



XÁC THỰC NHANH FIDO



**CÔNG TY TNHH ĐẦU TƯ VÀ PHÁT TRIỂN
CÔNG NGHỆ THÔNG MINH**

www.vtcsmarttech.com.vn

TỔNG QUÁT

- 1 CÁC VẤN ĐỀ XÁC THỰC HIỆN NAY
- 2 TIÊU CHUẨN XÁC THỰC FIDO
- 3 HỢP TÁC STID - FIDO
- 4 GIẢI PHÁP TÍCH HỢP

CÁC VẤN ĐỀ CỦA XÁC THỰC HIỆN NAY

XÁC THỰC ĐANG LÀ VẤN ĐỀ LỚN CỦA CHÚNG TA

AUTHENTICATION IS OUR BIGGEST PROBLEM 

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*

Fortune
LinkedIn Lost 167 Million Account Credentials in Data
Breach

The Register
Sensitive client emails, usernames,
passwords exposed in Deloitte hack

Mashable
Someone is selling 33 million Twitter
passwords on the dark web

ars technica
Cluster of “megabreaches” compromises
a whopping 642 million passwords

2 All Rights Reserved | FIDO Alliance | Copyright 2018

The New York Times

***Russian Hackers Amass Over
a Billion Internet Passwords***

By Nicole Perlroth and David Gelles

Aug. 5, 2014

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

How the Eurograbber attack stole 36 million euros

SmartNA, PortPlus - High Performance Visibility Solutions that scale with your network.

Check Point has revealed how a sophisticated malware attack was used to steal an estimated 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

Tấn công vật lý có thể diễn ra đối với thiết bị thất lạc hoặc bị đánh cắp

5

Tấn công vật lý vào thiết bị của người dùng nhằm đánh cắp dữ liệu để mạo danh

6

Tấn công vật lý vào thiết bị của người dùng nhằm lạm dụng chính thiết bị để mạo danh

2

Tấn công từ xa trên số lượng lớn thiết bị người dùng

Nhằm đánh cắp dữ liệu để mạo danh người dùng

3

Tấn công từ xa trên số lượng lớn thiết bị người dùng

Nhằm lạm dụng thông tin người dùng để mạo danh

4

Tấn công từ xa trên số lượng lớn thiết bị người dùng

Nhằm lạm dụng phiên xác thực để mạo danh

1

Tấn công từ xa đến máy chủ trung tâm để đánh cắp thông tin người dùng hàng loạt nhằm mục đích mạo danh

Tấn công diện rộng

CÁC VẤN ĐỀ CỦA XÁC THỰC HIỆN NAY

Ransomware cyberattacks span globe

Below are the top 20 countries affected in the first few hours of WannaCry's ransomware cyberattack.

■ More than 70,000 attacks ■ More than 4,000 attacks ■ Less than 4,000 attacks



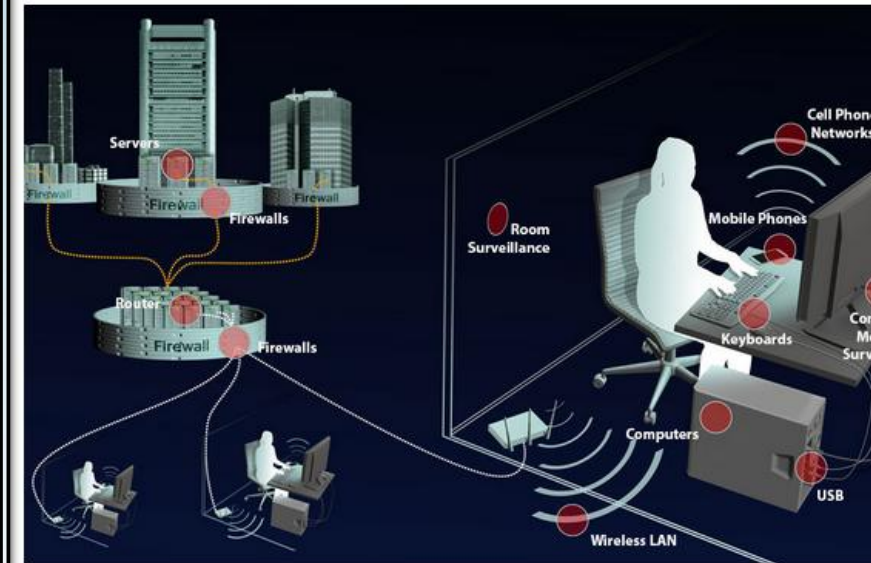
SOURCES: Kaspersky Lab

AP

An ninh mạng hay an toàn dữ liệu cho Việt Nam?

11/05/2018 08:00 - **Hào Linh**

Việt Nam không thể chống đỡ những cuộc tấn công của các nhóm tin tặc chuyên nghiệp và được sự hậu thuẫn của chính phủ các nước khác nếu không thể làm chủ được các thiết bị phần cứng và phần mềm trong hệ thống mạng.



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-
Nghệ 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.

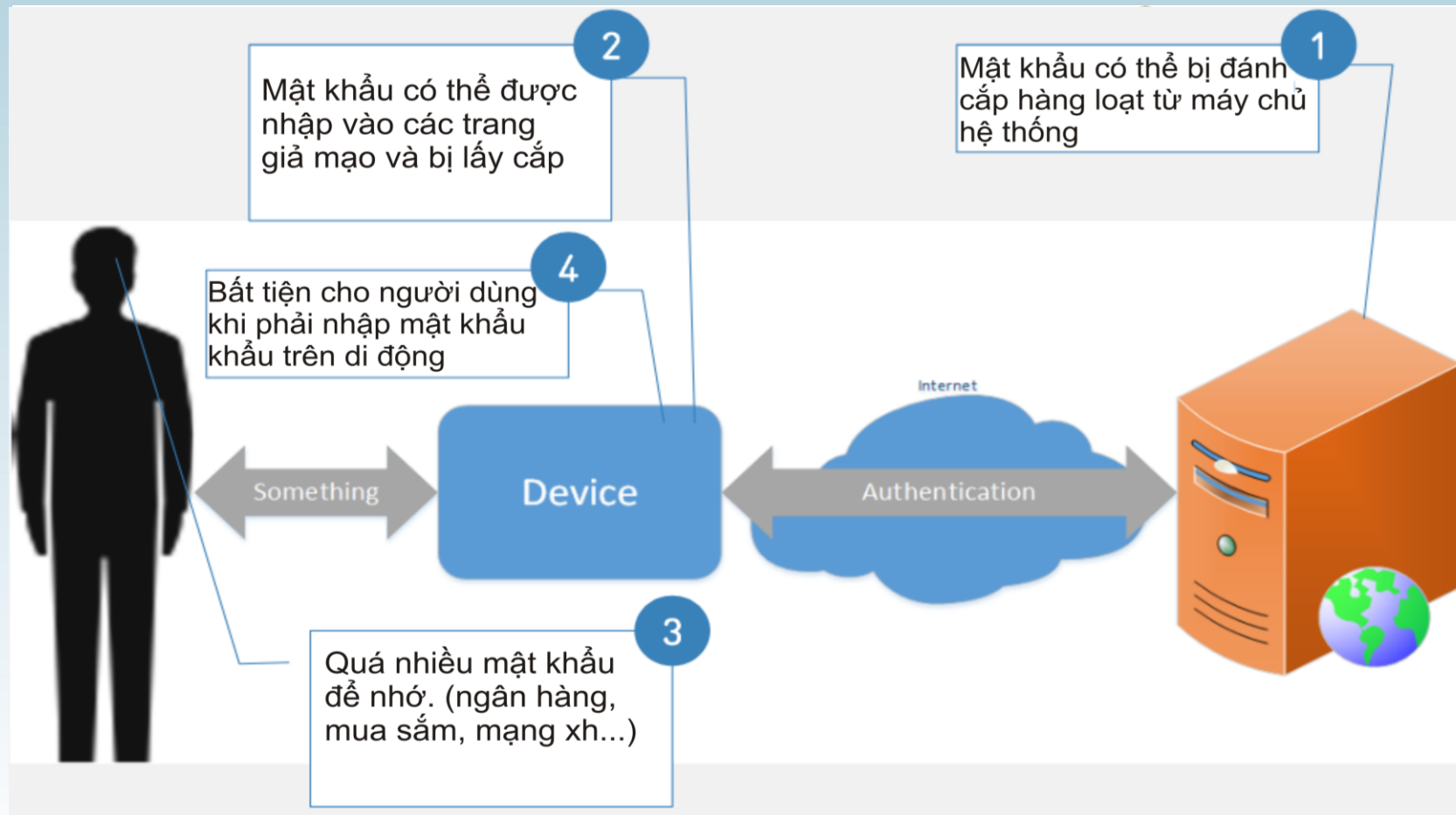
Theo cục Viễn thông (bộ Thông tin và Truyền thông), tỷ lệ người dùng internet tại Việt Nam đã đạt 53% trên tổng dân số. Việt Nam đứng vị trí thứ 16 trong top 20 quốc gia có số người sử dụng internet nhiều nhất tại Châu Á và độ tuổi người sử dụng đa phần là người trẻ, chiếm hơn 50% so với tổng dân số.

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”*

CÁC VẤN ĐỀ CỦA XÁC THỰC HIỆN NAY

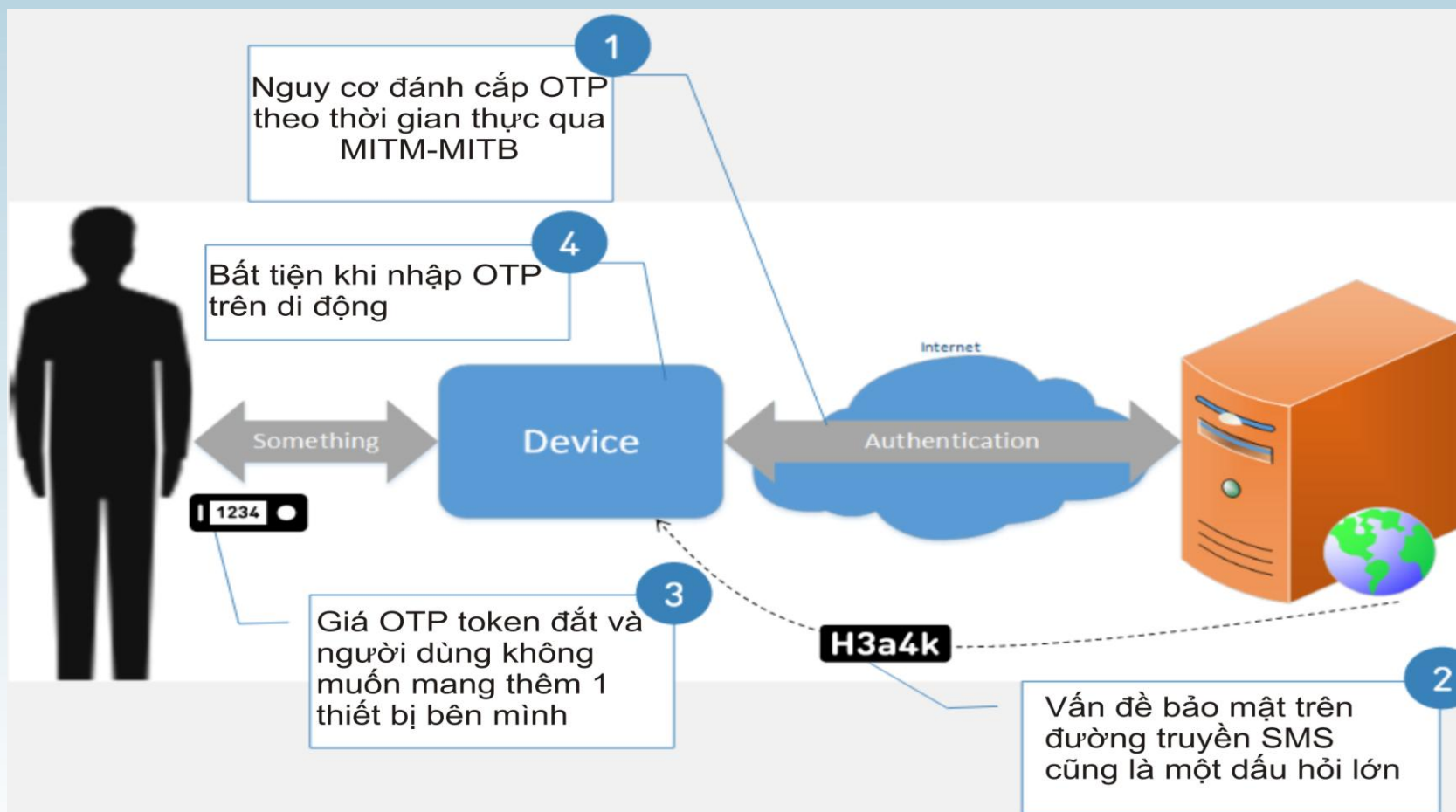
NHỮNG VẤN ĐỀ ĐỐI VỚI LƯU TRỮ VÀ XÁC THỰC TRUYỀN THỐNG



Xác thực bằng Password và lưu trữ bằng Cloud

CÁC VẤN ĐỀ CỦA XÁC THỰC HIỆN NAY

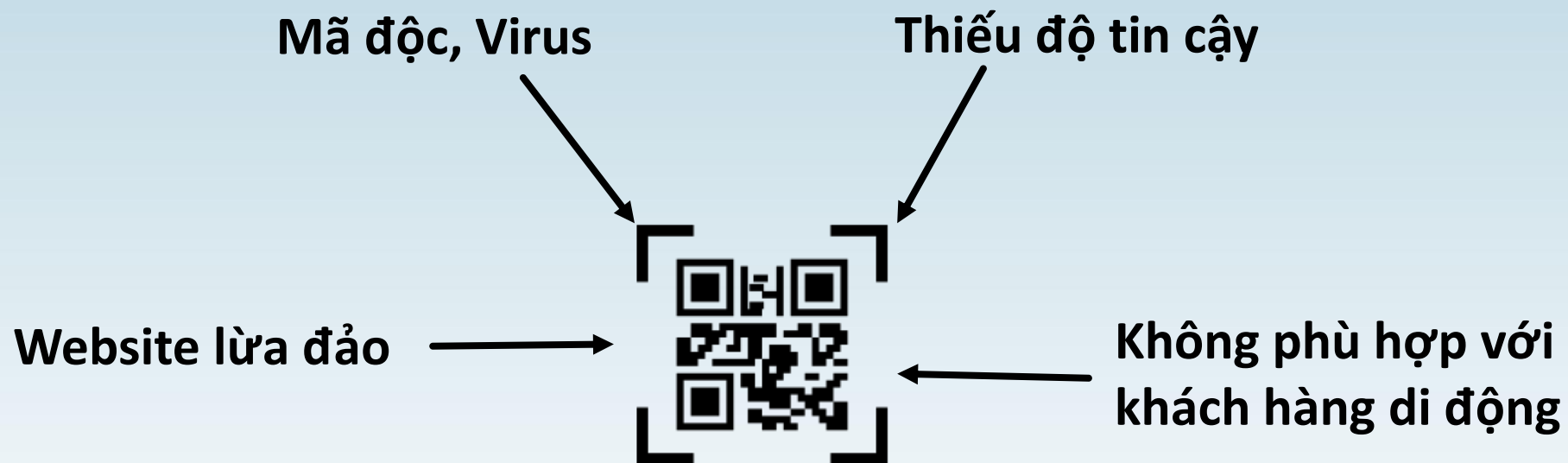
NHỮNG VẤN ĐỀ ĐỐI VỚI LƯU TRỮ VÀ XÁC THỰC TRUYỀN THÔNG



Xác thực với 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 với QR Code

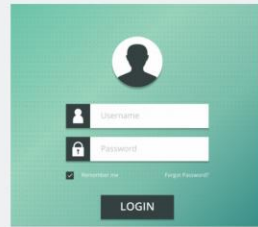
CÁC VẤN ĐỀ CỦA XÁC THỰC HIỆN NAY

NHỮNG VẤN ĐỀ CẦN ĐẾN XÁC THỰC HÀNG 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.

NHỮNG VẤN ĐỀ CẦN ĐẾN XÁC THỰC

1
Bạn có muốn đăng nhập?



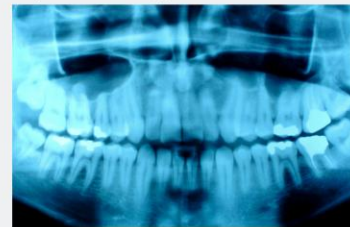
2
Bạn có muốn xóa tất cả email của bạn?



3
Bạn có muốn đổi địa chỉ nhận hàng?



4
Bạn có muốn chia sẻ thông tin về phim chụp nha khoa?



5
Bạn có muốn chuyển tiền cho bố/ mẹ mình?



6
Bạn có muốn chuyển khoản đến trang lazada.vn, tiki.vn,... để mua hàng trực tuyến?



=> 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 không đồng bộ, OTP HW 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.

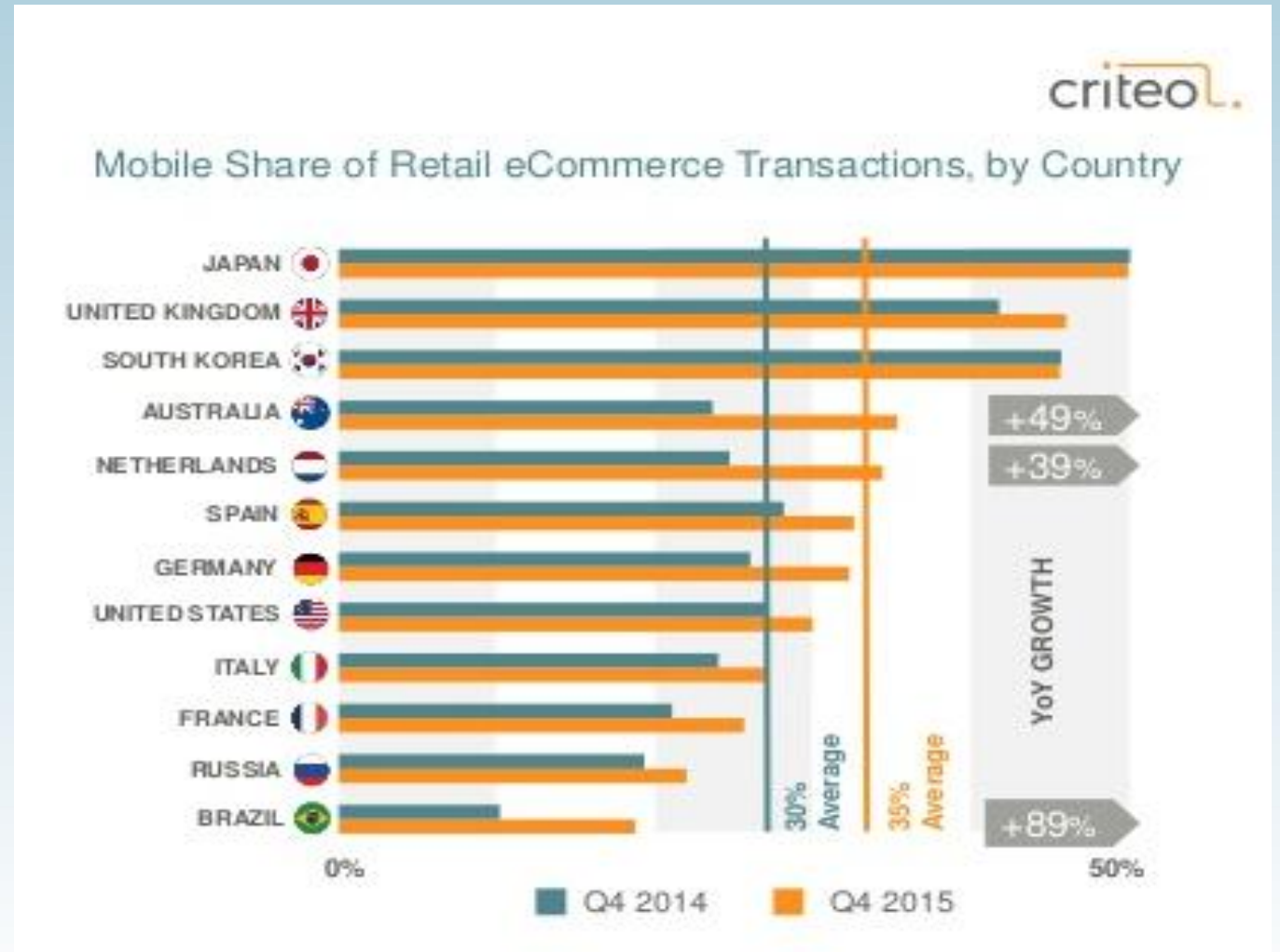
CÁC VẤN ĐỀ CỦA XÁC THỰC HIỆN NAY

- Dự kiến có 770 triệu ứng dụng có bảo mật sinh trắc học được tải về vào năm 2019.

- Báo cáo từ “Human Interface & Biometric Technologies: Emerging Ecosystems, Opportunities & Forecasts 2014-2019” cho thấy:

- * Xu hướng kết hợp TouchID của Apple và NFC trong thanh toán.

- * Những công nghệ sinh trắc học sẽ được xuất hiện ở các dòng điện thoại tầm trung trong tương lai gần.



Nguồn: Criteo, State of Mobile Commerce Report 4Q 2015

CÁC VẤN ĐỀ CỦA XÁC THỰC HIỆN NAY

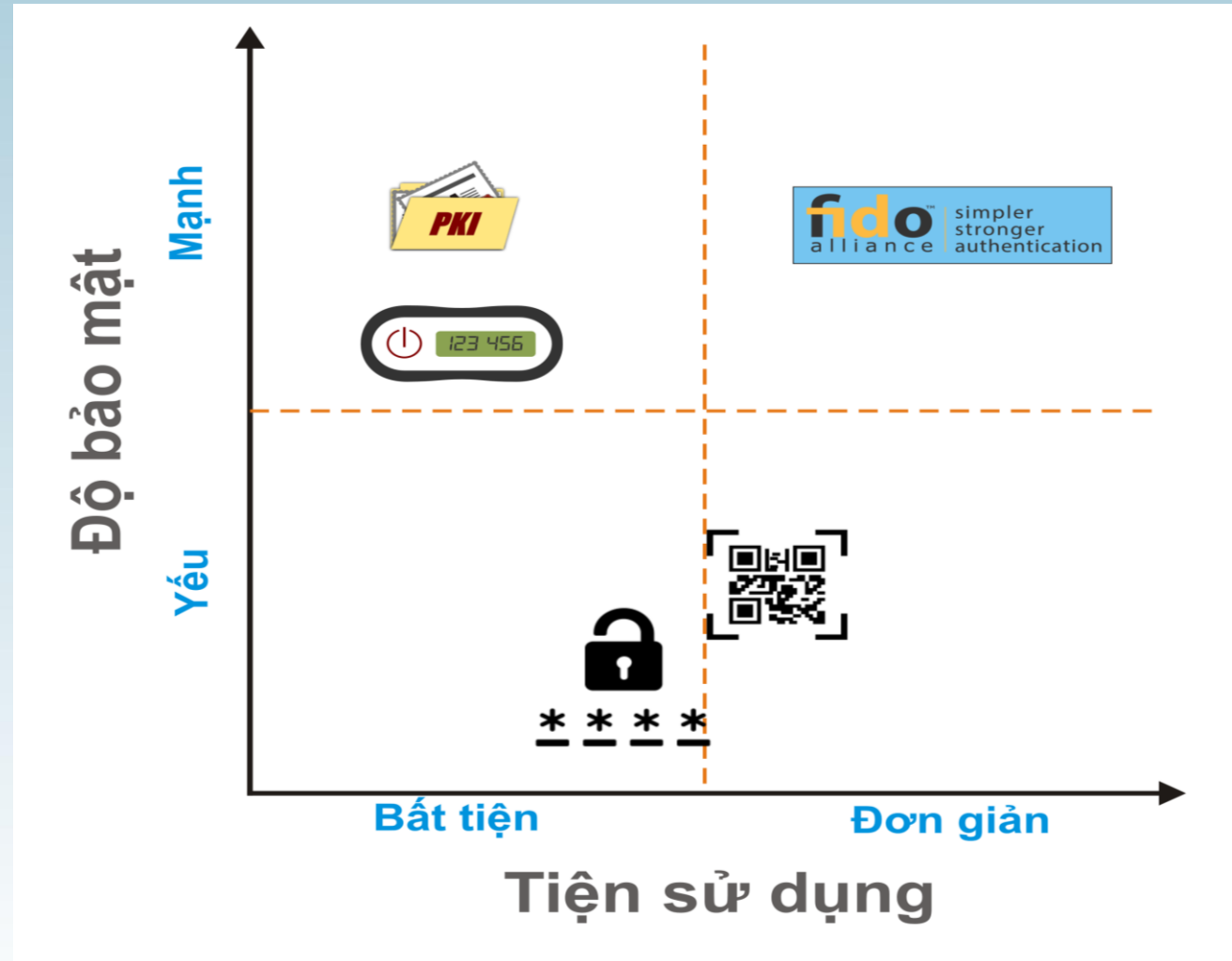


Chúng ta cần một mô hình mới!



Tiêu chuẩn xác thực Fast IDentity Online

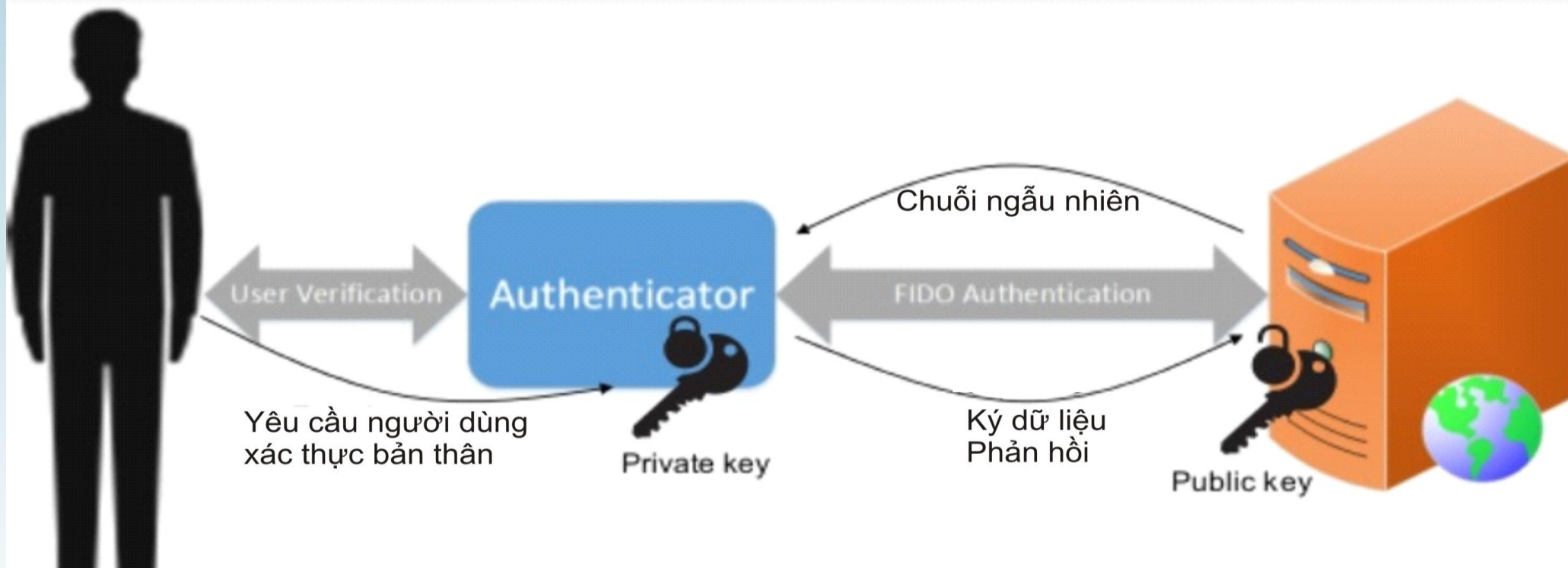
TIÊU CHUẨN XÁC THỰC FIDO



MỤC TIÊU CỦA FIDO

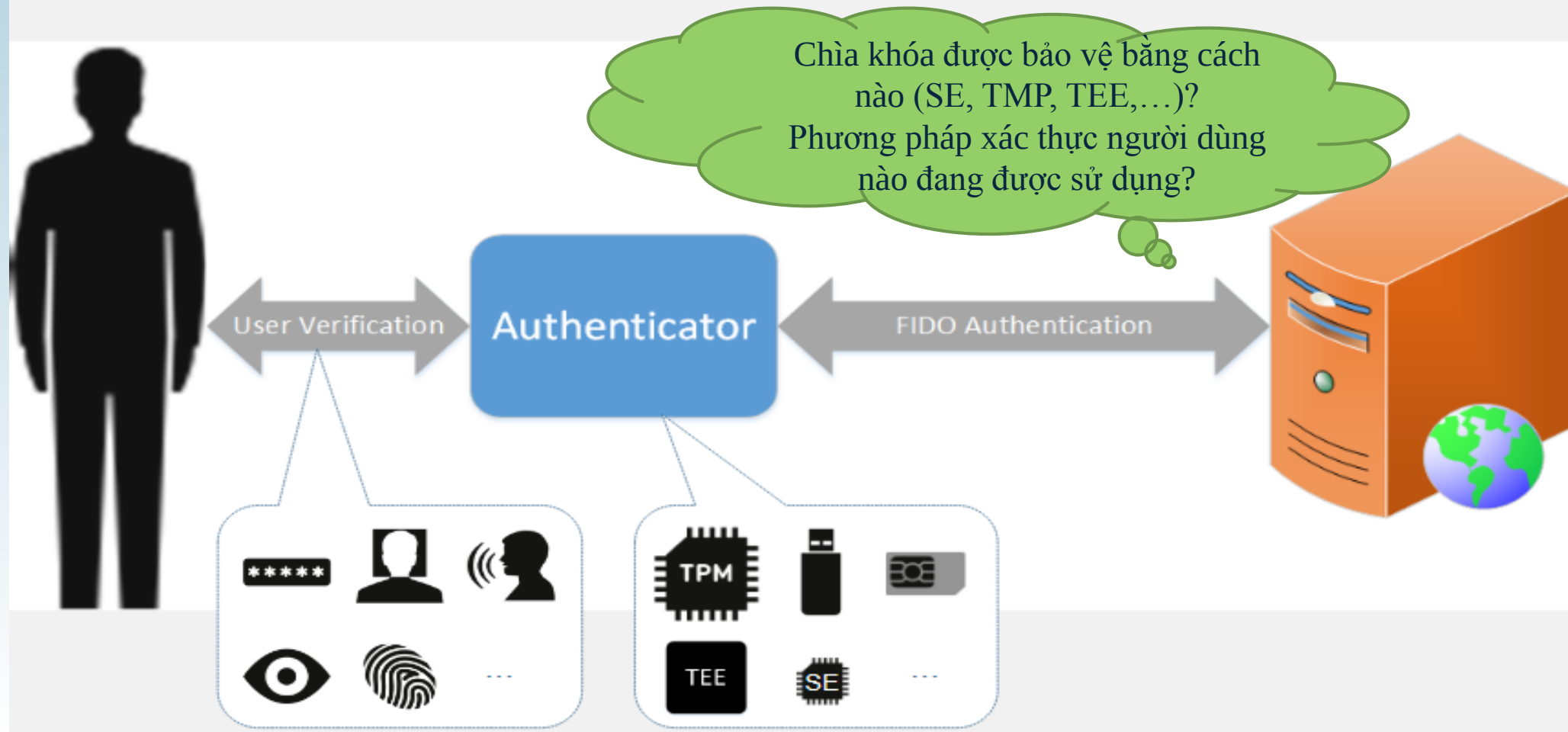
TIÊU CHUẨN XÁC THỰC FIDO

FIDO hoạt động như thế nào?



TIÊU CHUẨN XÁC THỰC FIDO

FIDO hoạt động như thế nào?



TIÊU CHUẨN XÁC THỰC FIDO

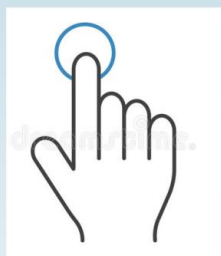
XÁC THỰC ĐƠN GIẢN HƠN

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

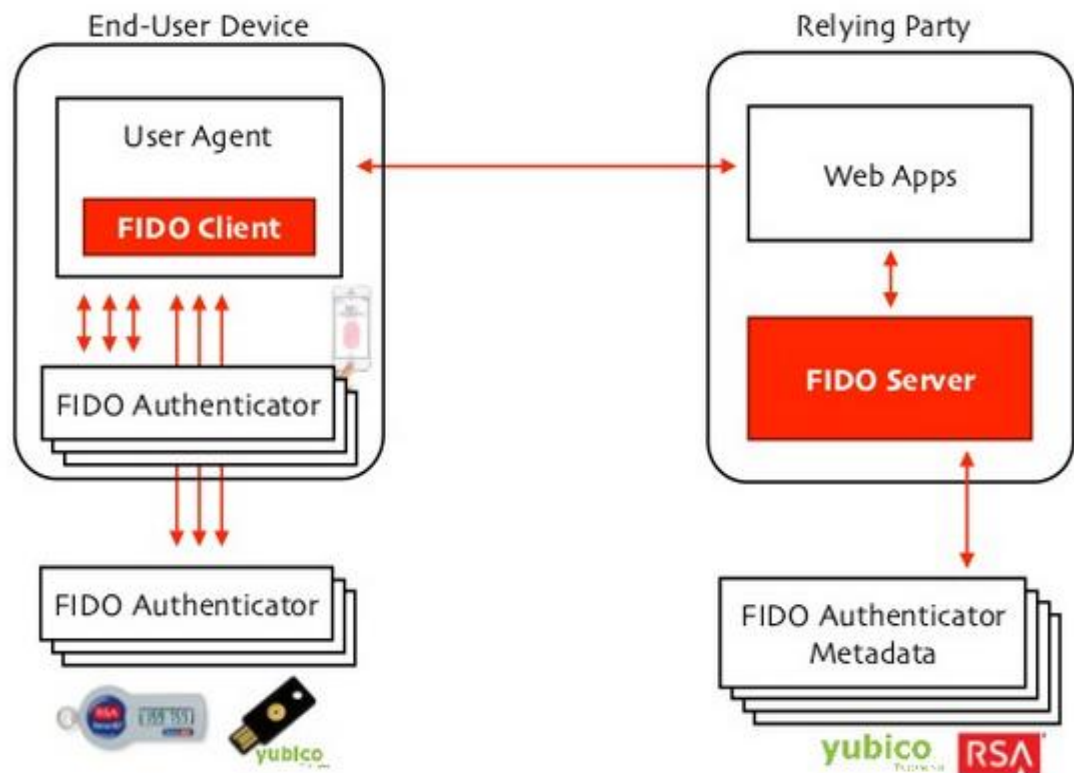
TIÊU CHUẨN XÁC THỰC FIDO

XÁC THỰC AN TOÀN HƠN

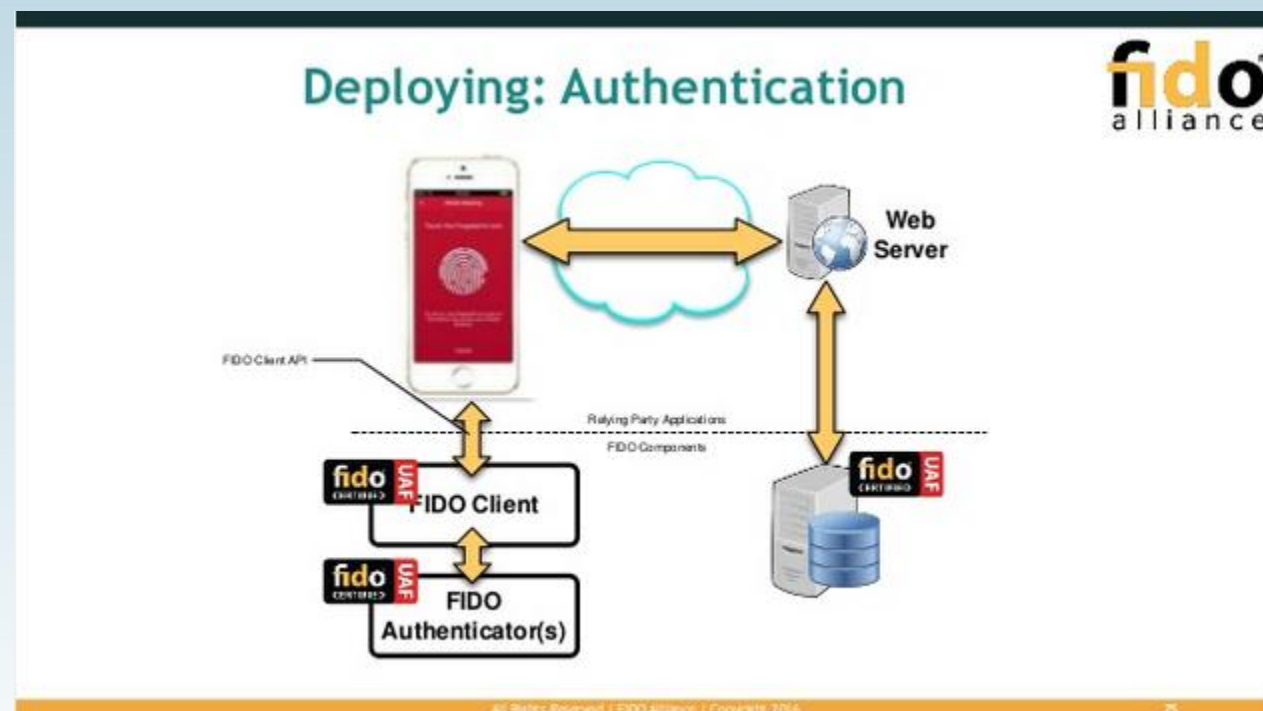


TIÊU CHUẨN XÁC THỰC FIDO

FIDO U2F 1.x



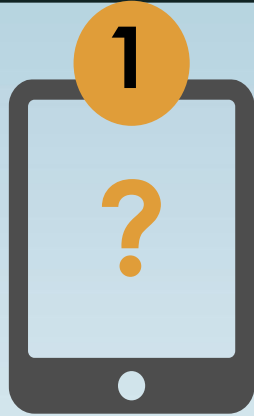
FIDO UAF 1.x



TIÊU CHUẨN XÁC THỰC FIDO

Quy trình xác thực với FIDO

Passwordless Experience (UAF Standards) – Xác thực không mật khẩu



Yêu cầu xác thực



Xác thực vân tay*



Xác thực trực tuyến

Second Factor Experience (U2F Standards) – Xác thực 2 lớp



Xác thực với Username/Password



Cắm thiết bị* / Nhấn nút



Xác thực trực tuyến

TIÊU CHUẨN XÁC THỰC FIDO

HỖ TRỢ ĐA NỀN TẢNG VÀ CÁC DỊCH VỤ TRỰC TUYẾN

FIDO CROSS-PLATFORM SUPPORT



SAMPLE: FIDO-ENABLED SERVICES



AVAILABLE TO PROTECT
3.5 BILLION+
ACCOUNTS WORLDWIDE



TIÊU CHUẨN XÁC THỰC FIDO

CÁC THIẾT BỊ HÀNG ĐẦU SỬ DỤNG CÔNG NGHỆ FIDO

QUALCOMM

SAMSUNG



S5, Mini



Alpha



Note 4,5



Note Edge



Tab S,
Tab S2



S6,
S6 Edge



S7,
S7 Edge



Vernee
Thor

SHARP



Aquos Zeta

SONY



Xperia Z5



Xperia Z5
Compact



Xperia Z5
Premium

LG Electronics



V1
0



G5

FUJITSU



Arrows
NX



Arrows
Fit



Arrows
Tab

HUAWEI



Mate 8

Lenovo



Phab2 Pro
Phab2 Plus

ZUK
a Lenovo company



Z2, Z2 Pro

TIÊU CHUẨN XÁC THỰC FIDO

CÁC ỨNG DỤNG FIDO CŨNG HỖ TRỢ TRÊN SẢN PHẨM APPLE

Supported iOS Fingerprint Devices

Bank of America.

NTT
docomo

ebay™



iPhone SE



iPhone



iPhone+



iPhone 8, X



iPad Air



iPad Mini



iPad Pro

TIÊU CHUẨN XÁC THỰC FIDO

1. Hỗ trợ: Windows, Linux, MacOS, nhiều phương thức xác thực (thiết bị keychain, điện thoại di động, đầu đọc vân tay, ...) và các phương pháp truyền thông khác nhau (USB, NFC, Bluetooth).
2. Hỗ trợ cho các dịch vụ tài chính và Internet hàng đầu (Google, Bank of America và hơn 250 công ty trong liên minh FIDO). U2F/UAF cho phép mọi nhà cung cấp dịch vụ trở thành nhà cung cấp dịch vụ nhận dạng độc lập, hoặc cho phép người dùng xác thực thông qua một nhà cung cấp dịch vụ liên kết.
3. Một thiết bị U2F/UAF tạo ra cặp khóa mới cho mỗi dịch vụ, khoá công khai chỉ được lưu trữ trên dịch vụ cụ thể mà nó kết nối. Vì vậy, không có bí mật nào được chia sẻ giữa các nhà cung cấp dịch vụ.
4. Xác thực hai yếu tố, sử dụng nền tảng khóa công khai và hỗ trợ trình duyệt (Chrome,...), chống lừa đảo, chiếm quyền kiểm soát riêng, tấn công và các phần mềm độc hại. Dễ dàng sử dụng, xác thực nhanh, không cần phải cài đặt.
5. Đảm bảo khả năng nhận diện cao, ràng buộc thiết bị với danh tính người dùng.
6. Nhà cung cấp dịch vụ không tốn chi phí và hỗ trợ phân phối thiết bị U2F/UAF. Người dùng có thể chọn các thiết bị phù hợp từ nhiều nhà cung cấp (NFC, USB Touch, thiết bị di động...).



HỢP TÁC STID - FIDO



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

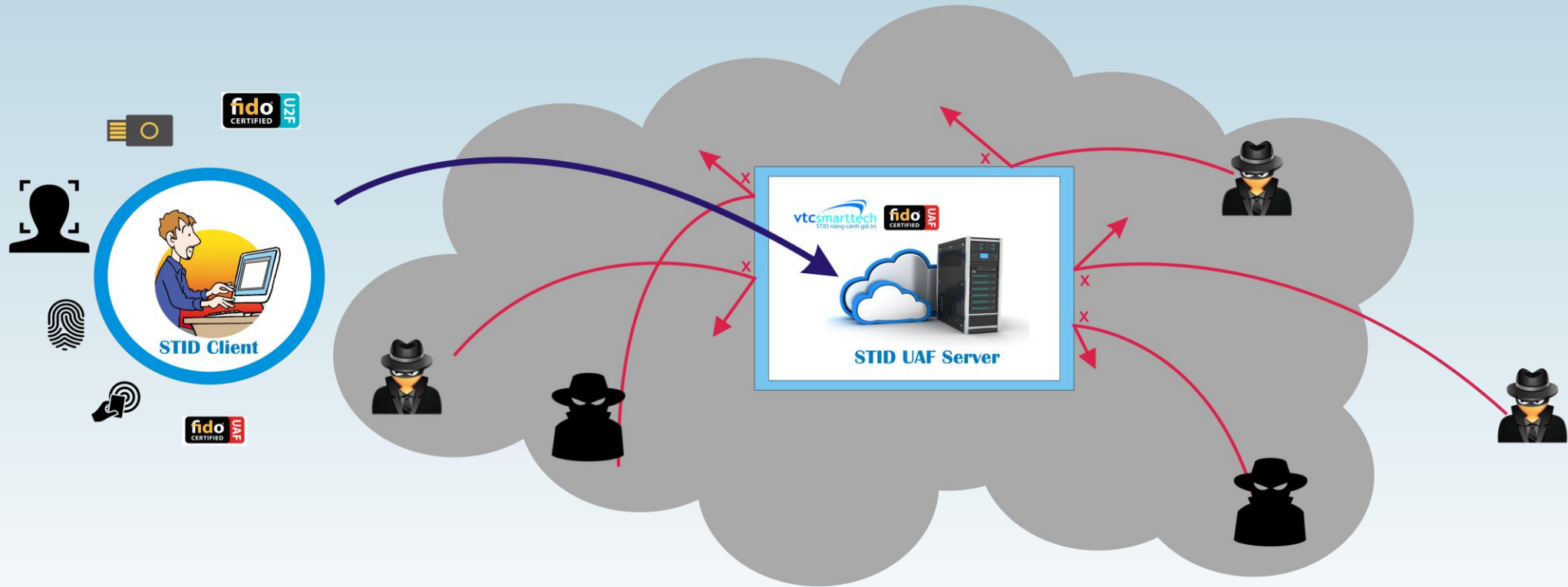
HỢP TÁC STID - FIDO



STID đã được FIDO Alliance cấp chứng chỉ cho U2F Authenticator (tháng 3 năm 2017)

GIẢI PHÁP TÍCH HỢP

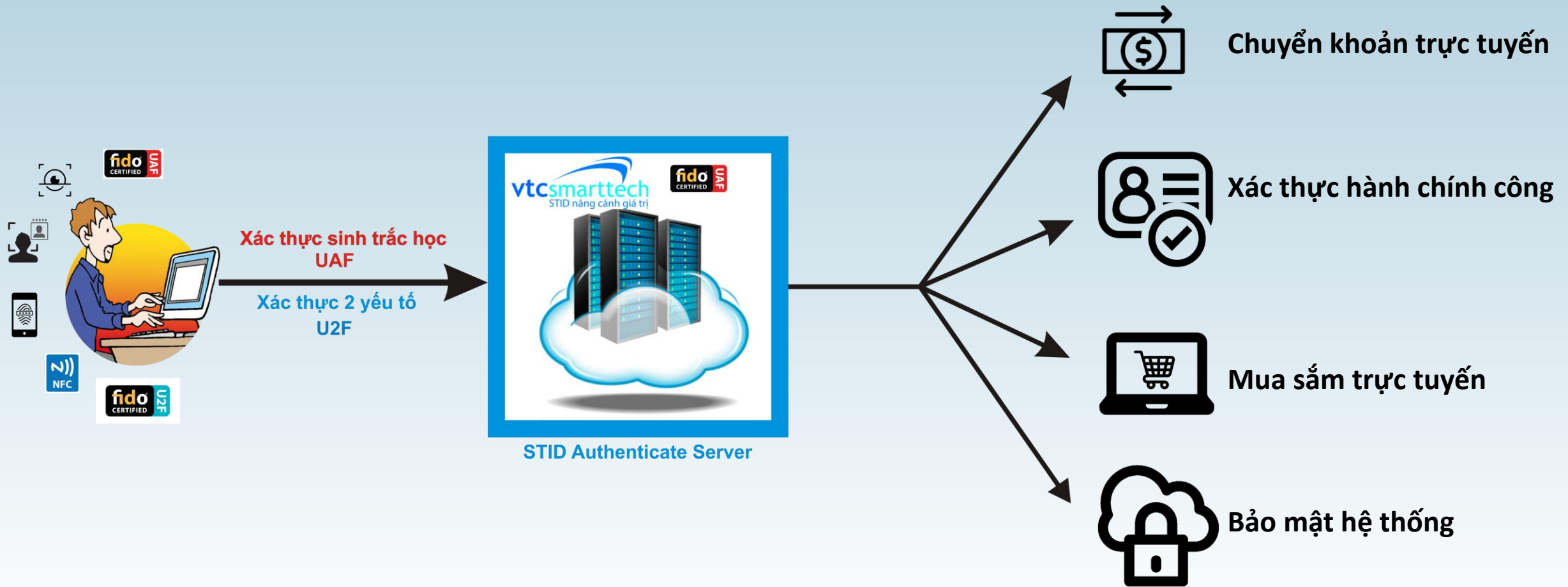
STID FIDO SERVER VÀ STID FIDO CLIENT/AUTHENTICATOR



STID mang sứ mệnh bảo vệ an toàn cho người dùng trực tuyến

GIẢI PHÁP TÍCH HỢP

DỊCH VỤ TRỰC TUYẾN TỪ STID FIDO U2F/UAF



GIẢI PHÁP TÍCH HỢP

GIẢI PHÁP CHUYỂN KHOẢN/THANH TOÁN TRỰC TUYẾN

Gói sản phẩm



STID FIDO UAF Server



STID FIDO Client/Authenticator API

Các tính năng



Đăng nhập Internet Banking/
Mobile Banking bằng sinh trắc học



Bảo vệ giao dịch trực tuyến
bằng sinh trắc học

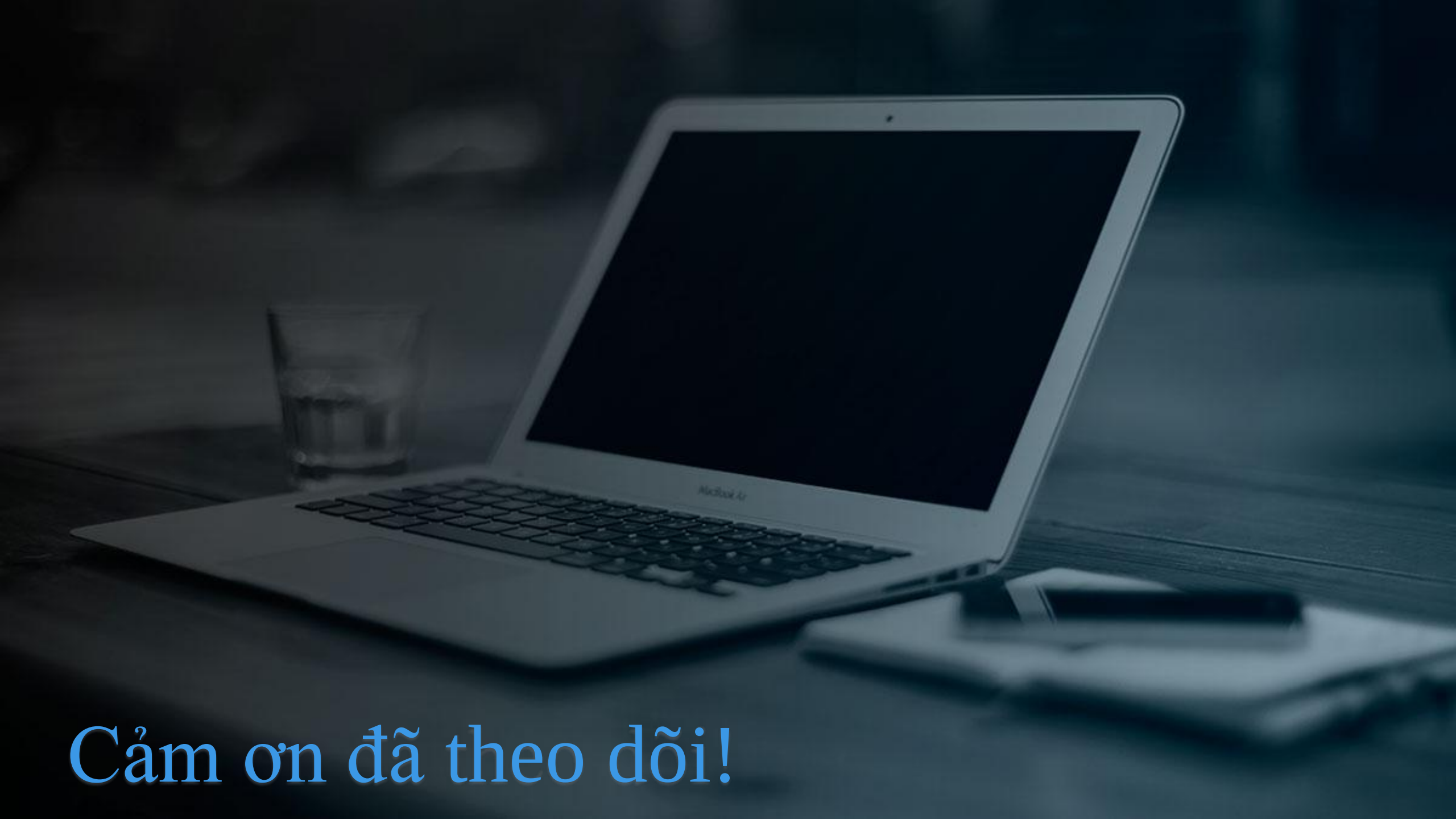
Hỗ trợ



Cài đặt và tích hợp



Bảo trì và sửa chữa



Cảm ơn đã theo dõi!