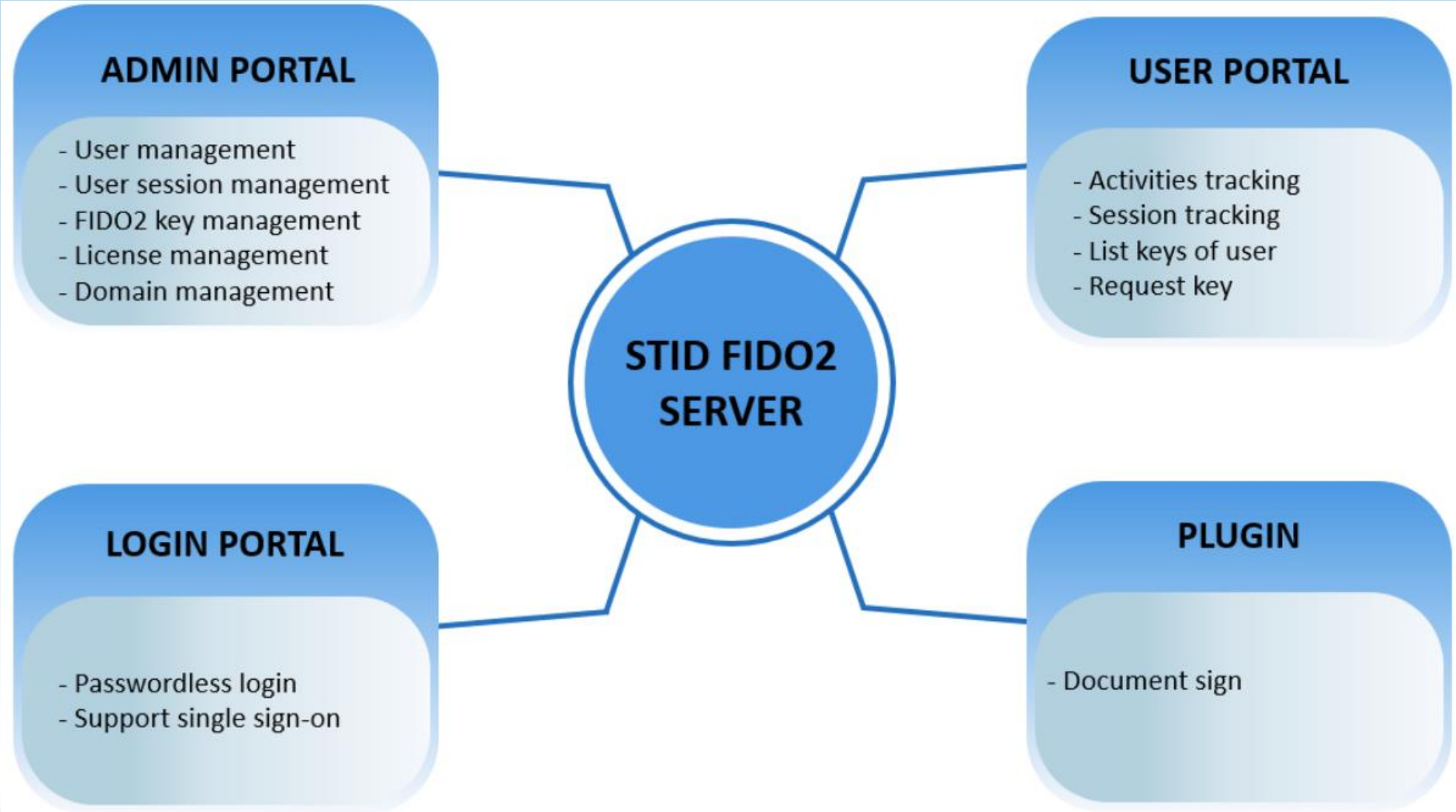
TÍCH HỢP HỆ THỐNG FIDO2

MÔ HÌNH HỆ THỐNG



TÍCH HỢP HỆ THỐNG FIDO2

CHỨC NĂNG HỆ THỐNG STID FIDO2 SERVER



TÍCH HỢP HỆ THỐNG FIDO2

CÁC BƯỚC TÍCH HỢP

1. **Liên kết ứng dụng với FIDO2 Server thông qua API**: cấu hình liên kết FIDO2 Server, kết nối FIDO2 với tài khoản ứng dụng của người dùng, tích hợp vào quy trình quản lý của ứng dụng để có thể thêm, xóa hoặc cập nhật thông tin FIDO2 của người dùng.

2. **Đăng ký tài khoản FIDO2**: ứng dụng sẽ chuyển yêu cầu đăng ký đến FIDO2 Server, người dùng sử dụng một thiết bị xác thực (FIDO2 key, điện thoại, máy tính,...) để thực hiện quá trình đăng ký FIDO2.

3. **Yêu cầu đăng nhập**: khi người dùng tạo yêu cầu đăng nhập, ứng dụng sẽ chuyển yêu cầu đăng nhập đến FIDO2 Server, cùng với thông tin về ứng dụng hoặc dịch vụ được yêu cầu truy cập và các thông tin xác thực của người dùng. FIDO2 Server sẽ tạo yêu cầu xác thực.

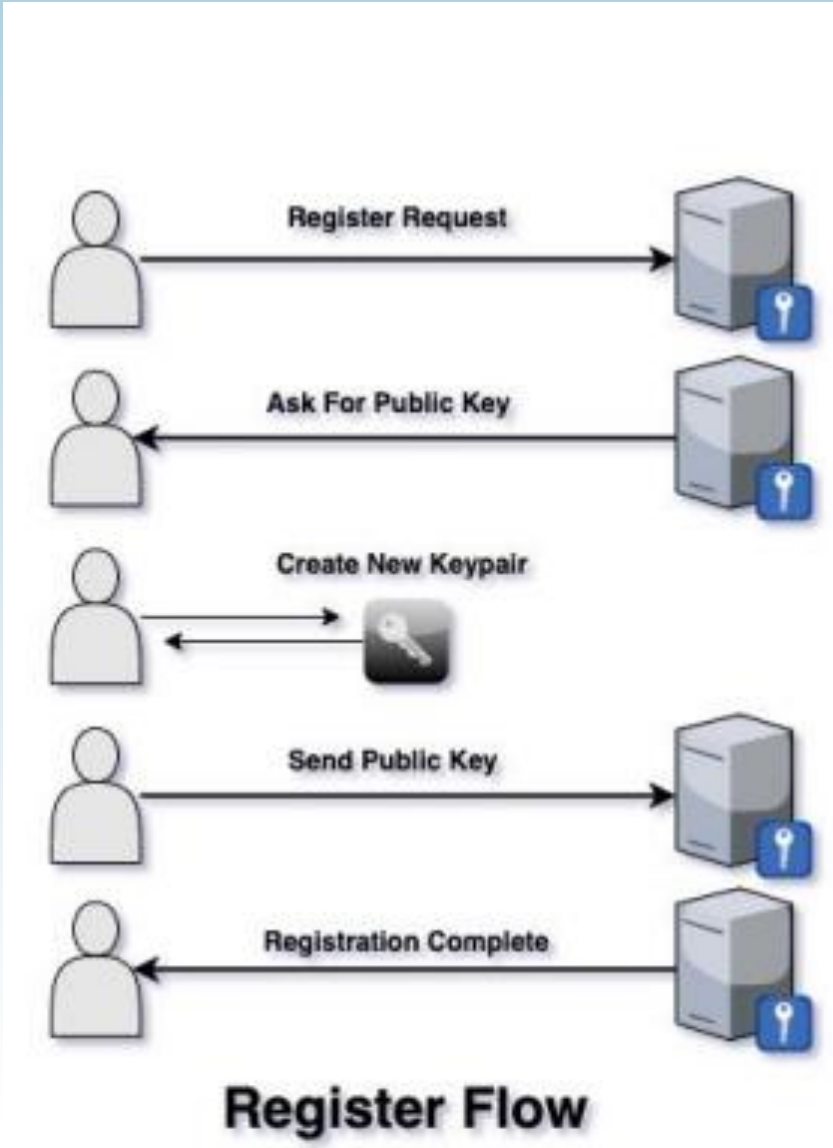
TÍCH HỢP HỆ THỐNG FIDO2

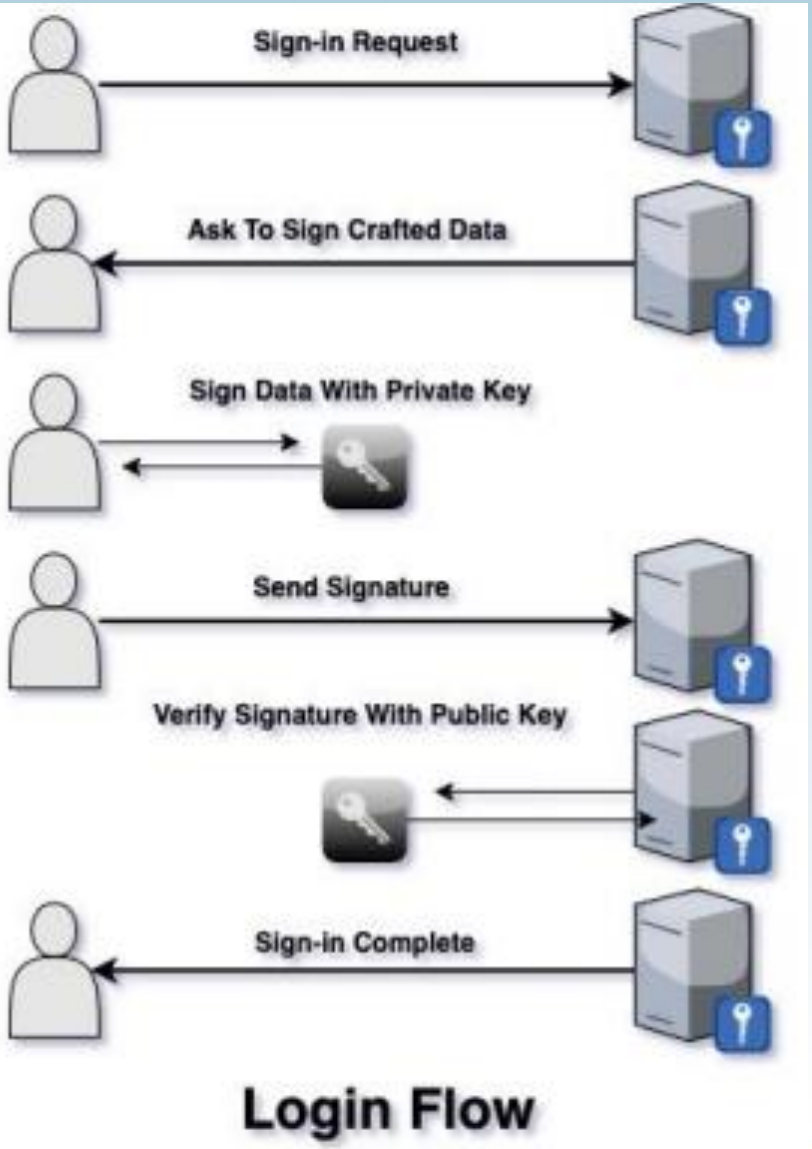
CÁC BƯỚC TÍCH HỢP

4. **Xác thực đăng nhập**: người dùng sử dụng một trong các thiết bị xác thực FIDO2 đã đăng ký để xác thực. FIDO2 Server sẽ xác minh thông tin cùng với yêu cầu xác thực FIDO2. Nếu xác thực thành công, FIDO2 Server sẽ cấp phép truy cập cho người dùng vào ứng dụng hoặc dịch vụ được yêu cầu.

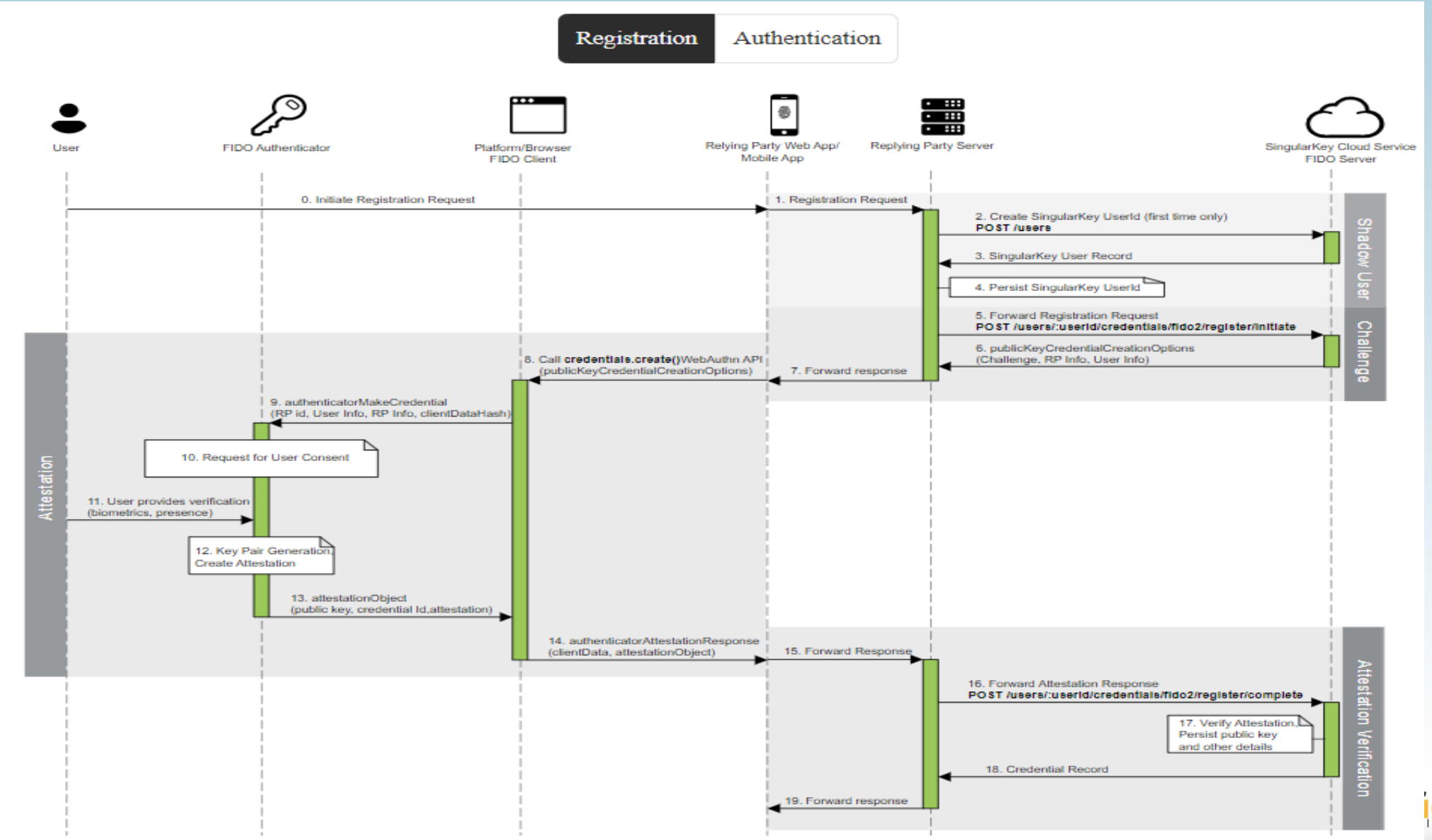
5. **Thực hiện đăng xuất**: khi người dùng hoàn thành việc sử dụng ứng dụng hoặc dịch vụ, ứng dụng sẽ thực hiện đăng xuất và hủy bỏ phiên làm việc của người dùng.

TÍCH HỢP HỆ THỐNG FIDO2

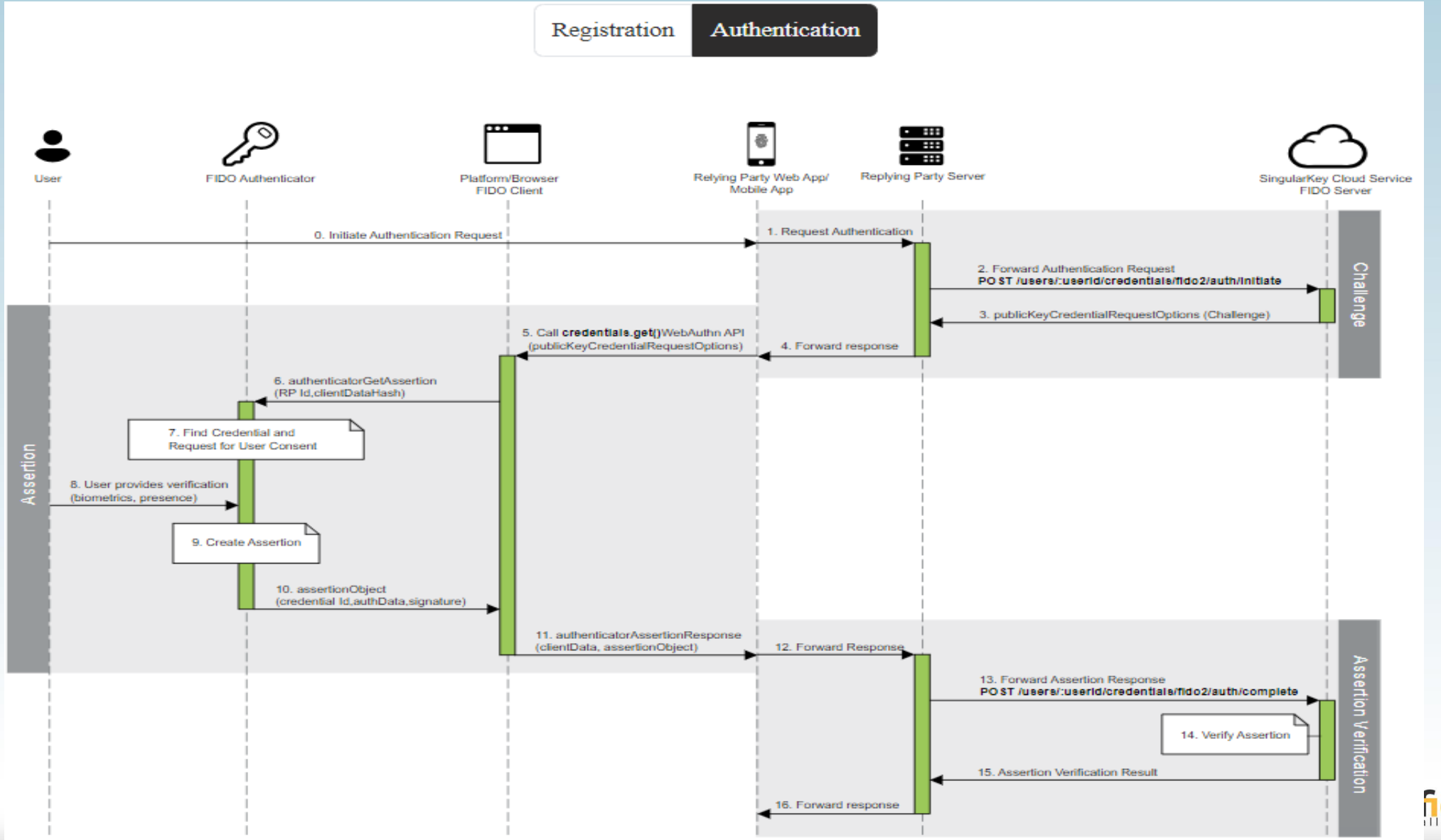




TÍCH HỢP HỆ THỐNG FIDO2



TÍCH HỢP HỆ THỐNG FIDO2



TÍCH HỢP HỆ THỐNG FIDO2

XEM DEMO

TRÂN TRỌNG CẢM ƠN!

www.vtcsmarttech.com.vn