

HƯỚNG DẪN SỬ DỤNG VINCSS FIDO2® FINGERPRINT



Ngày: 01/03/2024

Số hiệu: CSS-PRD-PQMC-USG-240301-005

Phiên bản: 2.2

Phân loại tài liệu: Tài liệu công bố

Thực hiện: Trung tâm Sản phẩm, VinCSS

CÔNG TY CỔ PHẦN DỊCH VỤ AN NINH MẠNG VINCSS

Số 7 Đường Băng Lăng 1, Khu đô thị sinh thái Vinhomes Riverside, Phường
Việt Hưng, Quận Long Biên, Thành phố Hà Nội.

THEO DÕI PHIÊN BẢN

Phiên bản	Ngày	Người viết	Vị trí	Liên hệ	Nội dung
2.0	19/04/2023				Cập nhật nội dung phần xác thực không mật khẩu
2.1	27/04/2023				Cập nhật nội dung phần kết nối với máy tính trên nền tảng Windows
2.2	03/01/2024				Cập nhật nội dung phần kết nối với máy tính trên nền tảng Windows/Linux



MỤC LỤC

THEO DÕI PHIÊN BẢN	2
MỤC LỤC	3
I. THÔNG TIN SẢN PHẨM	7
I.1. Thông số kỹ thuật	7
I.2. Ý nghĩa của các đèn hiệu.....	8
II. QUẢN LÝ MÃ PIN VÀ VÂN TAY	9
II.1. Nền tảng Windows.....	9
II.1.1. Kết nối với máy tính	9
II.1.1.1 Sử dụng qua kết nối USB	10
II.1.1.2 Sử dụng qua kết nối NFC	10
II.1.1.3 Sử dụng qua kết nối Bluetooth	10
II.1.2. Tạo mã PIN mới.....	13
II.1.3. Thay đổi mã PIN.....	14
II.1.4. Thêm vân tay	16
II.1.5. Xóa vân tay.....	18
II.1.6. Thiết lập cài đặt gốc	20
II.2. Nền tảng macOS	24
II.2.1. Kết nối với máy tính	24
II.2.2. Tạo mới mã PIN.....	24
II.2.3. Thay đổi mã PIN.....	26
II.2.4. Thêm vân tay	27
II.2.5. Xóa vân tay.....	29
II.2.6. Quản lý dữ liệu đăng nhập	30
II.2.7. Thiết lập cài đặt gốc	32
II.3. Nền tảng Linux.....	33
II.3.1. USB.....	33
II.3.2. Bluetooth	34
III.1.1.1. Cài đặt Blueman trên Ubuntu	35
III.1.1.2. Kết nối khoá bảo mật VinCSS FIDO2® Fingerprint.....	35

III. XÁC THỰC KHÔNG MẬT KHẨU VỚI VINCSS FIDO2® FINGERPRINT 35

III.1. Đăng nhập với Window 35

III.1.1. Câu hình trên hệ thống Azure AD 35

III.1.1.3. Câu hình Azure AD 35

III.1.1.4. Đăng nhập Windows 10 sử dụng FIDO2 với provisioning packages 36

III.1.1.5. Đăng ký khóa xác thực cho tài khoản Azure AD 37

III.1.1.3.1. Sử dụng qua kết nối Bluetooth 40

III.1.1.3.2. Sử dụng qua kết nối USB 42

III.1.1.3.3. Sử dụng qua kết nối NFC 44

III.1.1.6. Kết nối User vào Azure Work Account 46

III.1.2. Đăng nhập Windows 50

III.1.2.1. Sử dụng qua kết nối Bluetooth 50

III.1.2.2. Sử dụng qua kết nối USB 51

III.1.2.3. Sử dụng qua kết nối NFC 51

III.2. Xác thực không mật khẩu tài khoản Microsoft 52

III.2.1. Đăng ký khóa bảo mật 52

III.2.1.1. Sử dụng qua kết nối Bluetooth 55

III.2.1.2. Sử dụng qua kết nối USB 57

III.2.1.3. Sử dụng qua kết nối NFC 58

III.2.2. Xác thực không mật khẩu tài khoản Microsoft 60

III.2.2.1. Sử dụng qua kết nối Bluetooth 61

III.2.2.2. Sử dụng qua kết nối USB 62

III.2.2.3. Sử dụng qua kết nối NFC 62

III.3. VinCSS OVPN Client 63

III.3.1. Windows 63

III.3.1.1. Đăng ký khóa bảo mật VinCSS FIDO2® Fingerprint 63

III.3.1.1.1. Sử dụng qua kết nối Bluetooth 64

III.3.1.1.2. Sử dụng qua kết nối USB 65

III.3.1.1.3. Sử dụng qua kết nối NFC 65

III.3.1.2. Xác thực bằng khoá bảo mật VinCSS FIDO2® Fingerprint 66

III.3.1.2.1. Xác thực không mật khẩu 69

III.3.1.2.2. Xác thực không tên người dùng 69

III.3.1.2.2.1.	Sử dụng qua kết nối Bluetooth	70
III.3.1.2.2.2.	Sử dụng qua kết nối USB	70
III.3.1.2.2.3.	Sử dụng qua kết nối NFC	71
III.3.2.	<i>macOS</i>	72
III.3.2.1.	Đăng ký khóa bảo mật VinCSS FIDO2® Fingerprint (<i>Chỉ hỗ trợ kết nối USB</i>)	72
III.3.2.2.	Xác thực bằng khoá bảo mật VinCSS FIDO2® Fingerprint.....	73
III.3.2.2.1.	Xác thực không mật khẩu	76
III.3.2.2.2.	Xác thực không tên người dùng.....	76
III.3.2.2.2.1.	Sử dụng qua kết nối Bluetooth	77
III.3.2.2.2.2.	Sử dụng qua kết nối USB	78
III.3.2.2.2.3.	Sử dụng qua kết nối NFC	78
III.4.	Xác thực 2 yếu tố tài khoản Facebook	79
III.4.1.	<i>Đăng ký khoá bảo mật</i>	79
III.4.1.1.	Sử dụng qua kết nối Bluetooth	81
III.4.1.2.	Sử dụng qua kết nối USB	82
III.4.1.3.	Sử dụng qua kết nối NFC	82
III.4.2.	<i>Xác thực 2 yếu tố với dịch vụ Facebook</i>	83
III.4.2.1.	Sử dụng qua kết nối Bluetooth	84
III.4.2.2.	Sử dụng qua kết nối USB	84
III.4.2.3.	Sử dụng qua kết nối NFC	85
III.5.	Xác thực 2 yếu tố với Twitter	85
III.5.1.	<i>Đăng ký khoá bảo mật</i>	85
III.5.1.1.	Sử dụng qua kết nối Bluetooth	87
III.5.1.2.	Sử dụng qua kết nối USB	87
III.5.1.3.	Sử dụng qua kết nối NFC	88
III.5.2.	<i>Xác thực 2 yếu tố với dịch vụ Twitter</i>	89
III.5.2.1.	Sử dụng qua kết nối Bluetooth	89
III.5.2.2.	Sử dụng qua kết nối USB	90
III.5.2.3.	Sử dụng qua kết nối NFC	90
III.6.	Xác thực 2 yếu tố với Google	90
III.6.1.	<i>Đăng ký khoá bảo mật</i>	90
III.6.1.1.	Sử dụng qua kết nối Bluetooth	96
III.6.1.2.	Sử dụng qua kết nối USB	97

III.6.1.3.	Sử dụng qua kết nối NFC	97
III.6.2.	Xác thực 2 yếu tố với dịch vụ Google	99
III.6.2.1.	Sử dụng qua kết nối Bluetooth	99
III.6.2.2.	Sử dụng qua kết nối USB	100
III.6.2.3.	Sử dụng qua kết nối NFC	100
THAM KHẢO.....		102



I. THÔNG TIN SẢN PHẨM

I.1. Thông số kỹ thuật



Hình ảnh VinCSS FIDO2® Fingerprint

Thông tin	Chi tiết
Tên sản phẩm	VinCSS FIDO2® Fingerprint
USB	USB Type-C
Bluetooth	Bluetooth Low Energy 5.0
NFC	ISO7816/ISO14443
Hệ điều hành hỗ trợ	Windows, MacOS, Linux, Android, iOS
Tiêu chuẩn xác thực	Passwordless, Strong Two Factor, Strong Multi-Factor
Chứng chỉ	FIDO2 Certified, FCC, JQA
Giao thức hỗ trợ	WebAuthn, FIDO2 CTAP1, FIDO2 CTAP2, Universal 2nd Factor (U2F)
Trình duyệt hỗ trợ	Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge, Microsoft Edge Chromium
Thuật toán mã hóa	ECC p256

Kiến trúc CPU	32-bit ARM® Cortex™-M4
Số lượng tài khoản có thẻ lưu	50
Số lượng vân tay có thẻ lưu	5
Đèn LED báo hiệu	RGB Led
Độ phân giải cảm biến	508 dpi
Tỉ lệ chấp nhận sai FAR	<0.0002%
Thời gian xác thực vân tay	< 1s
Cân nặng	20gr
Kích thước sản phẩm	43,5 x 38 x 8 (mm)
Dung lượng/Loại pin	25mAh, Pin Lithium-ion
Thời lượng pin	5-7 ngày (12 lần xác thực/ngày)
Thời gian chờ	4 tháng
Thời gian sạc đầy	2 giờ 30 phút
Nguồn điện sử dụng	5V/1A
Vật liệu sử dụng	Nhựa Polycarbonate cao cấp chịu lực, đảm bảo độ bền cho sản phẩm
Nhiệt độ hoạt động	-10°C ~ 60°C
Màu sắc	Đen, Trắng , Xanh
Phụ kiện đi kèm	Cáp USB Type – C, móc khoá, giá đỡ
Xuất xứ	Việt Nam

I.2. Ý nghĩa của các đèn hiệu

Đèn hiệu của VinCSS FIDO2® Fingerprint sẽ cho người dùng biết trạng thái hiện tại của pin, trạng thái đang sạc pin, hoặc chế độ hoạt động.

Tín hiệu	Ý nghĩa	Trạng thái
Nháy đèn đỏ ba lần liên tiếp	Sắp hết pin, cần sạc	Đang sử dụng Bluetooth hoặc NFC
Đèn bật màu hổ phách	Khoá đang được sạc	Đang kết nối với USB
Đèn bật màu xanh lá cây	Khoá đã sạc đầy	Đang kết nối với USB
Đèn bật màu xanh nước biển	Bật chế độ Bluetooth, và khoá đã được kết nối với một thiết bị Bluetooth	Đang sử dụng Bluetooth
Đèn nháy sáng màu xanh nước biển	Khoá bảo mật vào chế độ ghép nối	Đang sử dụng Bluetooth
Đèn bật màu tím	Đã kích hoạt NFC	Đang sử dụng NFC
Nhấp nháy nhanh với đèn màu trắng	Khoá bảo mật đang trong quá trình xử lý và yêu cầu người dùng tương tác.	Yêu cầu người dùng xác nhận bằng cách chạm vào cảm biến vân tay

II. QUẢN LÝ MÃ PIN VÀ VÂN TAY

Việc đặt mã PIN cho VinCSS FIDO2® Fingerprint là yêu cầu bắt buộc để có thể thêm/xóa vân tay, nhằm đảm bảo an toàn cho thiết bị, tránh trường hợp thêm vân tay trái phép, thử vân tay quá nhiều lần hoặc xóa vân tay từ người lạ.

Trường hợp người dùng cần tạo mới, thay đổi mã PIN/vân tay hoặc reset thiết bị VinCSS FIDO2® Fingerprint thì có thể thực hiện theo các bước dưới đây.

II.1. Nền tảng Windows

II.1.1. Kết nối với máy tính

Lưu ý: Pin sẽ được set ở chế độ nghỉ để duy trì thời gian chờ của pin được lâu hơn. Với lần đầu tiên sử dụng chức năng NFC/Bluetooth của khoá bảo mật, người dùng cần kết nối khoá bảo mật thông qua kết nối USB để kích hoạt pin của khoá.

II.1.1.1 Sử dụng qua kết nối USB

Tiến hành kết nối khoá bảo mật VinCSS FIDO2® Fingerprint vào máy tính thông qua dây USB, đảm bảo rằng khoá bảo mật đang **không** trong chế độ Bluetooth hoặc NFC. Nếu đèn LED nháy đỏ 3 lần liên tiếp cho biết mức pin đang ở dưới 20%, đèn LED màu hổ phách cho biết khoá bảo mật đang được sạc, đèn LED màu xanh lá cây cho biết pin đã được sạc đầy. Khoá bảo mật VinCSS FIDO2® Fingerprint có thể được sử dụng khi đang sạc.

II.1.1.2 Sử dụng qua kết nối NFC

Tiến hành đặt khoá bảo mật VinCSS FIDO2® Fingerprint lên đầu đọc NFC. Khi đèn LED màu tím, có thể sử dụng tính năng NFC.

Lưu ý:

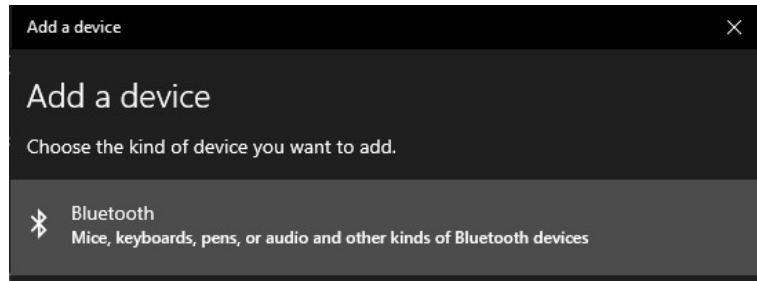
- *Đối với các dòng iPhone từ iPhone 7/8, iPhone 7/8 Plus và iPhone X: Mở trung tâm điều khiển, bật chế độ NFC Tag Reader, sau đó đặt khoá bảo mật VinCSS FIDO2 Fingerprint lên camera trước của iPhone, sau đó di chuyển khoá xuống phía dưới từ 1/2 đến 2/3 chiều dài khoá bảo mật. Khi đèn hiện màu tím có nghĩa kết nối NFC đã thành công.*
- *Đối với các dòng iPhone từ iPhone XS, iPhone XS max trở lên: có thể kết nối trực tiếp khoá bảo mật với thiết bị theo hướng dẫn bên trên mà không cần mở chế độ NFC Tag Reader tại trung tâm điều khiển.*

II.1.1.3 Sử dụng qua kết nối Bluetooth

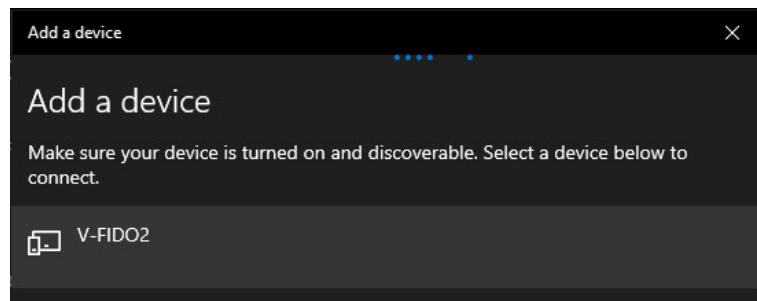
- Tại trạng thái tắt (*không có đèn sáng*), chuyển khoá bảo mật VinCSS FIDO2® Fingerprint vào chế độ kết nối Bluetooth bằng cách giữ cảm biến vân tay trong 5 giây. Khi đèn LED chuyển sang màu xanh lam, có thể sử dụng tính năng Bluetooth.
- Nếu đèn LED xanh lam không nhấp nháy, thực hiện giữ cảm biến vân tay trong vòng 5 giây để chuyển sang chế độ ghép đôi.
- Truy cập **Windows > Settings > Devices**. Tại mục **Bluetooth** chọn **On**, sau đó chọn **Add Bluetooth or other device**.



- Tại mục **Add a device**, chọn **Bluetooth**.

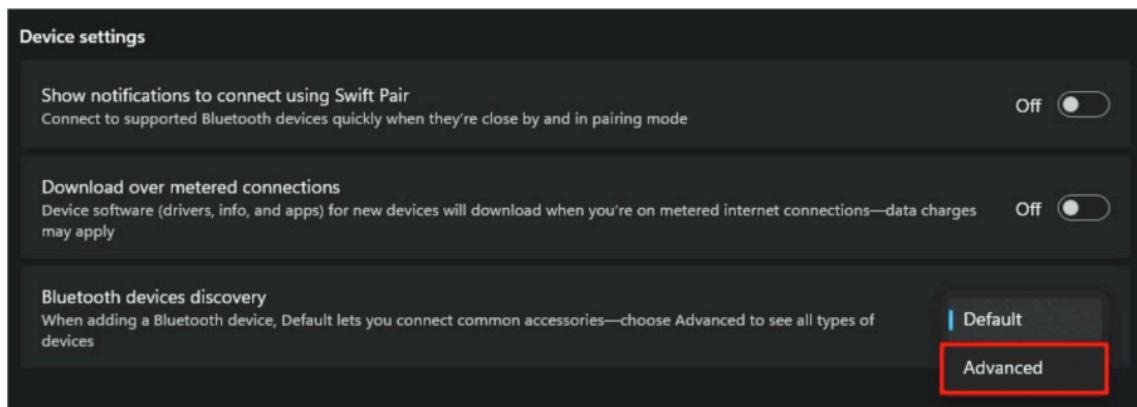


- Chọn thiết bị có tên **V-FIDO2**.



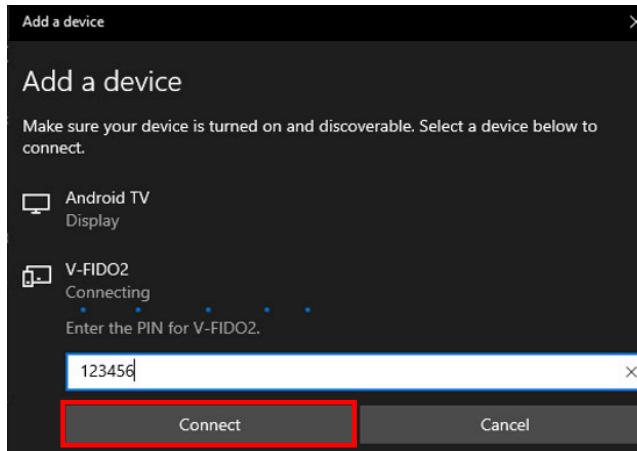
Lưu ý:

- *Do thay đổi trong chính sách hiển thị thiết bị Bluetooth trên Windows 11, máy tính có thể không tìm thấy khoá bảo mật. Khi đó vui lòng thực hiện thay đổi cài đặt như hướng dẫn dưới đây:*
 - *Truy cập Windows > Settings > Bluetooth & Devices > Devices > Devices Settings.*
 - *Tại mục Bluetooth devices , chọn Advance.*

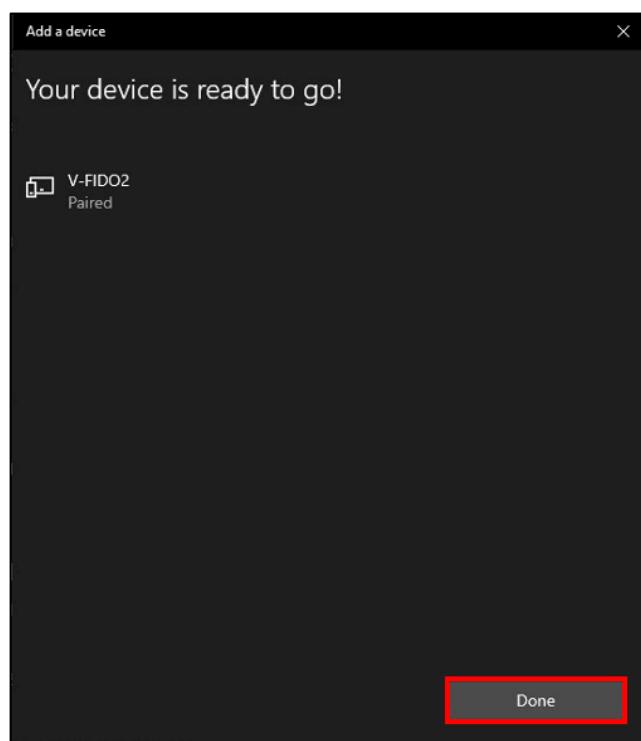


- Nhập mã ghép đôi để kết nối. Sau đó nhấn **Connect**.

Lưu ý: Thiết bị sẽ có 1 mã serial bao gồm chữ và số được hiển thị ở mặt sau của khoá bảo mật. Mã ghép đôi là một dãy số gồm 6 chữ số cuối của mã serial. (Trong trường hợp mã serial chỉ có 5 chữ số cuối thì nhập thêm số “0” ở đầu dãy số. Ví dụ: XXX123456 => 123456 hoặc XXX12345 => 012345).



- Kết nối thành công. Nhấn **Done** để kết thúc.



- Sau khi kết nối thành công, trong danh sách thiết bị sẽ hiển thị khóa bảo mật VinCSS FIDO2® Fingerprint và dung lượng pin còn lại của khóa.

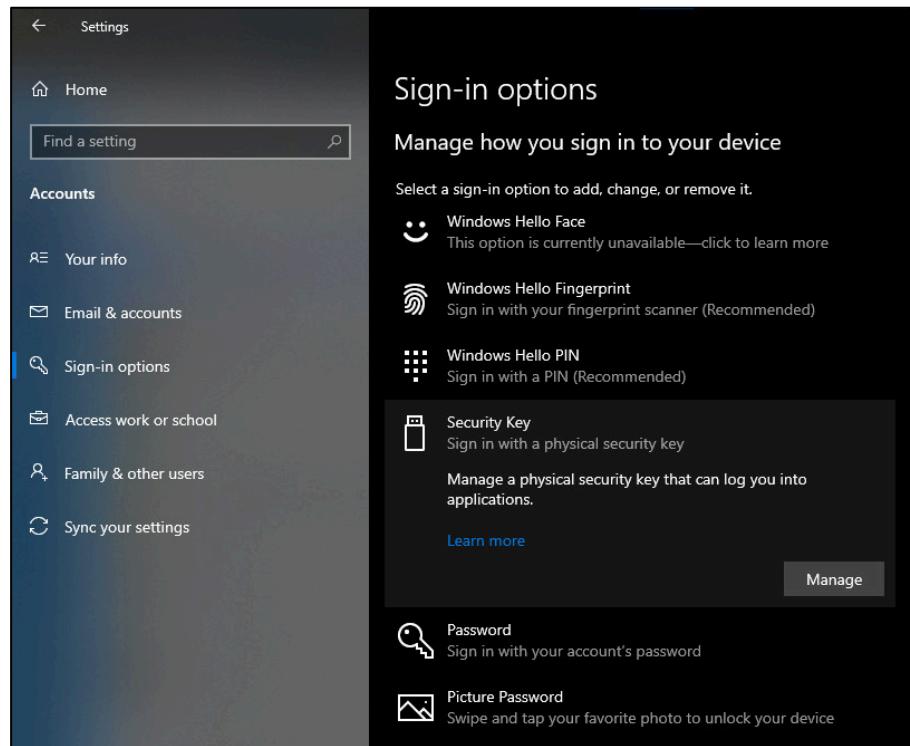


Lưu ý:

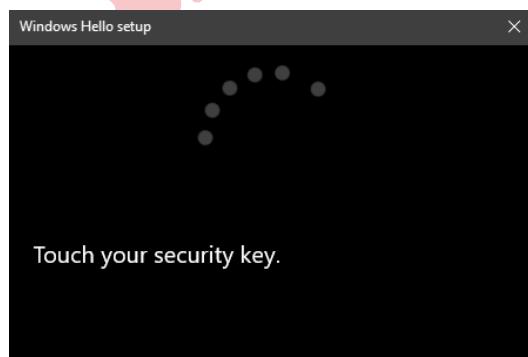
- Trong trường hợp muốn ghép nối với thiết bị mới, thực hiện nhấn giữ cảm biến vân tay trong vòng 5 giây khi khóa xác thực đang được bật.
- Nếu không có hoạt động xác thực trong 90 giây, đèn LED sẽ tắt, khóa tự chuyển vào chế độ Sleep.

II.1.2. Tạo mã PIN mới

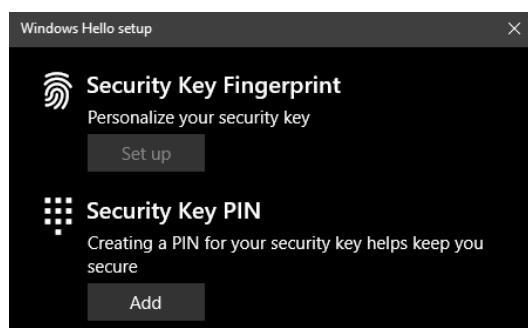
- Truy cập Start > Settings > Account > Sign-in options > Security Key, sau đó nhấn Manage.



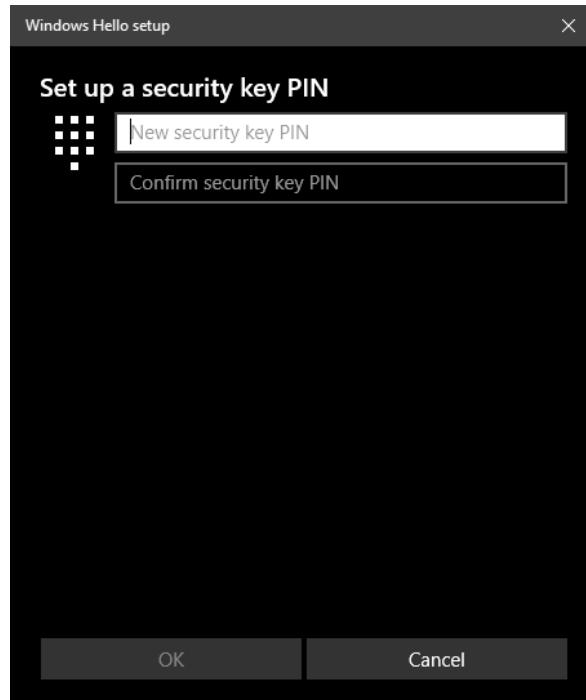
- **Chạm** vào cảm biến vân tay trên khóa bảo mật VinCSS FIDO2® Fingerprint.



- Mặc định ban đầu, VinCSS FIDO2® Fingerprint không có mã PIN, để tạo mã PIN mới, tại mục Security Key PIN, nhấp vào Add.

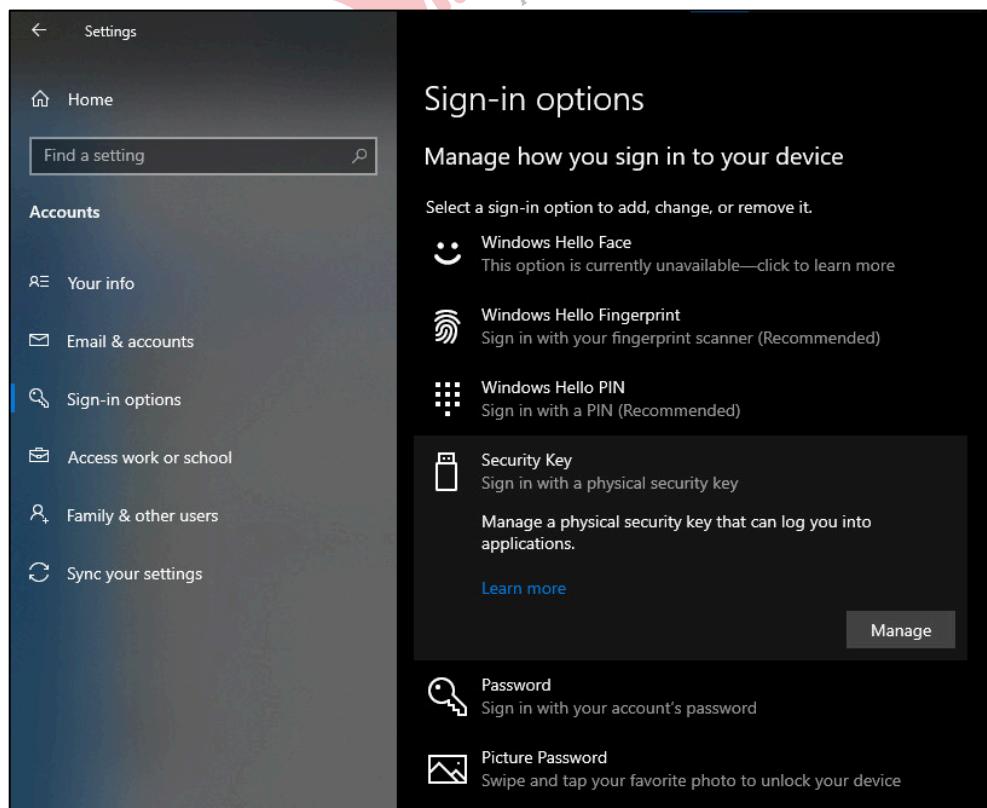


- Điền vào thông tin mã PIN mới (*Tối thiểu 4 ký tự, tối đa 63 ký tự; bao gồm chữ (chữ thường, chữ hoa), số và ký tự đặc biệt*), sau đó chọn **OK**.

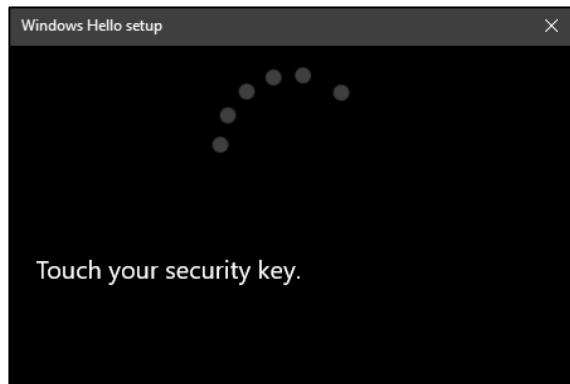


II.1.3. Thay đổi mã PIN

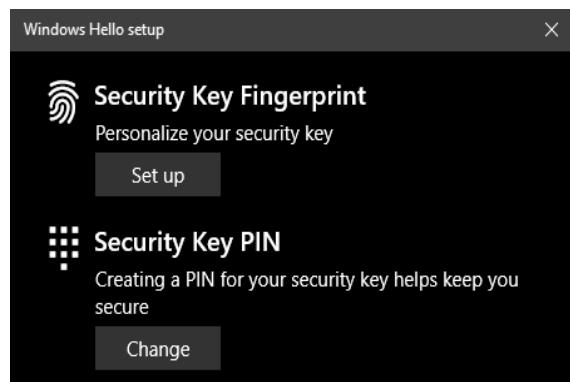
- Truy cập Start > Settings > Account > Sign-in options > Security Key. Sau đó chọn **Manage**.



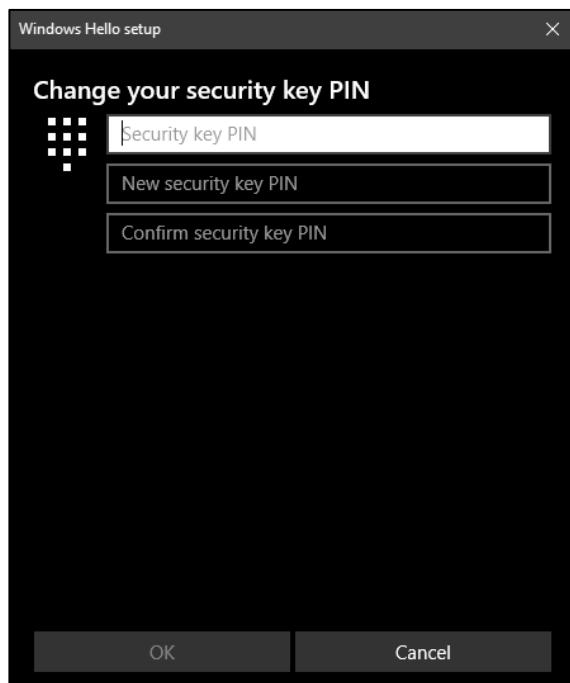
- **Chạm vào cảm biến vân tay trên khóa bảo mật.**



- Tại mục **Security Key PIN**, nhấn **Change** để thay đổi mã PIN của khóa bảo mật.



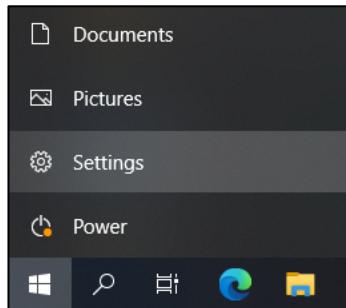
- Điền các thông tin theo thứ tự: mã PIN cũ, mã PIN mới, xác nhận mã PIN mới (*Tối thiểu 4 ký tự, tối đa 63 ký tự; bao gồm chữ (chữ thường, chữ hoa), số và ký tự đặc biệt*). Sau đó nhấn **OK**.



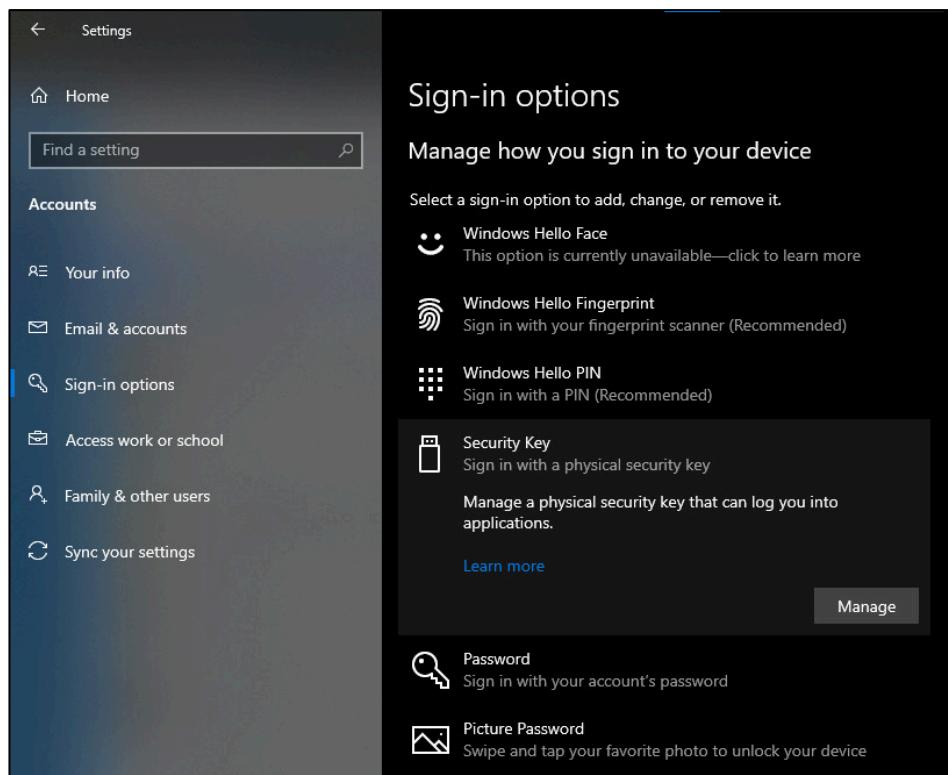
II.1.4. Thêm vân tay

Sau khi tạo mã PIN cho VinCSS FIDO2® Fingerprint thành công, người dùng có thể thêm vân tay cho thiết bị (*tối đa 5 vân tay*). Thực hiện các bước sau:

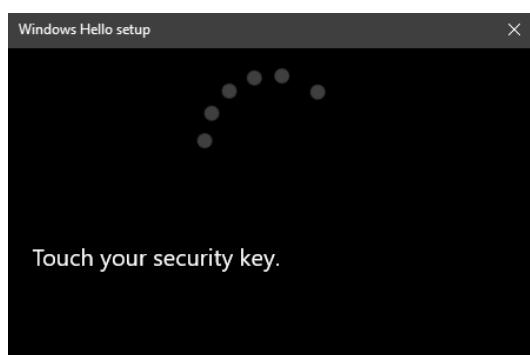
- Truy cập Start > Settings.



- Chọn Account > Sign-in options > Security Key. Sau đó chọn Manage.



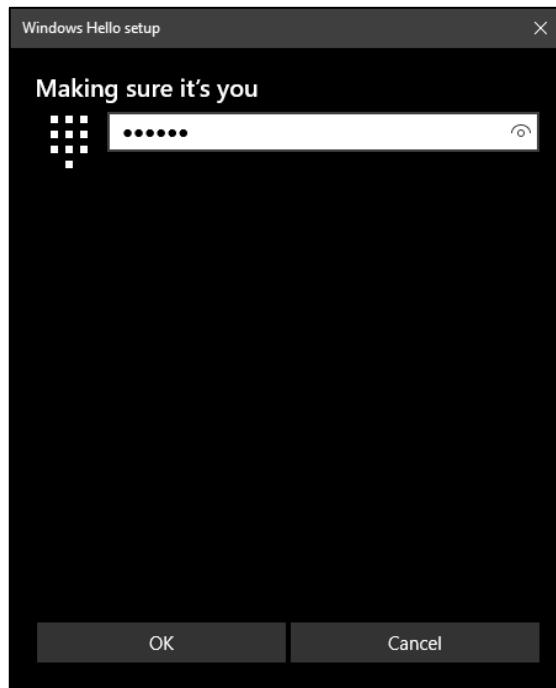
- **Chạm vào cảm biến vân tay trên khóa bảo mật.**



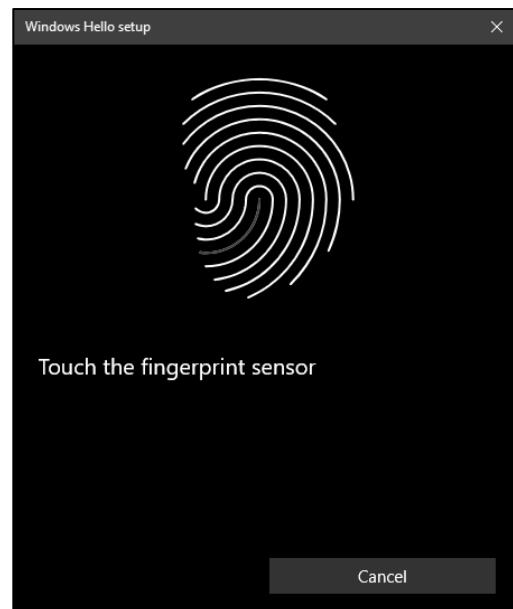
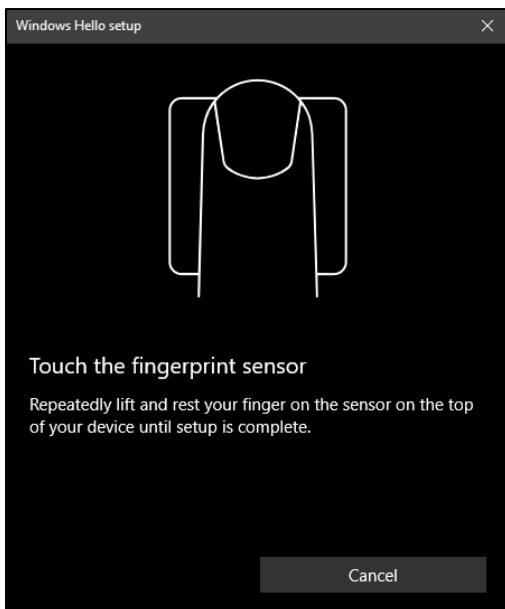
- Tại mục **Security Key Fingerprint**, nhấn **Set up**.



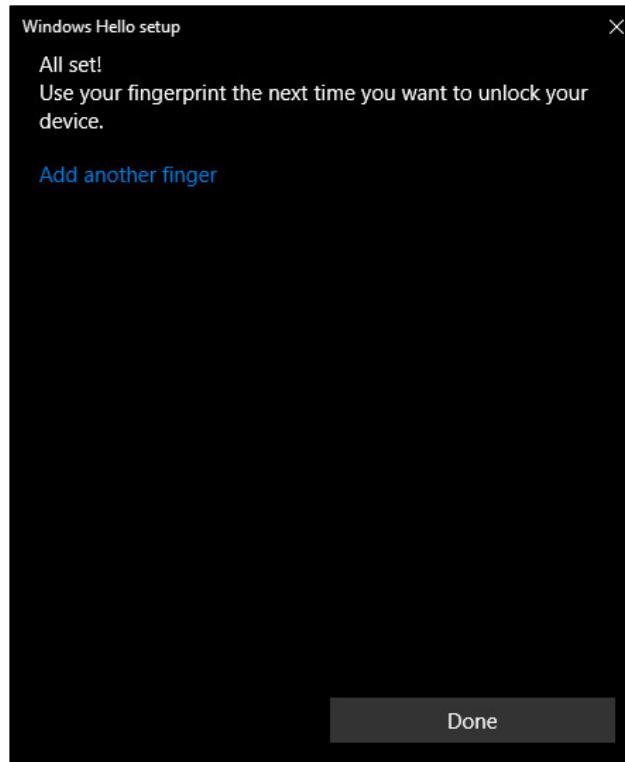
- Điền mã PIN (*đã tạo ở bước trên*), sau đó nhấn **OK**.



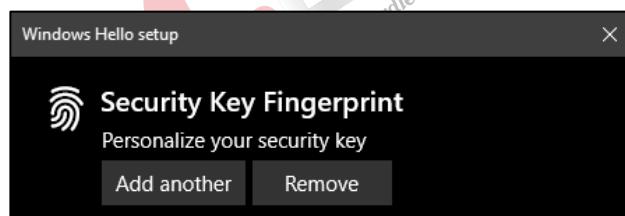
- Quét vân tay bằng cách chạm ngón tay vào vùng cảm biến vân tay của khoá bảo mật cho đến khi đèn hiển thị màu xanh lá, sau đó nhấc tay ra khỏi vùng cảm biến (*thực hiện 5 lần*).



- Sau khi quét xong vân tay, nhấn **Done** để kết thúc.



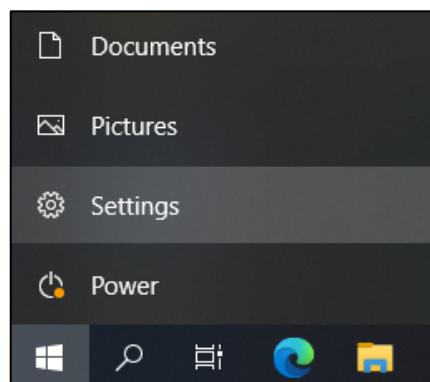
- Để thêm vân tay khác, tại mục **Security Key Fingerprint**, chọn **Add another**, sau đó thực hiện các bước tương tự như trên.



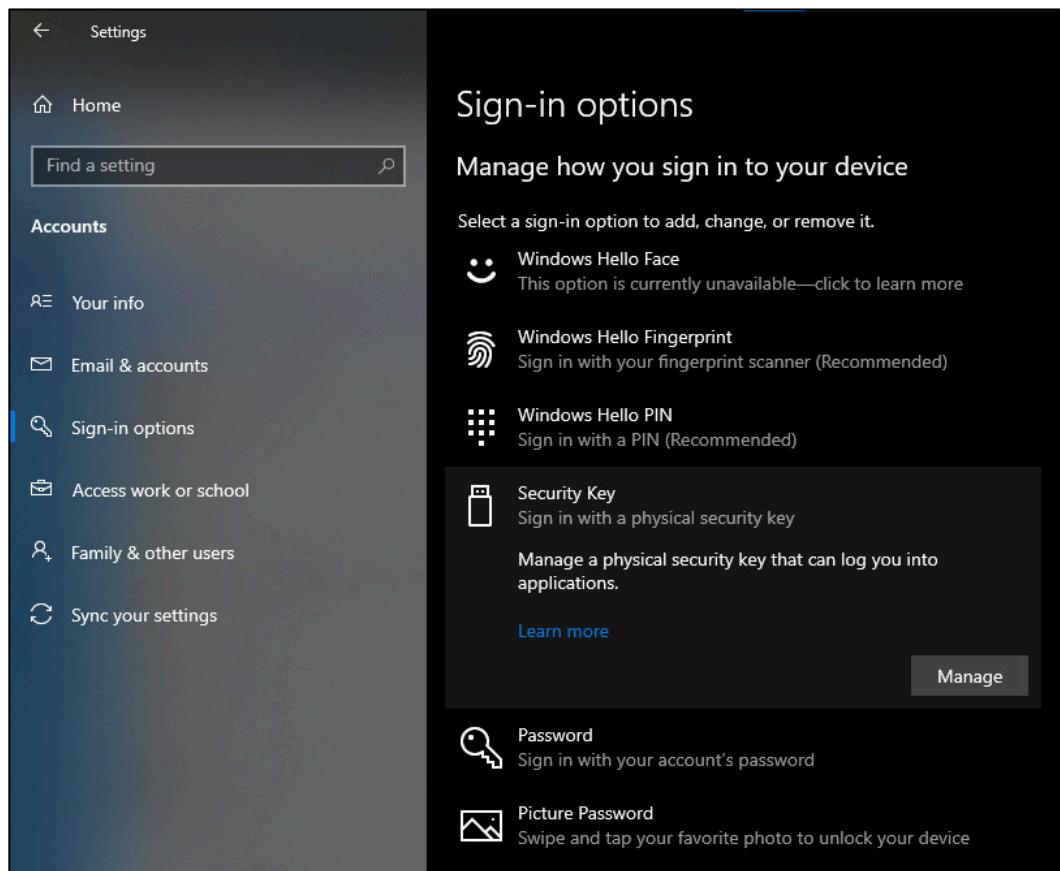
II.1.5. Xóa vân tay

Hiện hệ điều hành Windows chưa hỗ trợ xóa từng dấu vân tay trên khóa bảo mật, chỉ có thể xóa toàn bộ dấu vân tay. Các bước thực hiện như sau:

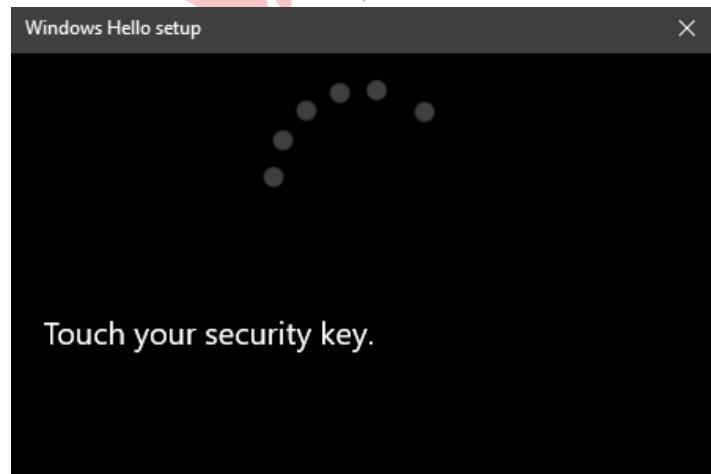
- Truy cập Start > Settings.



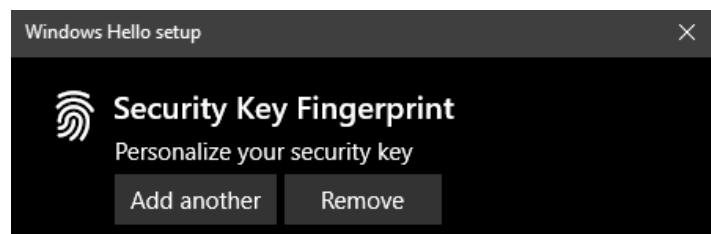
- Chọn Account > Sign-in options > Security Key, sau đó chọn Manage.



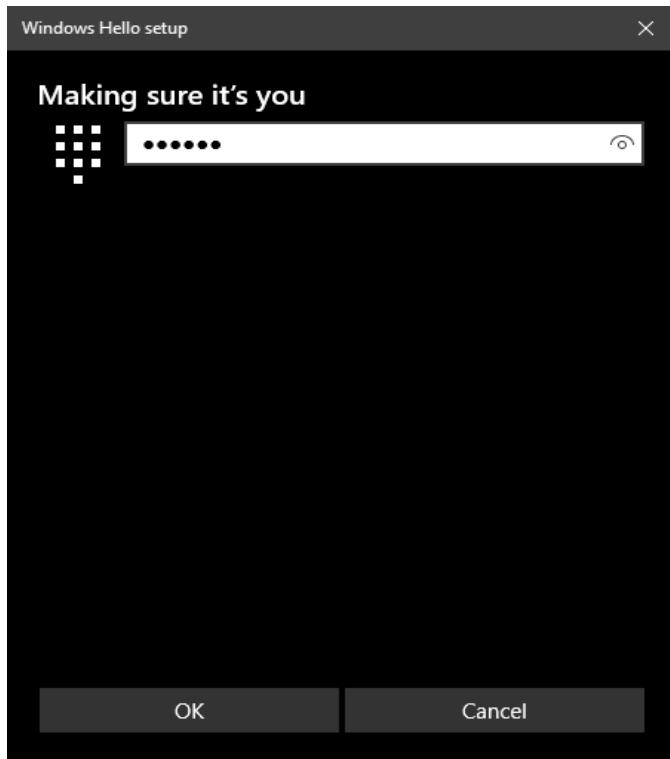
- Chạm vào cảm biến vân tay trên khóa bảo mật.



- Tại mục Security Key Fingerprint, chọn Remove.



- Điền mã PIN (*đã tạo ở bước trên*), sau đó nhấn **OK**.

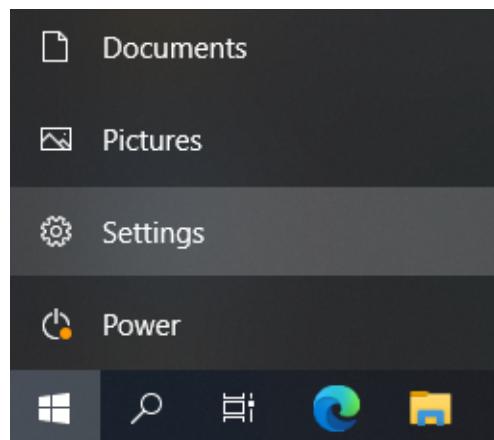


II.1.6. Thiết lập cài đặt gốc

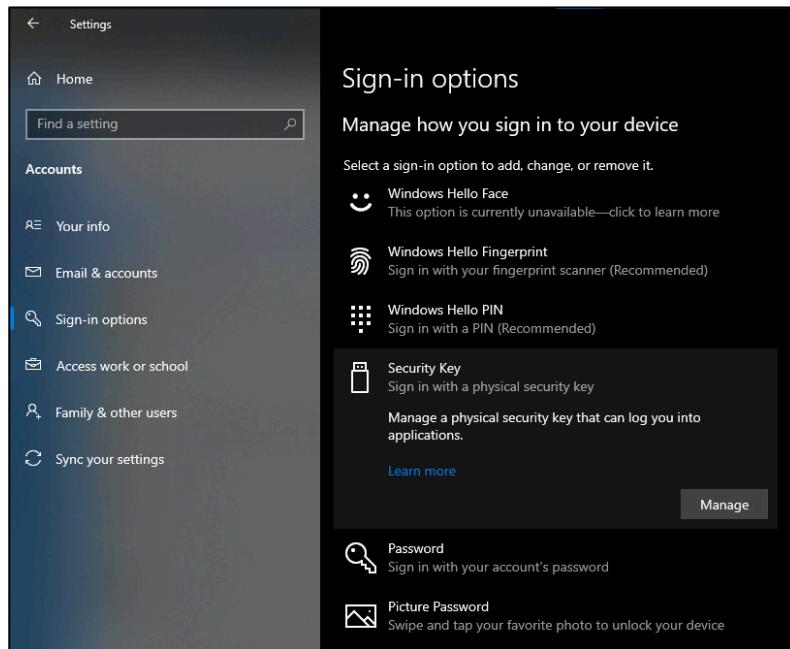
Trong trường hợp quên mã PIN của VinCSS FIDO2® Fingerprint, người dùng có thể reset thiết bị, tuy nhiên điều này sẽ khiến các dịch vụ đã đăng ký trước đó không thể xác thực được. Sau khi reset, thiết bị trở thành khóa bảo mật mới, vì vậy cần đăng ký lại các dịch vụ để có thể xác thực. Trong trường hợp nhập sai mã PIN nhiều lần (*trên 8 lần*) thì thiết bị sẽ bị khóa vĩnh viễn, người dùng bắt buộc phải reset để có thể sử dụng lại khóa bảo mật VinCSS FIDO2® Fingerprint như một thiết bị mới.

Để reset VinCSS FIDO2® Fingerprint, người dùng thực hiện các bước sau:

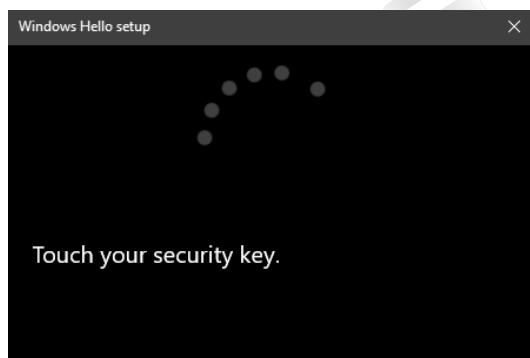
- Truy cập Start > Settings.



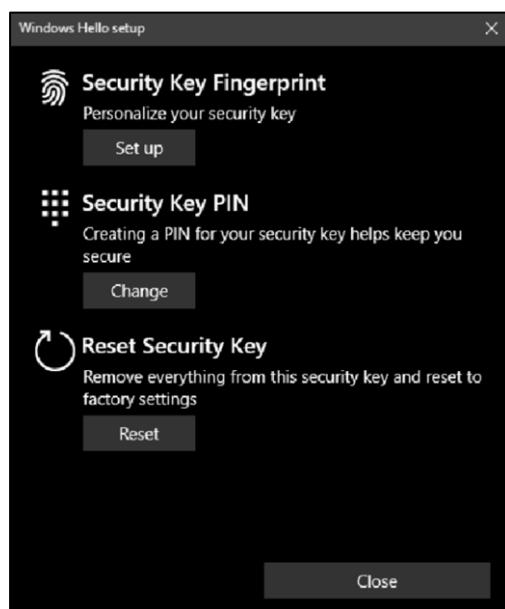
- Chọn **Account > Sign-in options > Security Key**. Sau đó nhấn **Manage**.



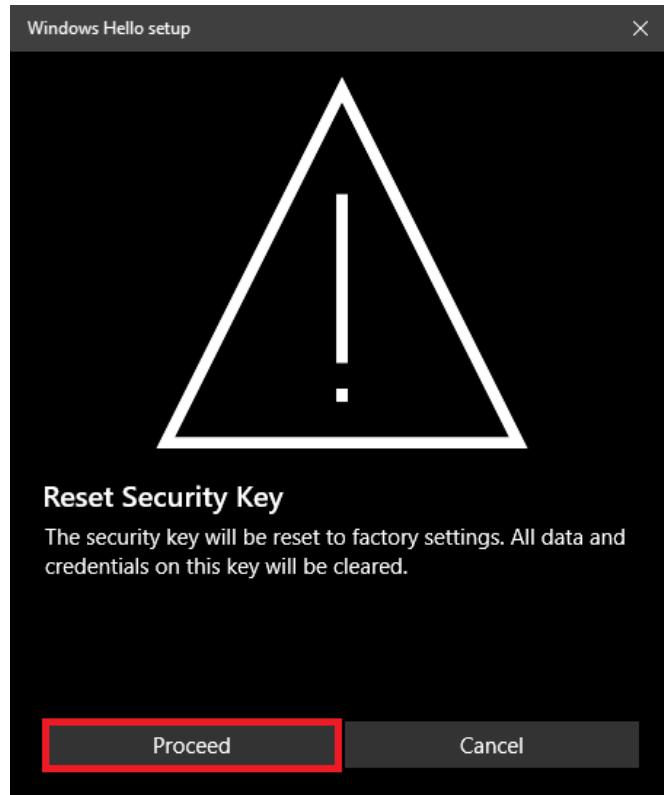
- **Chạm vào cảm biến vân tay trên khóa bảo mật.**



- Tại mục **Reset Security Key**, nhấn **Reset**.



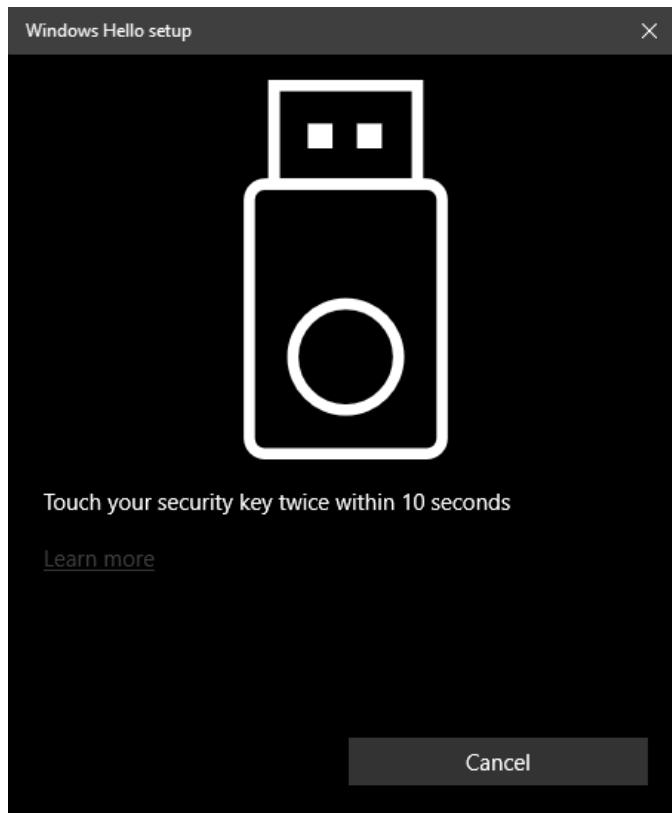
- Nhấn **Proceed** để tiến hành Reset khóa bảo mật VinCSS FIDO2® Fingerprint.



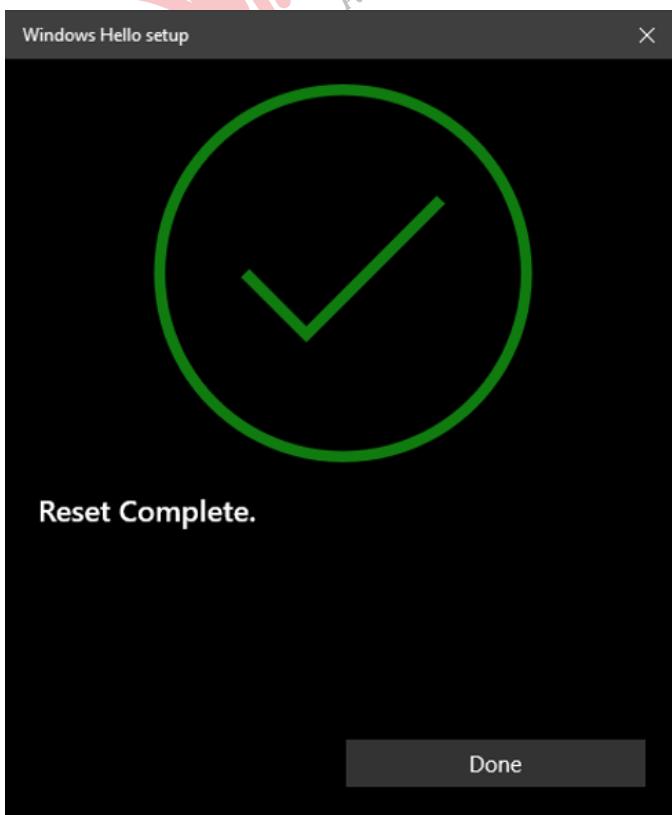
- Rút khóa bảo mật VinCSS FIDO2® Fingerprint ra khỏi máy tính, sau đó cắm lại.



- Khi hiện đèn màu trắng tay trên khóa bảo mật VinCSS FIDO2® Fingerprint, chạm 2 lần vào cảm biến vân tay trong 10s.



- Reset khóa bảo mật thành công, chọn **Done** để hoàn tất.



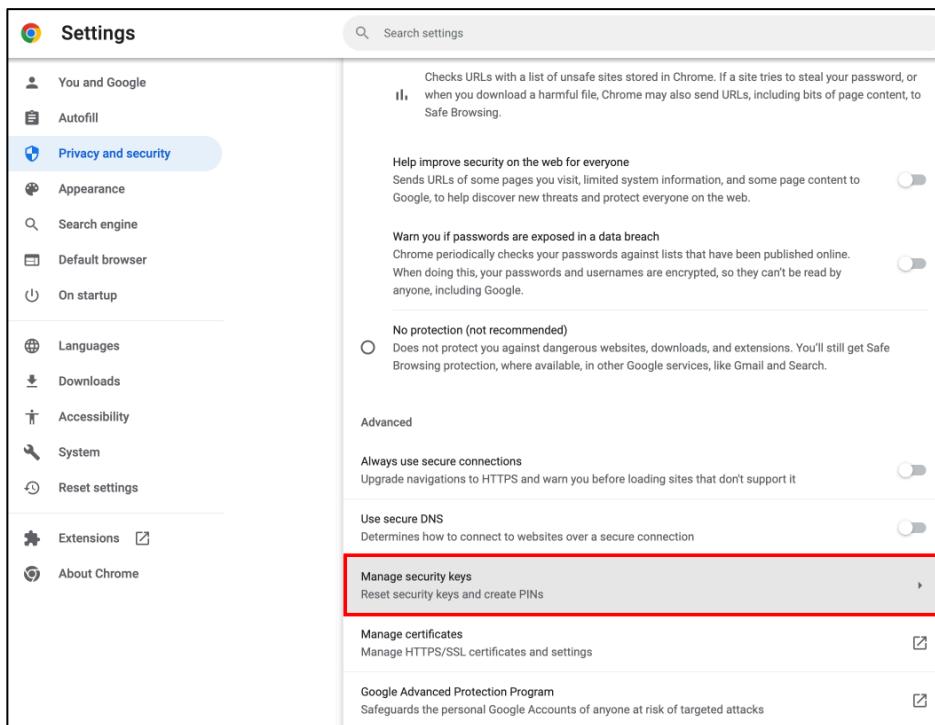
II.2. Nền tảng macOS

II.2.1. Kết nối với máy tính

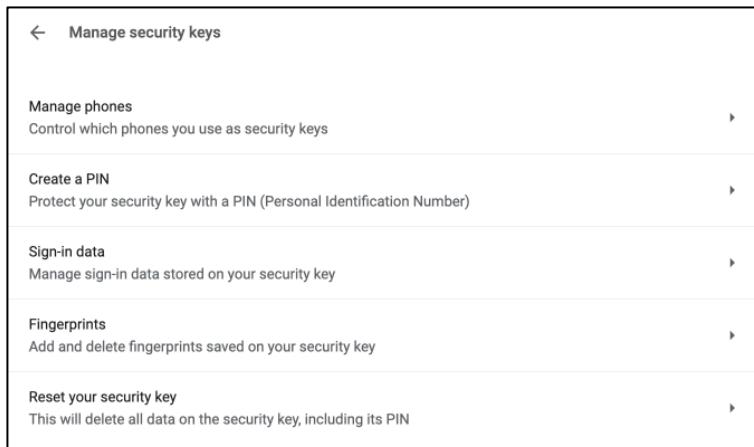
Tiến hành kết nối khoá bảo mật VinCSS FIDO2® Fingerprint vào máy tính thông qua dây USB. Nếu đèn LED nháy đỏ 3 lần liên tiếp cho biết mức pin đang ở dưới 20%, đèn LED màu hổ phách cho biết khoá bảo mật đang được sạc, đèn LED màu xanh lá cây cho biết pin đã được sạc đầy. Khoá bảo mật VinCSS FIDO2® Fingerprint có thể được sử dụng khi đang sạc.

II.2.2. Tạo mới mã PIN

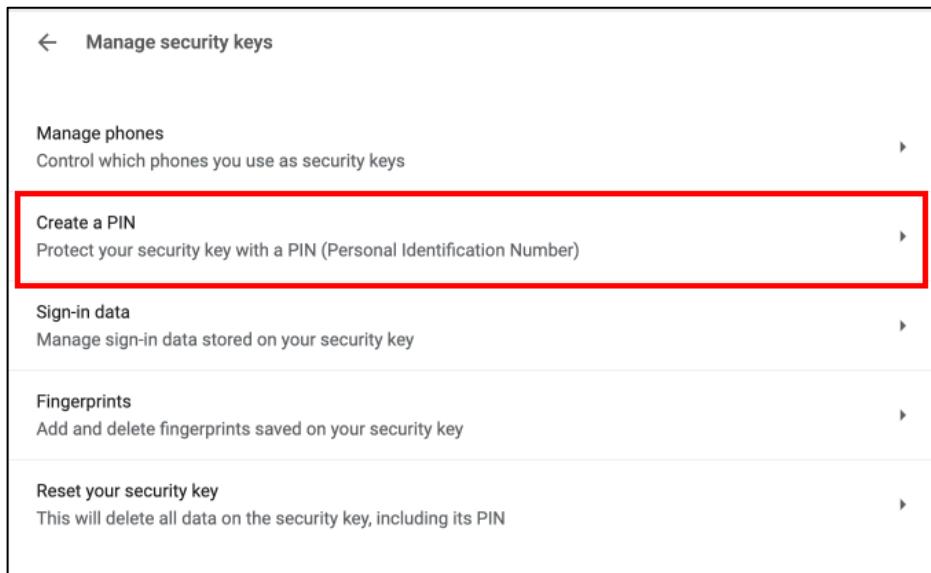
- Mở trình duyệt Chrome, chọn **Setting > Privacy and security > Security > Manage security keys.**



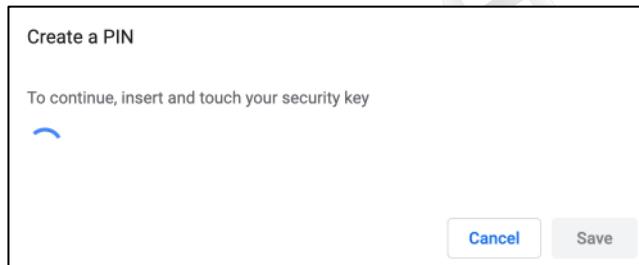
- Giao diện **Manage security keys** được mở lên.



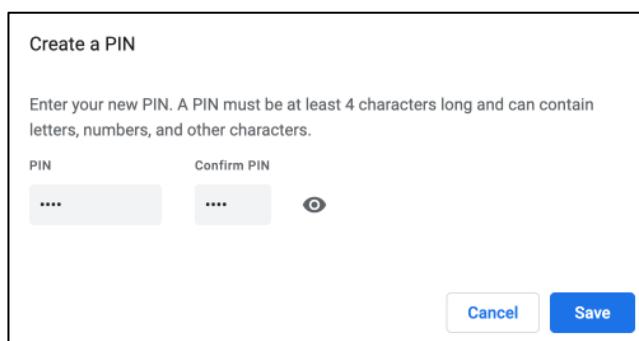
- Mặc định ban đầu, khóa bảo mật VinCSS FIDO2® Fingerprint không có mã PIN. Để tạo mới mã PIN, trên giao diện **Manage security keys**, chọn **Create a PIN**.



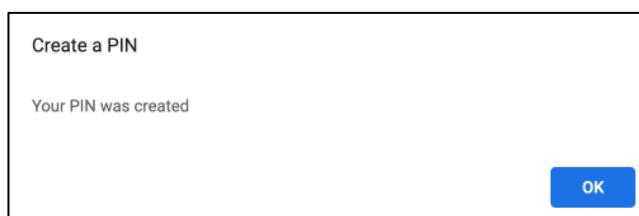
- Chạm vào cảm biến vân tay trên VinCSS FIDO2® Fingerprint để xác nhận.



- Nhập mã PIN (*Tối thiểu 4 ký tự, tối đa 63 ký tự; bao gồm chữ (chữ thường, chữ hoa), số và ký tự đặc biệt*) và xác nhận lại rồi nhấn **Save** để tạo mã PIN.

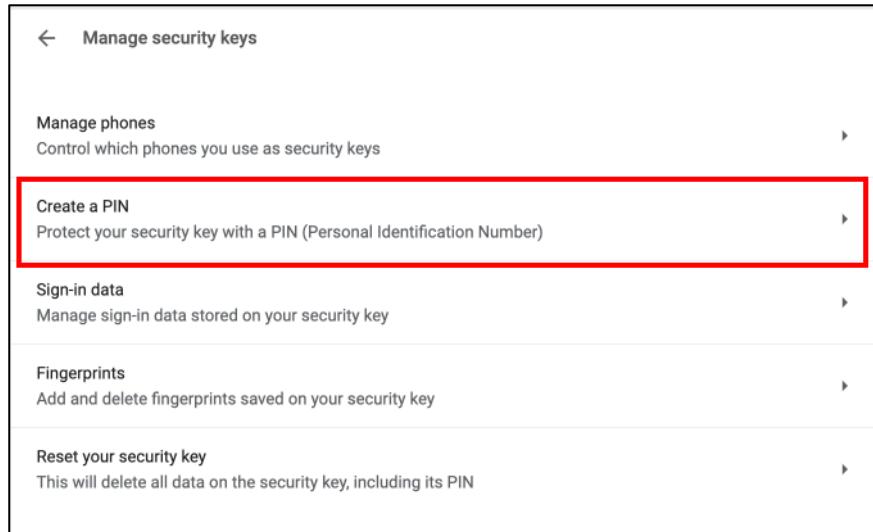


- Nhấn **OK** để hoàn thành việc tạo mã PIN cho khoá bảo mật.

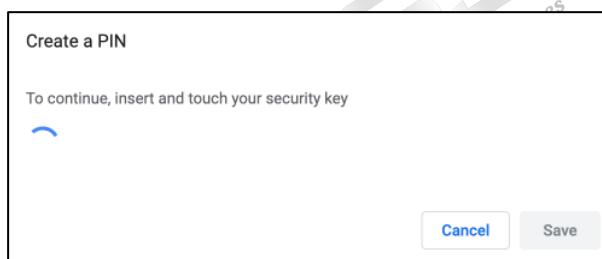


II.2.3. Thay đổi mã PIN

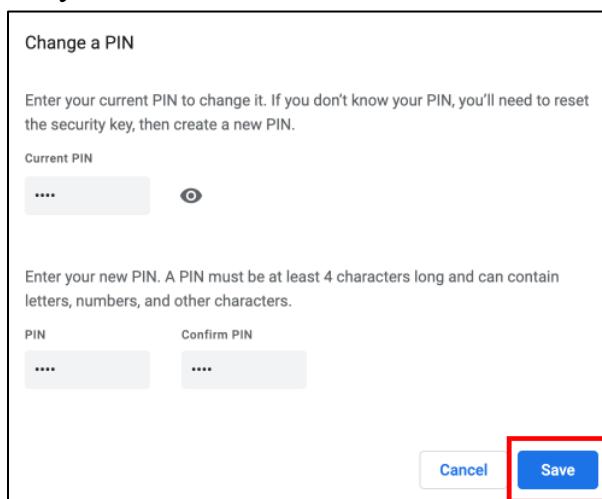
- Để thay đổi mã PIN cho VinCSS FIDO2® Fingerprint, trên giao diện **Manage security keys** (mở trình duyệt Chrome, chọn **Setting > Privacy and security > Security > Manage security keys**), chọn **Create a PIN**.



- Chạm vào cảm biến vân tay trên thiết bị để xác nhận.



- Tại cửa sổ **Change a PIN** nhập mã PIN hiện tại đang sử dụng, ở phía dưới nhập mã PIN mới cần thay đổi và xác nhận lại (*Tối thiểu 4 ký tự, tối đa 63 ký tự; bao gồm chữ (chữ thường, chữ hoa), số và ký tự đặc biệt*), sau đó chọn **Save** để thay đổi.



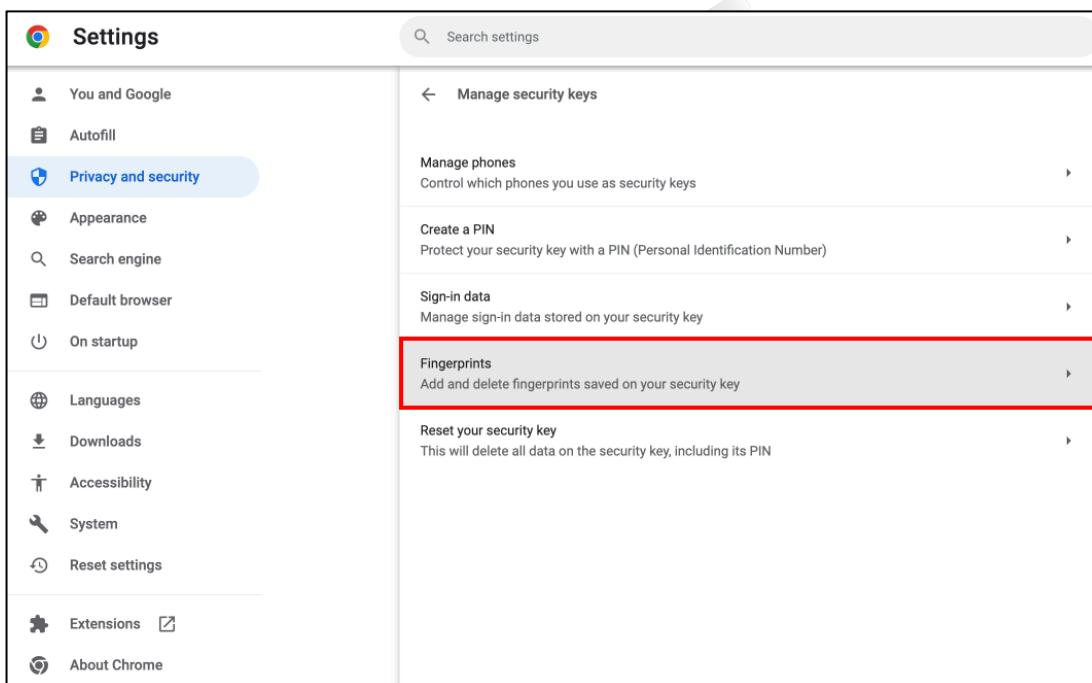
- Nhấn **OK** để hoàn thành việc thay đổi mã PIN cho VinCSS FIDO2® Fingerprint.



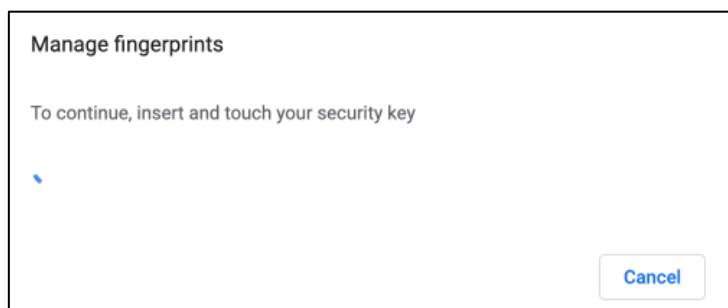
II.2.4. Thêm vân tay

Sau khi tạo mã PIN cho VinCSS FIDO2® Fingerprint thành công, người dùng có thể thêm vân tay cho thiết bị (*tối đa 5 vân tay*). Thực hiện các bước như sau:

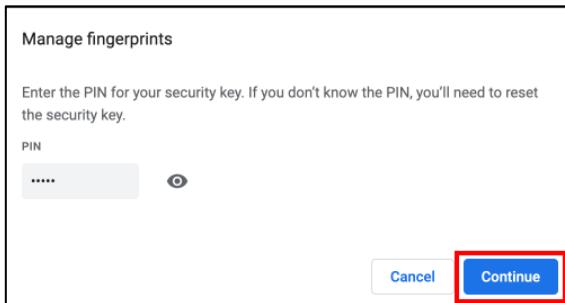
- Trên giao diện **Manage security keys** (*mở trình duyệt Chrome, chọn Setting > Privacy and security > Security > Manage security keys*), chọn **Fingerprints**.



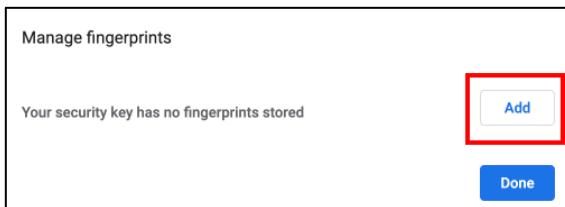
- Chạm vào cảm biến vân tay trên khóa bảo mật.



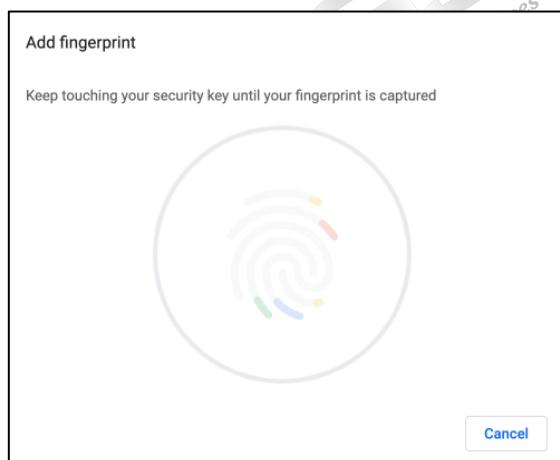
- Điền mã PIN (*đã tạo ở bước trên*), sau đó nhấn **Continue** để tiếp tục.



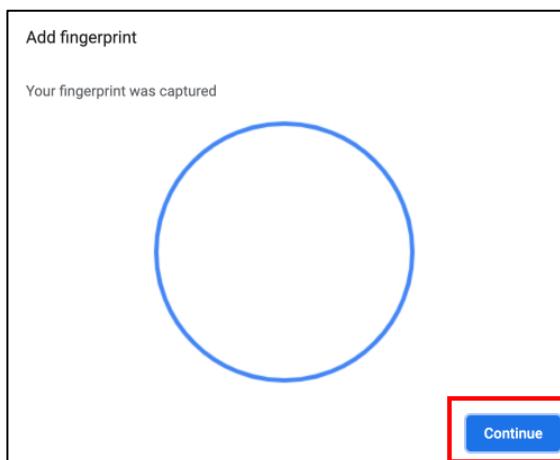
- Để thêm vân tay cho khóa bảo mật, nhấn **Add**.



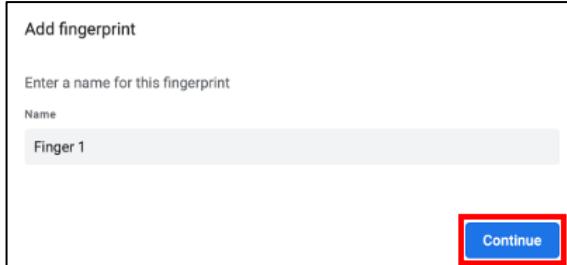
- Khi thiết bị nháy đèn trắng, tiến hành quét vân tay bằng cách chạm ngón tay vào cảm biến vân tay cho đến khi đèn hiển thị màu xanh lá, sau đó nhấc tay ra khỏi cảm biến (*thực hiện 5 lần*).



- Sau khi quét xong vân tay, nhấn **Continue** để tiếp tục.



- Đặt tên cho vân tay (*tối đa 30 ký tự không dấu*), sau đó nhấn **Continue** để tiếp tục.

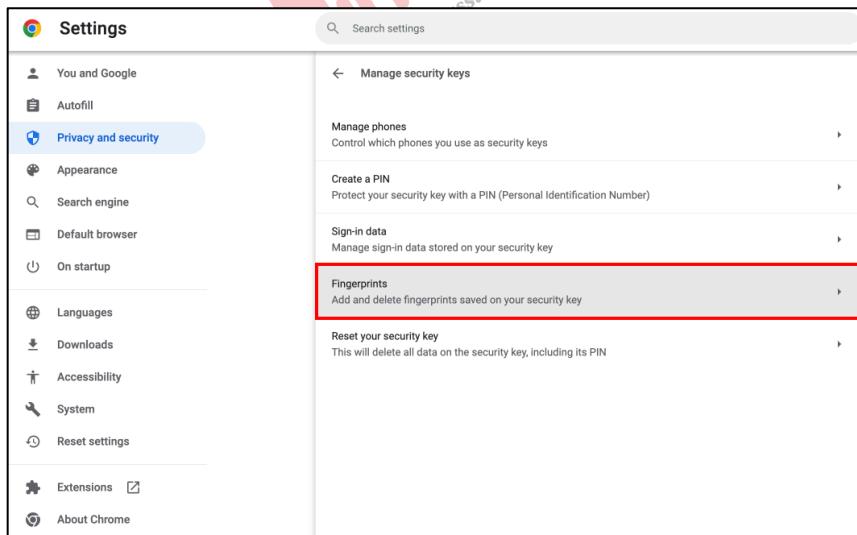


- Nhấn **Add** để tiếp tục thêm vân tay, hoặc nhấn **Done** để kết thúc.

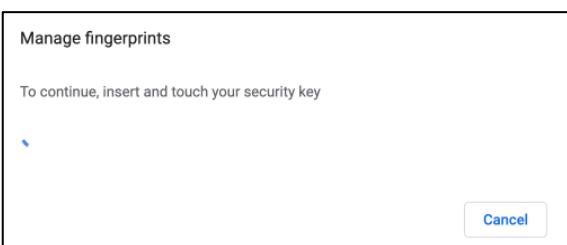


II.2.5. Xóa vân tay

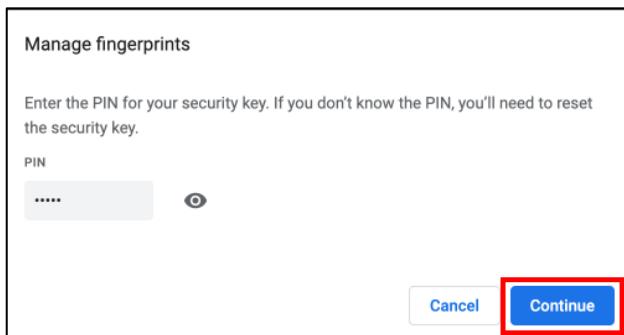
- Trên giao diện **Manage security keys** (*mở trình duyệt Chrome, chọn Setting > Privacy and security > Security > Manage security keys*), chọn **Fingerprints**.



- Chạm vào cảm biến vân tay trên khóa xác thực.



- Điền mã PIN (*đã tạo ở bước trên*), sau đó nhấn **Continue** để tiếp tục.

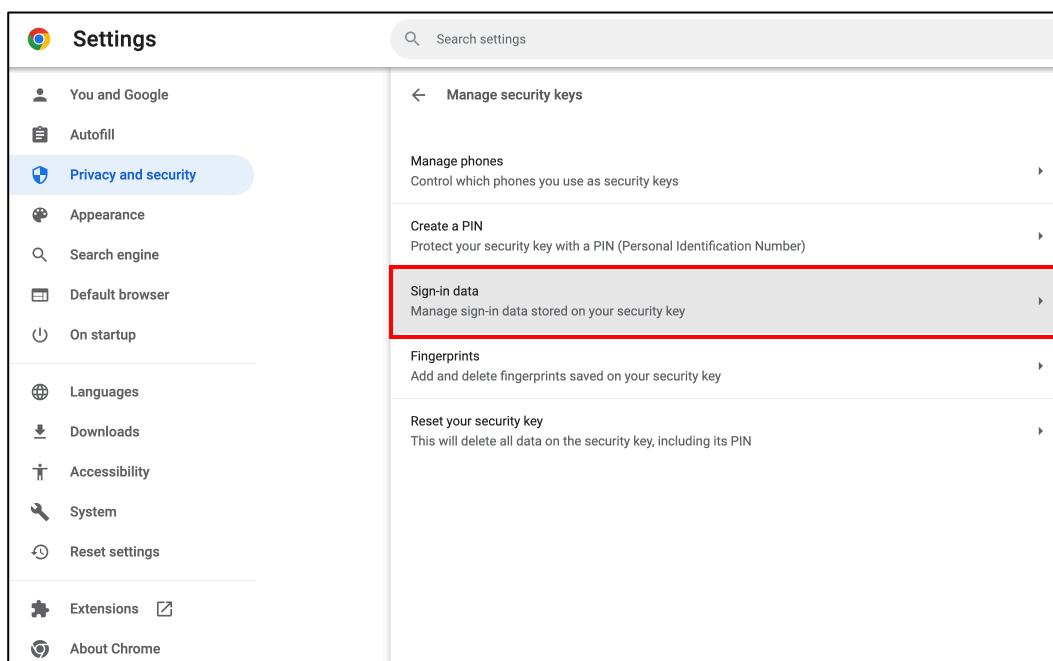


- Trên màn hình sẽ hiển thị danh sách vân tay đã được đăng ký trên khóa bảo mật. Nhấn vào biểu tượng chữ “X” tại mỗi vân tay tương ứng để xóa vân tay đã đăng ký.

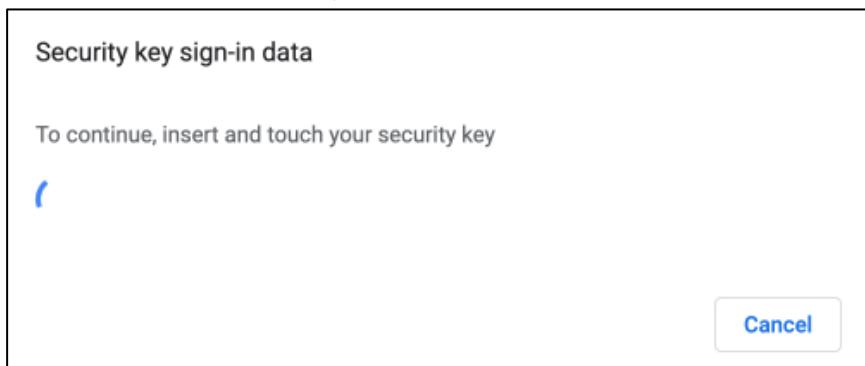


II.2.6. Quản lý dữ liệu đăng nhập

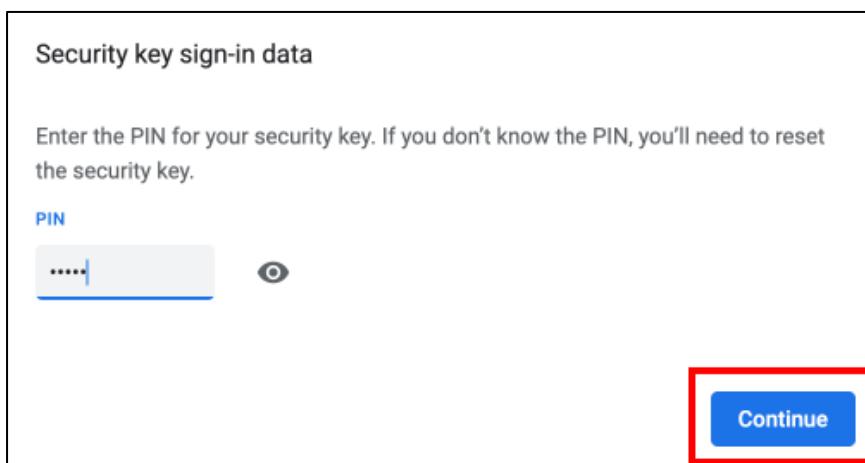
- Trên giao diện **Manage security keys** (*mở trình duyệt Chrome, chọn Setting > Privacy and security > Security > Manage security keys*), chọn **Sign-in data**.



- Chạm vào cảm biến vân tay trên khóa xác thực.



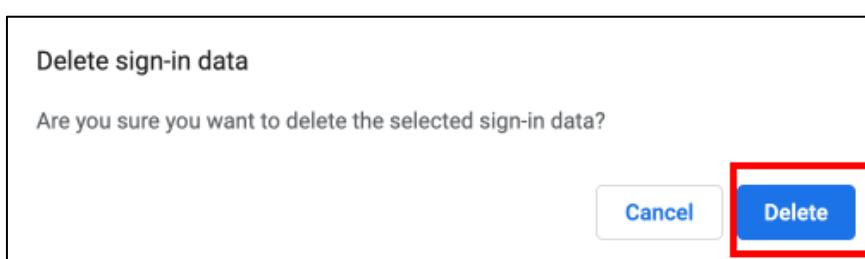
- Điền mã PIN (*đã tạo ở bước trên*), sau đó nhấn **Continue** để tiếp tục.



- Trên màn hình sẽ hiển thị danh sách dữ liệu đăng nhập, bao gồm tên website và tên đăng nhập.



- Để xóa dữ liệu đăng nhập, nhấp chọn vào biểu tượng  ở cuối mỗi dòng. Hộp thoại **Delete sign-in data** hiện ra. Nhấn **Delete**.



- Hoàn thành quá trình xoá dữ liệu đăng nhập. Quay trở lại hộp thoại **Security key sign-in data**. Nhấn **Done** để kết thúc.

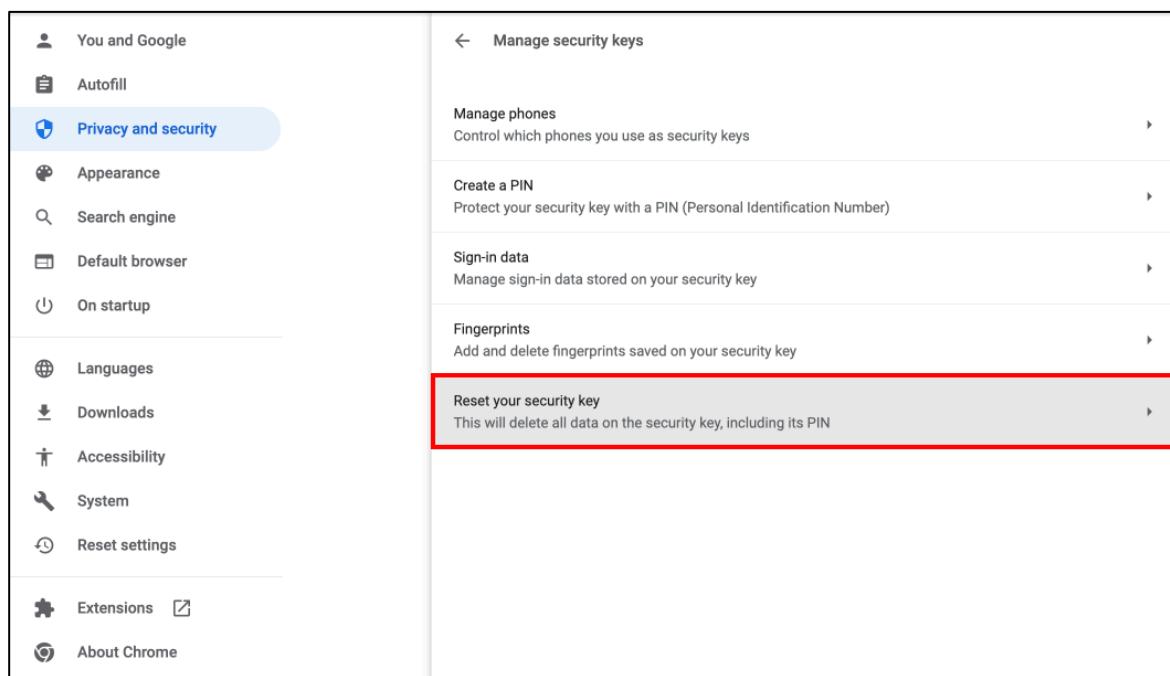


II.2.7. Thiết lập cài đặt gốc

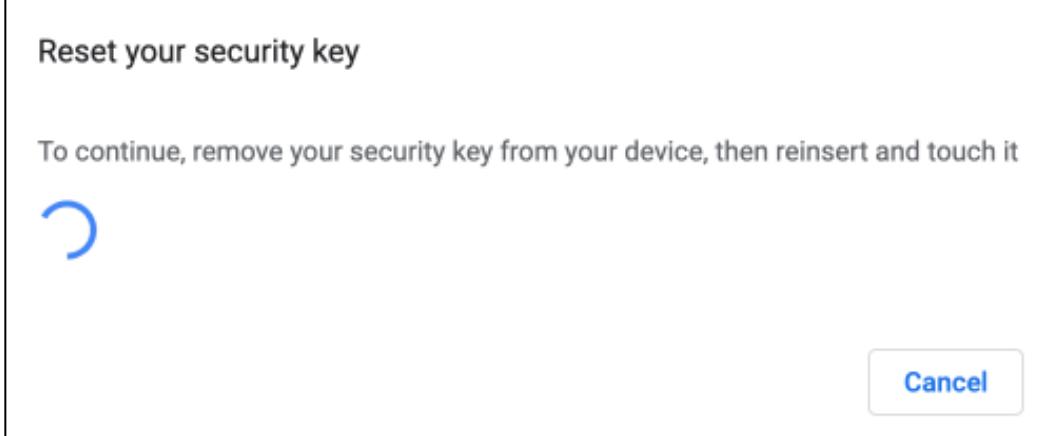
Trong trường hợp quên mã PIN của VinCSS FIDO2® Fingerprint, người dùng có thể reset thiết bị, tuy nhiên điều này sẽ khiến các dịch vụ đã đăng ký trước đó không thể xác thực được nữa. Sau khi reset, thiết bị trở thành khóa bảo mật mới, vì vậy cần đăng ký lại các dịch vụ để có thể xác thực. Trong trường hợp nhập sai mã PIN nhiều lần (*trên 8 lần*) thì thiết bị sẽ bị khóa vĩnh viễn, người dùng bắt buộc phải reset để có thể sử dụng lại khóa bảo mật VinCSS FIDO2® Fingerprint như một thiết bị mới.

Để reset VinCSS FIDO2® Fingerprint, thực hiện các bước sau:

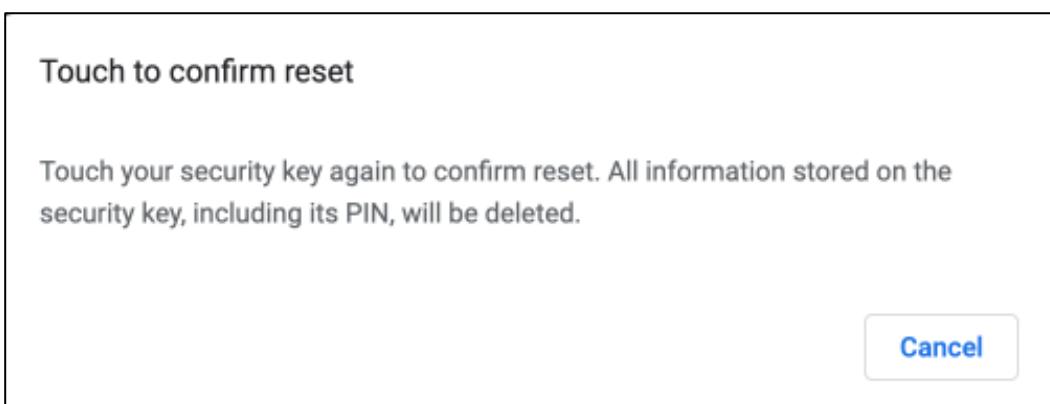
- Trên giao diện **Manage security keys** (*mở trình duyệt Chrome, chọn Setting > Privacy and security > Security > Manage security keys*), chọn **Reset your security key**.



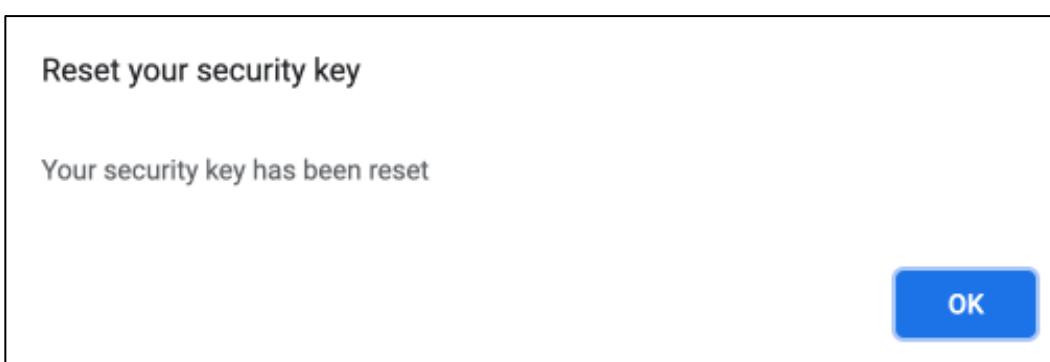
- Rút khoá bảo mật VinCSS FIDO2® Fingerprint ra khỏi máy tính và cắm lại. Chạm vào cảm biến vân tay trên khoá bảo mật để xác nhận.



- Chạm tiếp vào cảm biến vân tay trên VinCSS FIDO2® Fingerprint lần nữa để xác nhận việc reset VinCSS FIDO2® Fingerprint.



- Quá trình reset thành công. Nhấn **OK** để kết thúc.



II.3. Nền tảng Linux

II.3.1. USB

Kiểm tra phiên bản udev của thiết bị, người dùng chạy lệnh sau trong Terminal: “**sudo udevadm –version**”

Từ phiên bản udev 244 trở lên đã hỗ trợ sẵn khóa xác thực VinCSS FIDO2® Fingerprint. Với các phiên bản udev thấp hơn 244, ta cần thiết lập cấu hình “udev rules”. Để thiết lập hệ thống Linux:

- Xác minh rằng libu2f-udev đã được cài đặt trên hệ thống của bạn.
 - o Trên Debian và các phiên bản phát sinh của nó (*Ubuntu, Linux Mint, v.v.*), hãy kiểm tra xem libu2f-udev đã được cài đặt chưa bằng cách chạy lệnh sau trong Terminal: “`dpkg -s libu2f-udev`”
 - o Cài đặt bằng cách chạy lệnh sau trong Terminal (*Nếu đã được cài đặt, vui lòng bỏ qua bước này*): “`sudo apt cài đặt libu2f-udev`”
- Sao chép **99-vincss.rules** vào thư mục Linux: `/etc/udev/rules.d/`. Nếu tệp này đã có sẵn, hãy đảm bảo rằng nội dung trông giống như nội dung được cung cấp.



- Lưu tệp sau đó khởi động lại hệ thống.

Lưu ý:

- Nếu bạn đã thiết lập “udev rules” nhưng khoá xác thực vẫn không hoạt động, vui lòng liên hệ với chúng tôi để được hỗ trợ. Nguyên nhân có thể là do xung đột một số gói cài đặt trên thiết bị Linux.
- Các thao tác khác để quản lý khoá bảo mật được thực hiện trên trình duyệt Chrome (tương tự như nền tảng macOS – tham khảo mục [II.2. Nền tảng macOS](#)).

II.3.2. Bluetooth

Người dùng không nên ghép nối khoá xác thực VinCSS FIDO2® Fingerprint với Linux trong Settings/Bluetooth vì khi ghép nối khoá xác thực và thiết bị sẽ không cần mã PIN. Điều này khiến chức năng Bluetooth của khoá xác thực không hoạt động thiết bị. Để khắc phục, người dùng cần cài đặt Blueman Bluetooth Manager trên Ubuntu.

Điều kiện tiên quyết để cài đặt Blueman trên Ubuntu:

- Đã cài đặt và chạy Ubuntu.
- Kết nối Internet để tải xuống Blueman.
- Sudo Privileges.

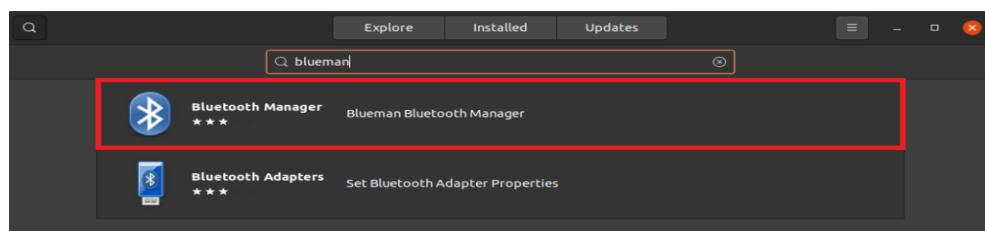
- Bộ chuyển đổi Bluetooth sẵn có hoặc bên ngoài.

Nếu Bluetooth chưa được thiết lập trên hệ thống, trước tiên hãy cài đặt BlueZ. Người dùng có thể kiểm tra xem libu2f-udev đã được cài đặt chưa bằng cách chạy lệnh sau trong Terminal: “**dpkg -s bluez**”.

- Cài đặt Bluez bằng lệnh sau: “**sudo apt install bluez bluez-tools**”.

II.3.2.1. Cài đặt Blueman trên Ubuntu

- Thông qua terminal: “**sudo apt install blueman**”
- Thông qua Ubuntu Software:
 - o Khởi động Ubuntu Software.
 - o Tìm kiếm rồi chọn Blueman Bluetooth Manager.



- o Nhấn để cài đặt và xác thực để cài đặt Blueman.

II.3.2.2. Kết nối khoá bảo mật VinCSS FIDO2® Fingerprint

- Mở Bluetooth Manager.
- Thiết lập thiết bị mới thông qua Bluetooth Manager, nhập mã PIN để sử dụng khoá bảo mật VinCSS FIDO2® Fingerprint trên Linux thông qua Bluetooth. (*Tham khảo phần II.2.2. Tao mới mã PIN để cài đặt mã PIN mới*).

III. XÁC THỰC KHÔNG MẬT KHẨU VỚI VINCSS FIDO2® FINGERPRINT

III.1. Đăng nhập với Window

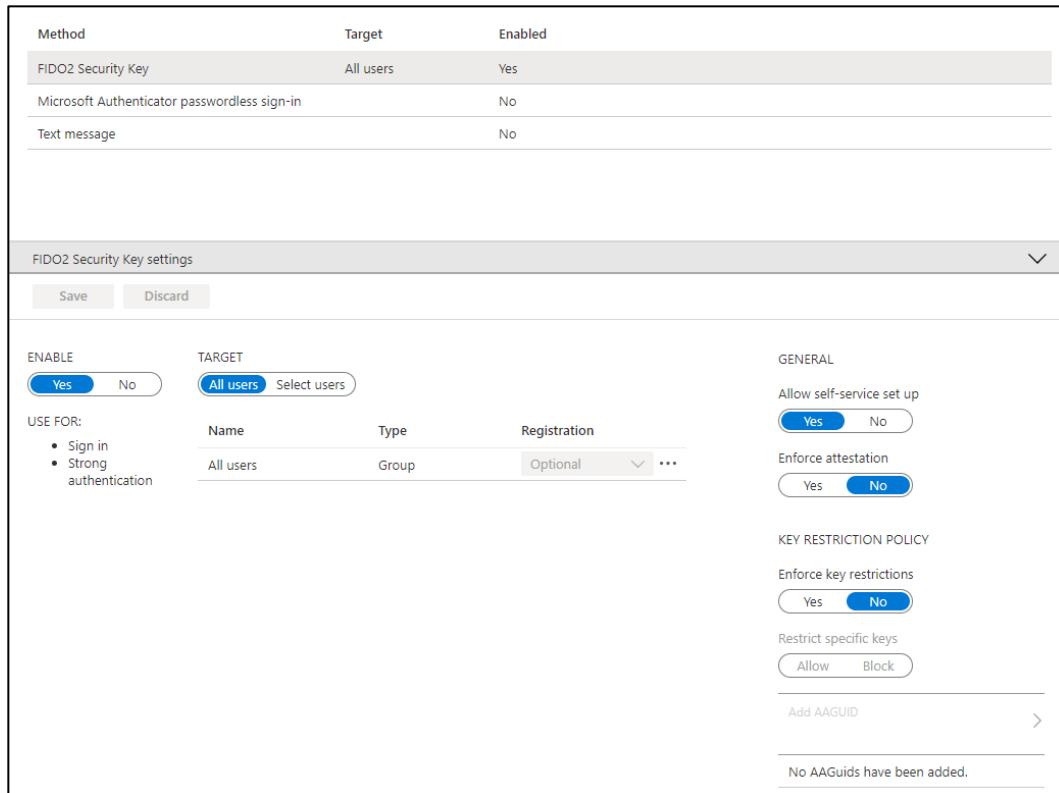
Lưu ý: Người dùng cần có tài khoản Azure AD.

III.1.1. Cấu hình trên hệ thống Azure AD

III.1.1.1. Cấu hình Azure AD

- Truy cập vào đường link sau: https://portal.azure.com/-blade/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/AdminAuthMethods

- Chọn **Method FIDO2 Security Key**, sau đó chọn các cấu hình như sau:

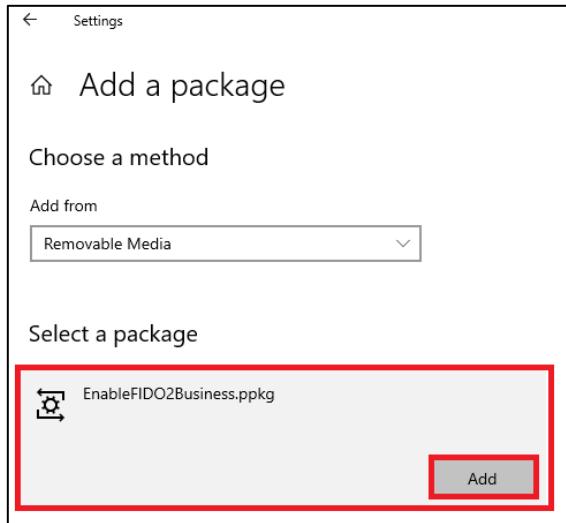


The screenshot shows the 'FIDO2 Security Key settings' page. At the top, there's a table with columns: Method, Target, and Enabled. The first row has 'FIDO2 Security Key' as the method, 'All users' as the target, and 'Yes' as the enabled status. Below this table, there's a section titled 'FIDO2 Security Key settings' with 'Save' and 'Discard' buttons. The main configuration area includes sections for 'ENABLE' (set to Yes), 'TARGET' (set to All users), 'GENERAL' (Allow self-service set up set to Yes, Enforce attestation set to No), 'KEY RESTRICTION POLICY' (Enforce key restrictions set to No, Restrict specific keys set to Allow), and an 'Add AAGUID' button. A note at the bottom says 'No AAGuids have been added.'

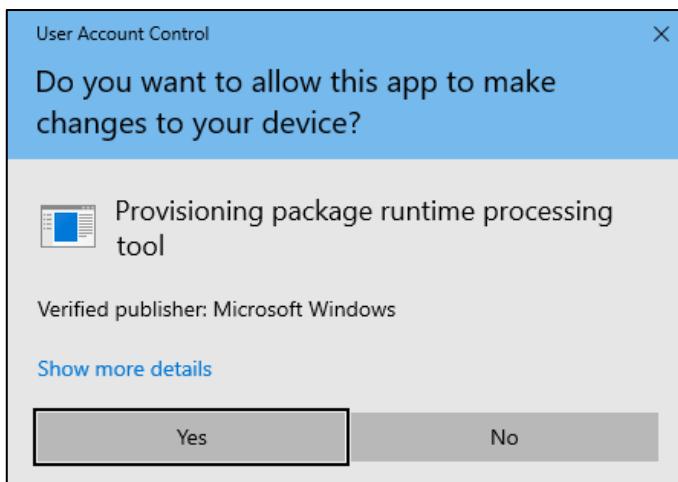
- Nhấn Save để lưu lại cấu hình.

III.1.1.2. Đăng nhập Windows 10 sử dụng FIDO2 với provisioning packages

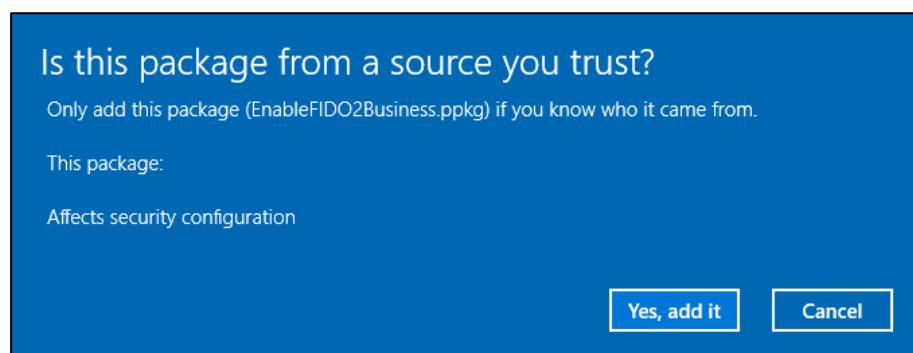
- Chuyển tải 2 file **EnableFIDO2Business.cat** và **EnableFIDO2Business.pkg** được VinCSS cung cấp vào thiết bị lưu trữ.
- Kết nối thiết bị lưu trữ đó với máy tính cần kích hoạt tính năng FIDO2, sau đó truy cập vào **Settings > Accounts > Access work or school > Add or remove a provisioning package > Add a package**, chọn vào gói và nhấn **Add**.



- Chọn Yes.

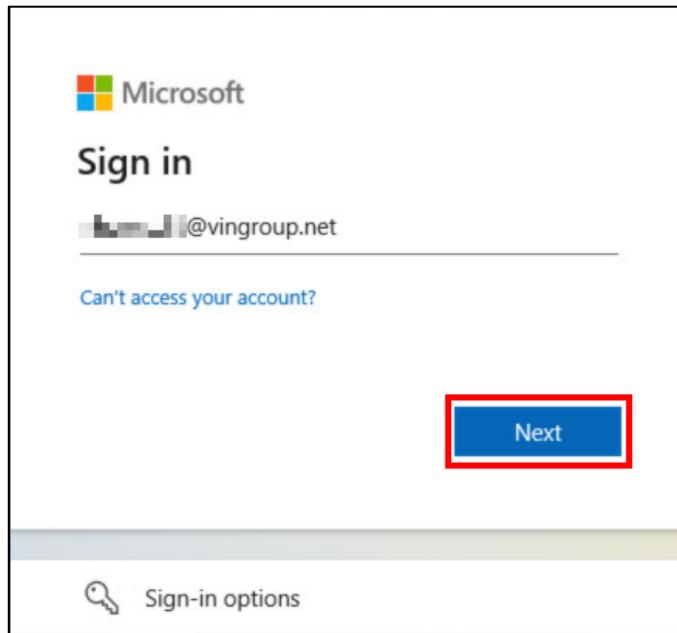


- Chọn Yes, add it.

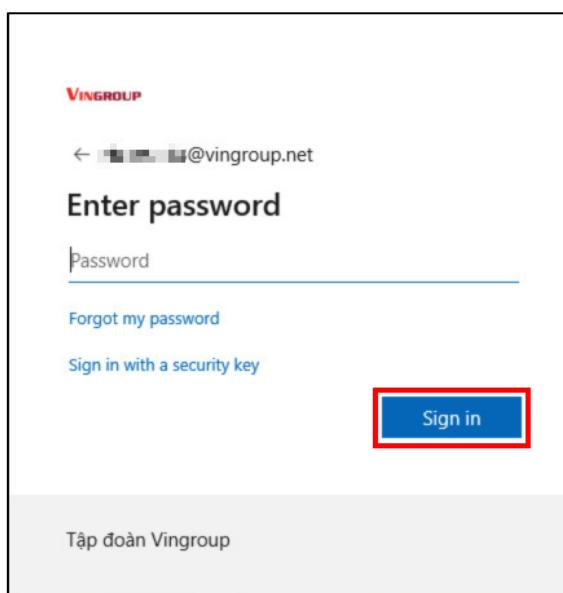


III.1.1.3. Đăng ký khóa xác thực cho tài khoản Azure AD

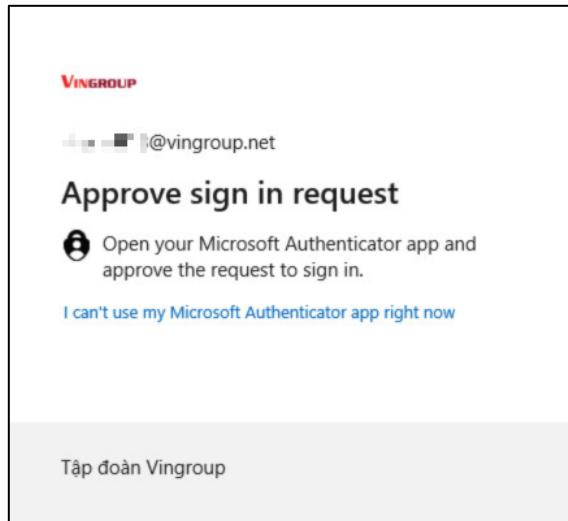
- Truy cập <https://myaccount.microsoft.com>, nhập thông tin tài khoản AD, sau đó nhấn Next.



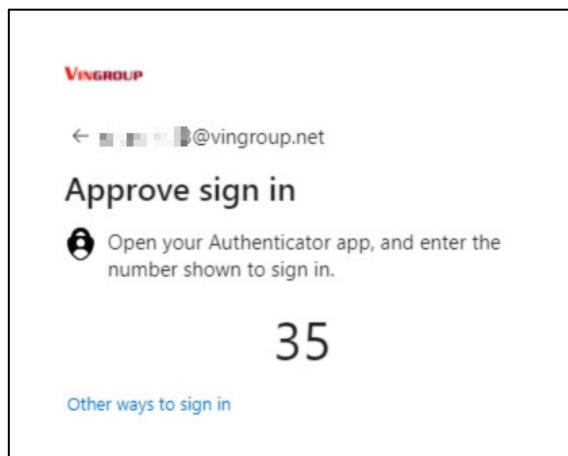
- Nhập mật khẩu của tài khoản AD rồi chọn **Sign in**.



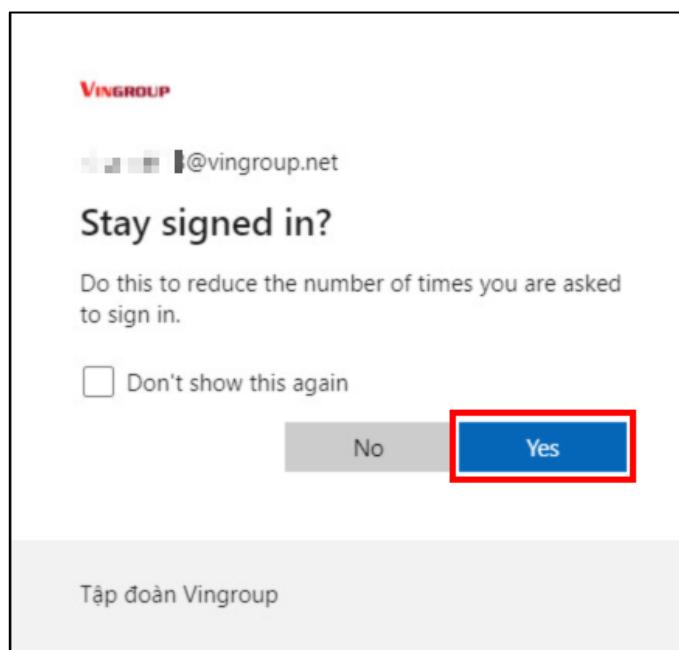
- Xác thực bằng ứng dụng Microsoft Authenticator trên điện thoại.



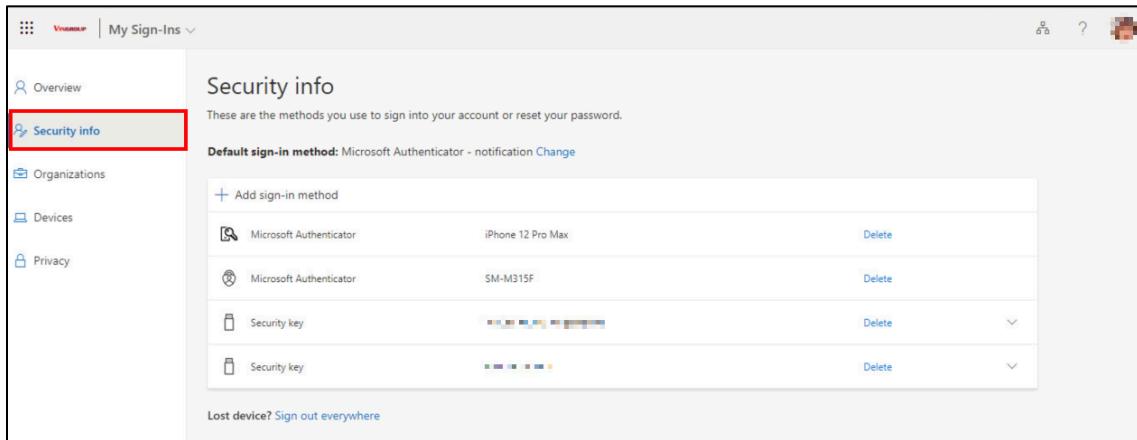
- Trên ứng dụng Authenticator, nhập vào điện thoại chữ số đã được hiển thị trên màn hình máy tính.



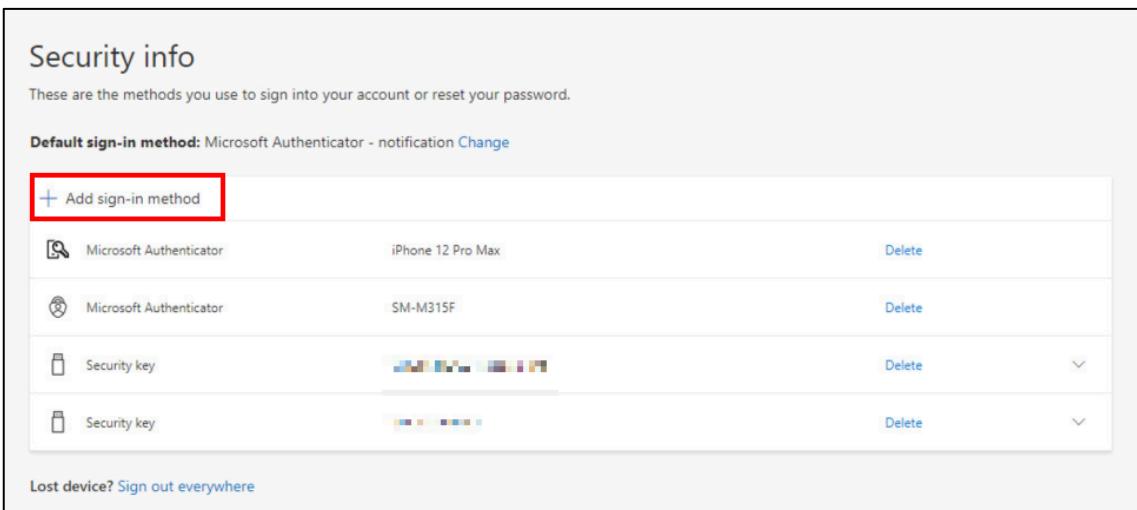
- Nhấn Yes để tiếp tục đăng nhập.



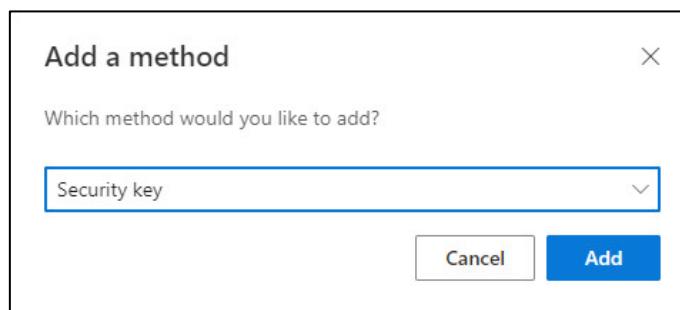
- Sau khi đăng nhập thành công, chọn **My sign-ins > Security info**.



- Chọn **Add sign-in method** để thêm phương thức bảo mật.

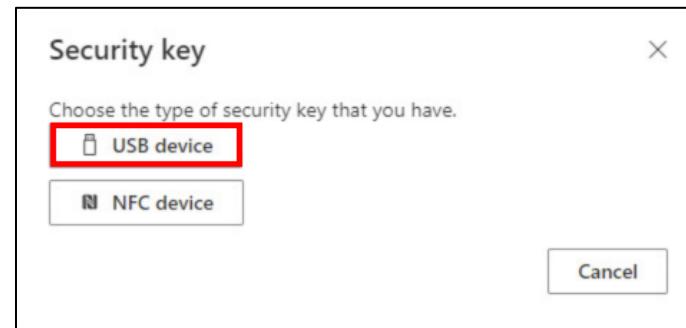


- Hộp thoại **Add a method** hiện ra, chọn **Security key** rồi nhấn **Add**.

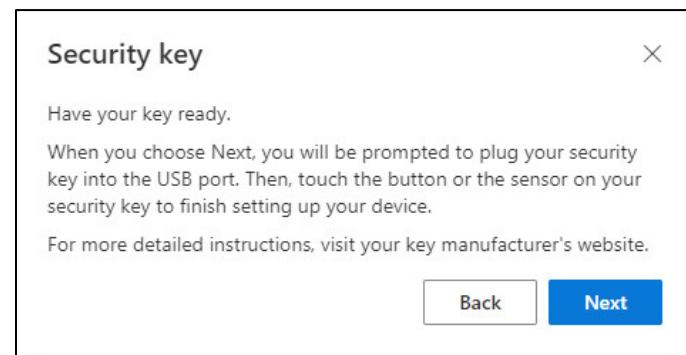


III.1.1.3.1. Sử dụng qua kết nối Bluetooth

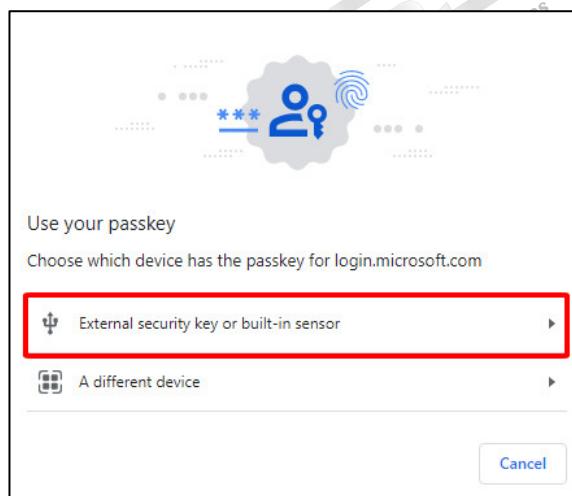
- Chọn **USB device**.



- Nhấn **Next** để tiếp tục.



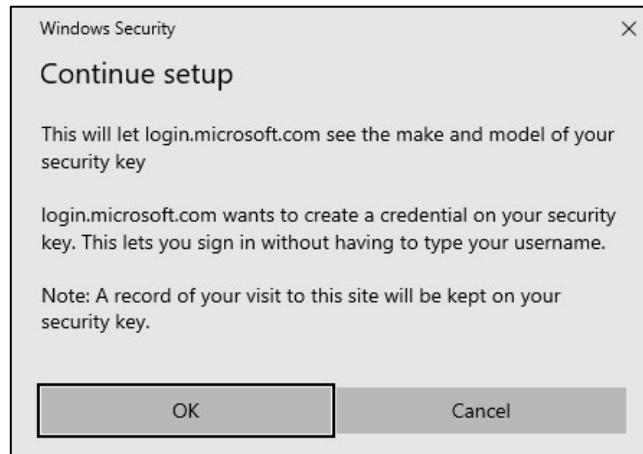
- Chọn **External security key or built-in sensor** để thiết lập khoá bảo mật.



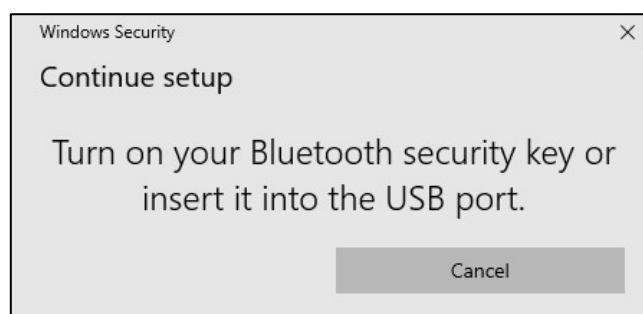
- Nhấn **OK** để tiếp tục thiết lập khoá bảo mật.



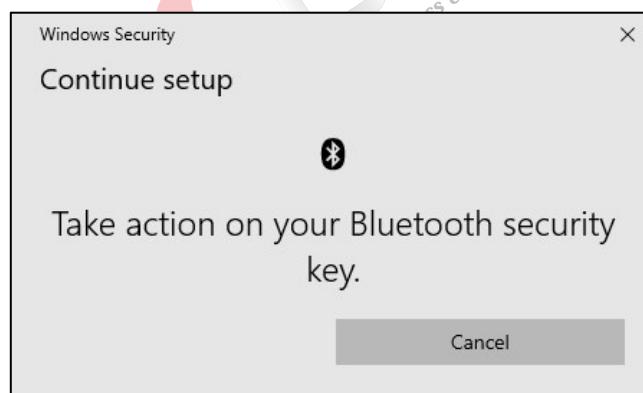
- Nhấn **OK** để tiếp tục.



- Kết nối khoá bảo mật với máy tính thông qua kết nối Bluetooth.

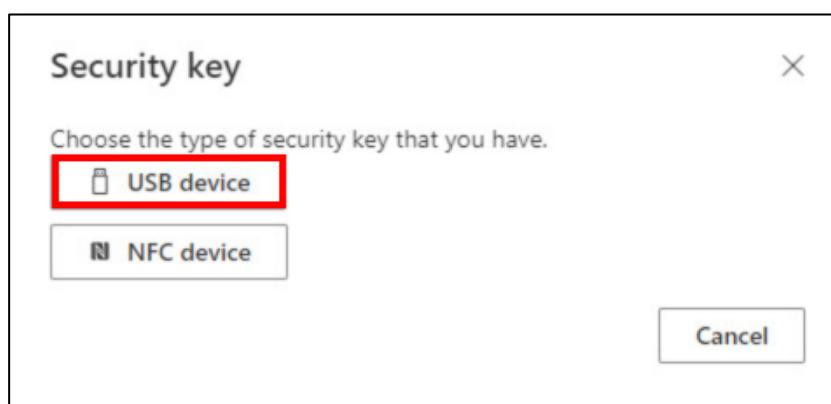


- Quét dấu vân tay khi nhận được thông báo.

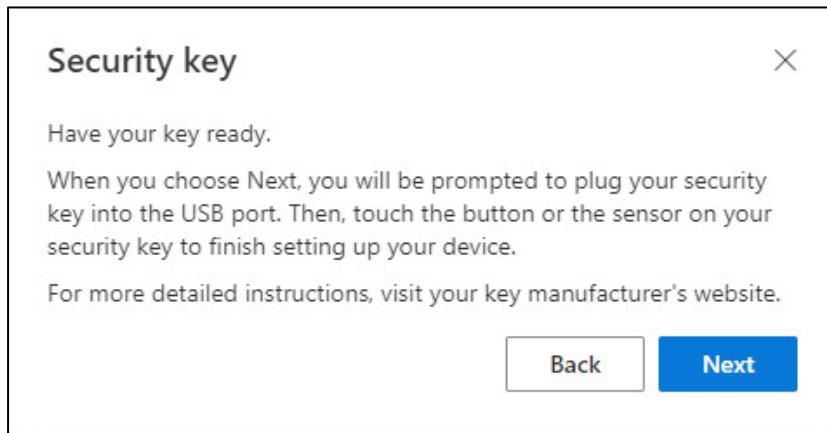


III.1.1.3.2. Sử dụng qua kết nối USB

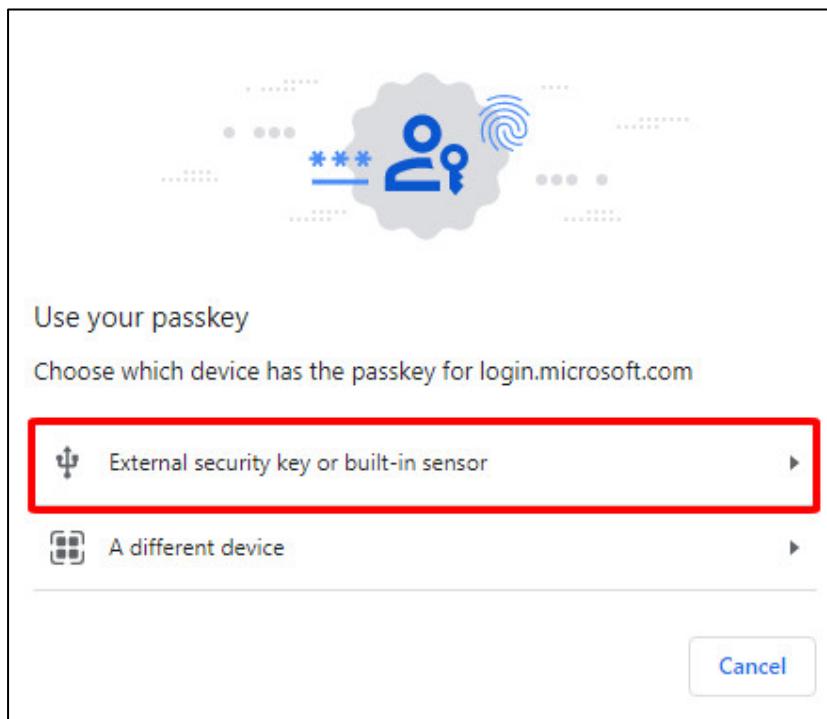
- Chọn **USB device**.



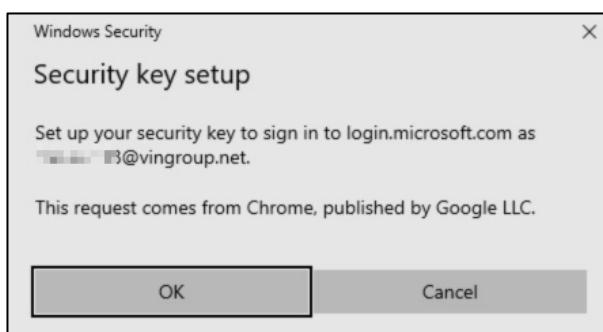
- Nhấn **Next** để tiếp tục.



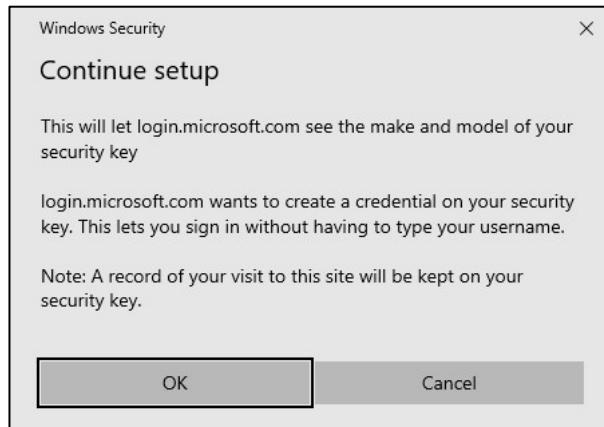
- Chọn **External security key or built-in sensor** để thiết lập khoá bảo mật.



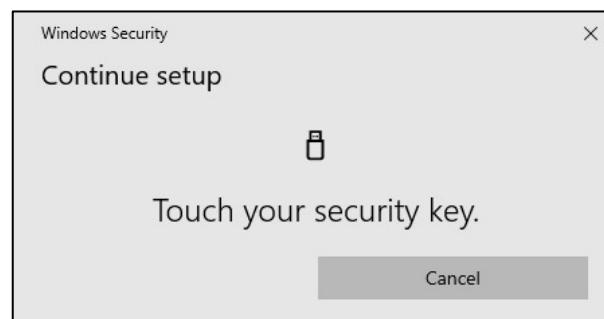
- Nhấn **OK** để tiếp tục thiết lập khoá bảo mật.



- Nhấn **OK** để tiếp tục.

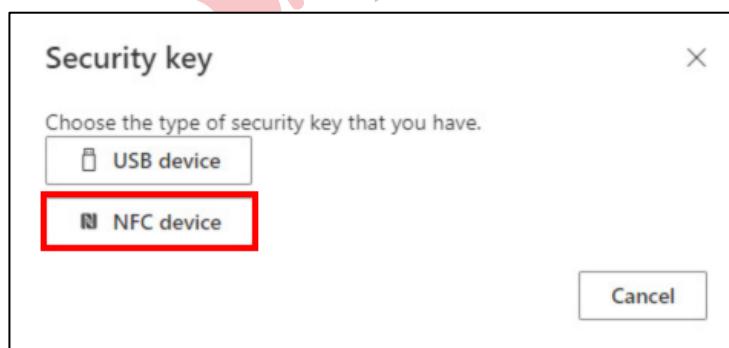


- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

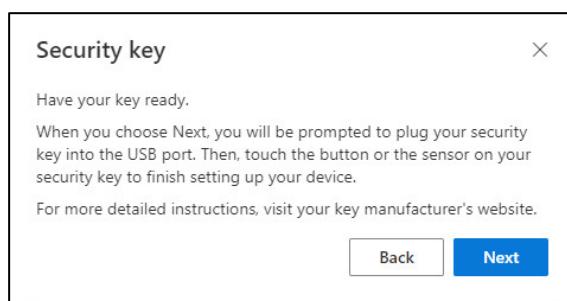


III.1.1.3.3. Sử dụng qua kết nối NFC

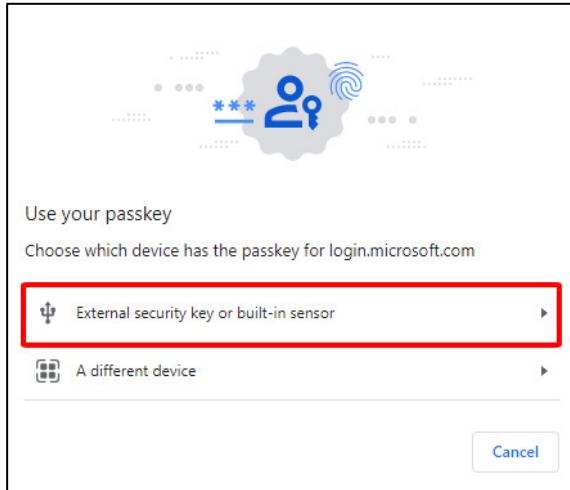
- Chọn **NFC device**.



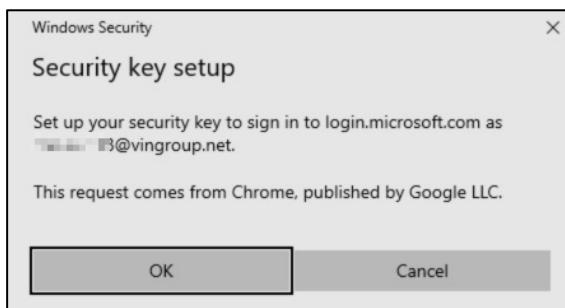
- Nhấn **Next** để tiếp tục.



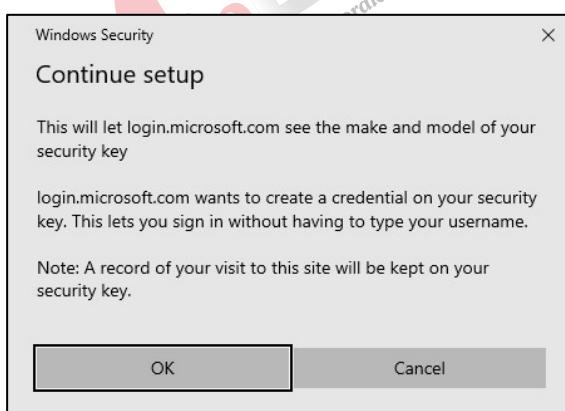
- Chọn **External security key or built-in sensor** để thiết lập khoá bảo mật.



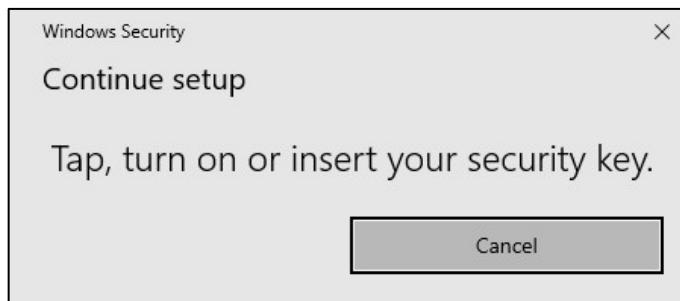
- Nhấn **OK** để tiếp tục thiết lập khoá bảo mật.



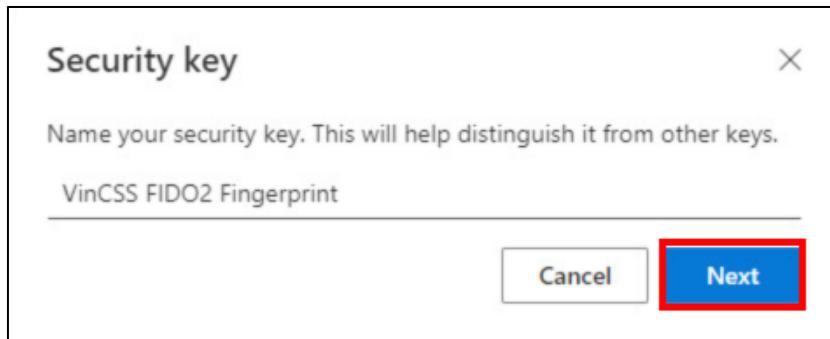
- Nhấn **OK** để tiếp tục.



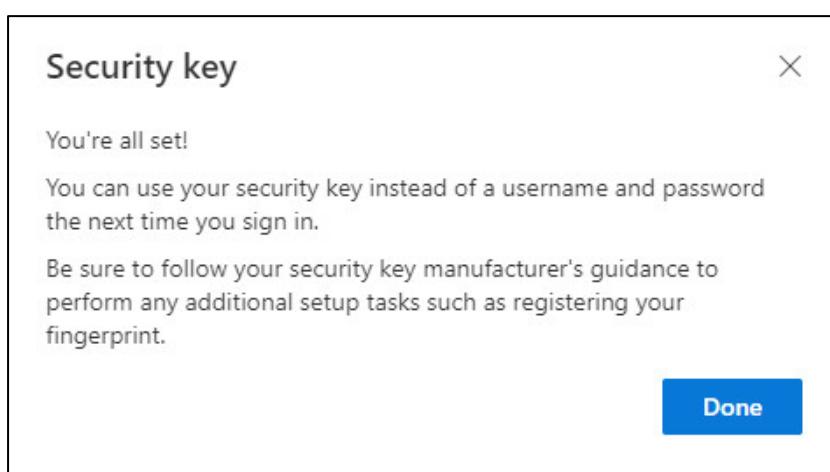
- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Đặt tên cho khoá bảo mật (*Tối đa 30 ký tự*) để phân biệt giữa các khoá rồi nhấn **Next**.

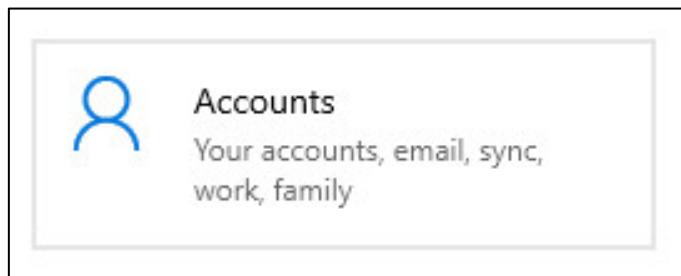


- Nhấn **Done** để hoàn tất đăng ký khoá bảo mật.

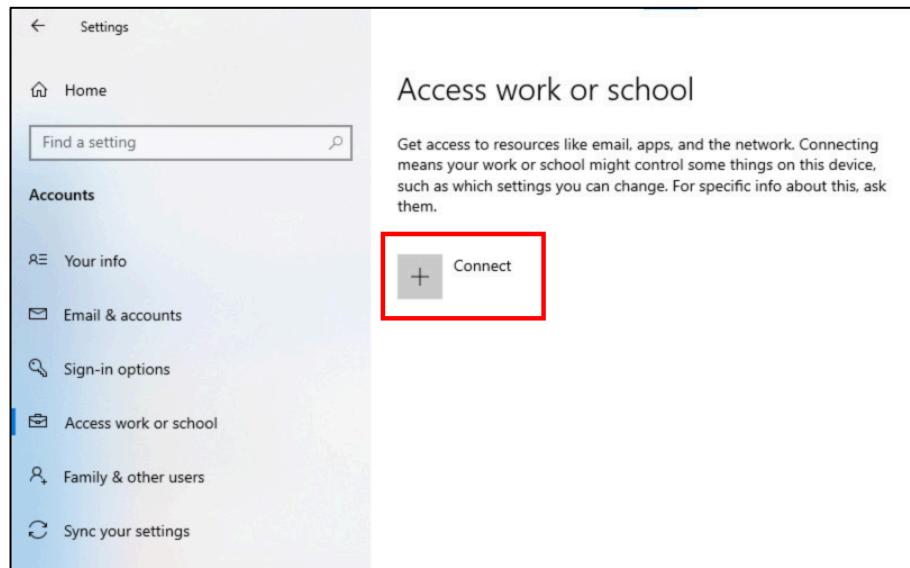


II.3.2.3. Kết nối User vào Azure Work Account

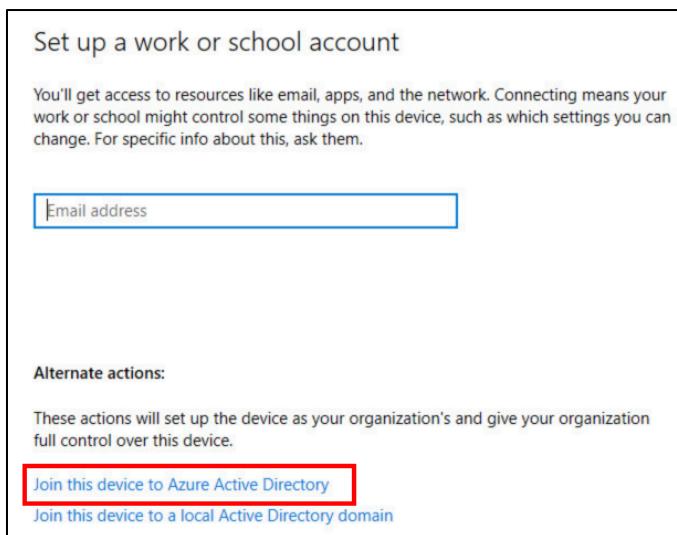
- Trên máy tính Windows, chọn **Settings > Account**.



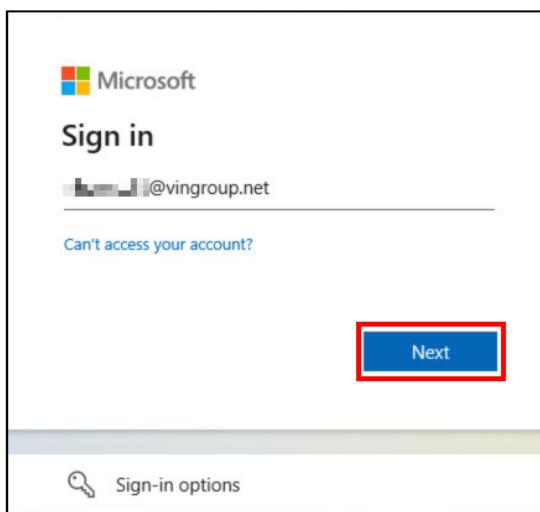
- Chọn **Access work or school > Connect**.



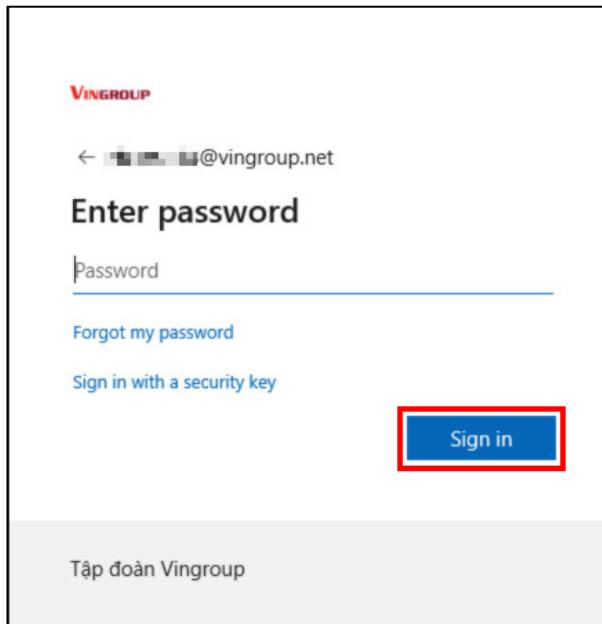
- Chọn **Join this device to Azure Active Directory.**



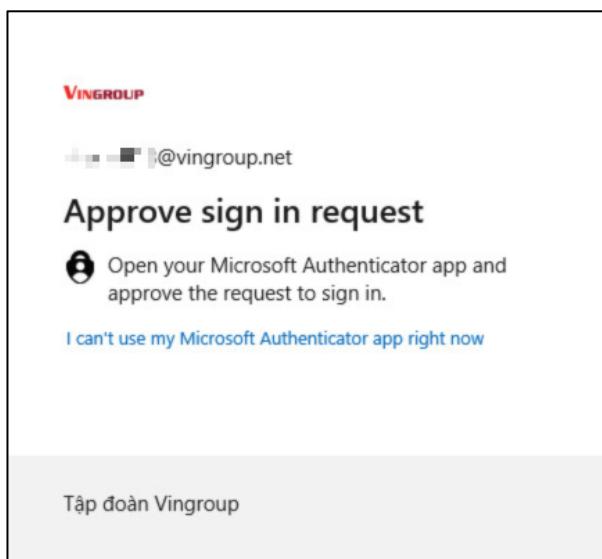
- Nhập thông tin tài khoản AD, sau đó nhấn **Next**.



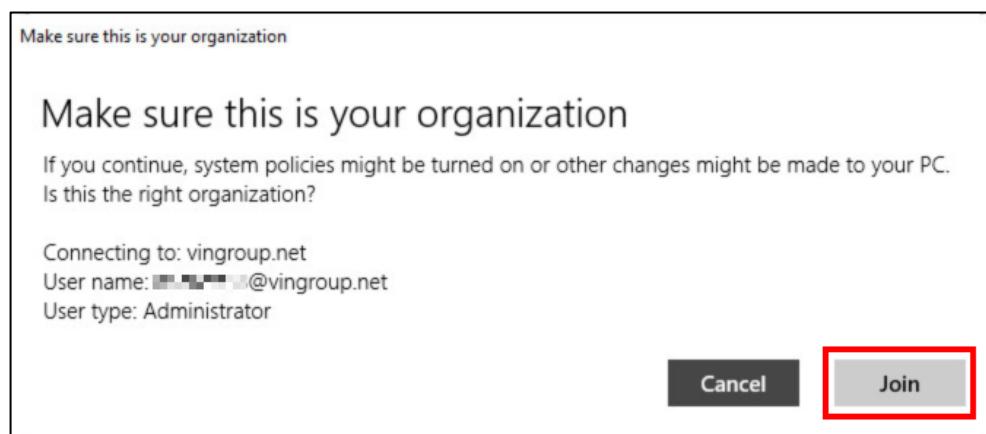
- Nhập mật khẩu của tài khoản AD rồi chọn **Sign in**.



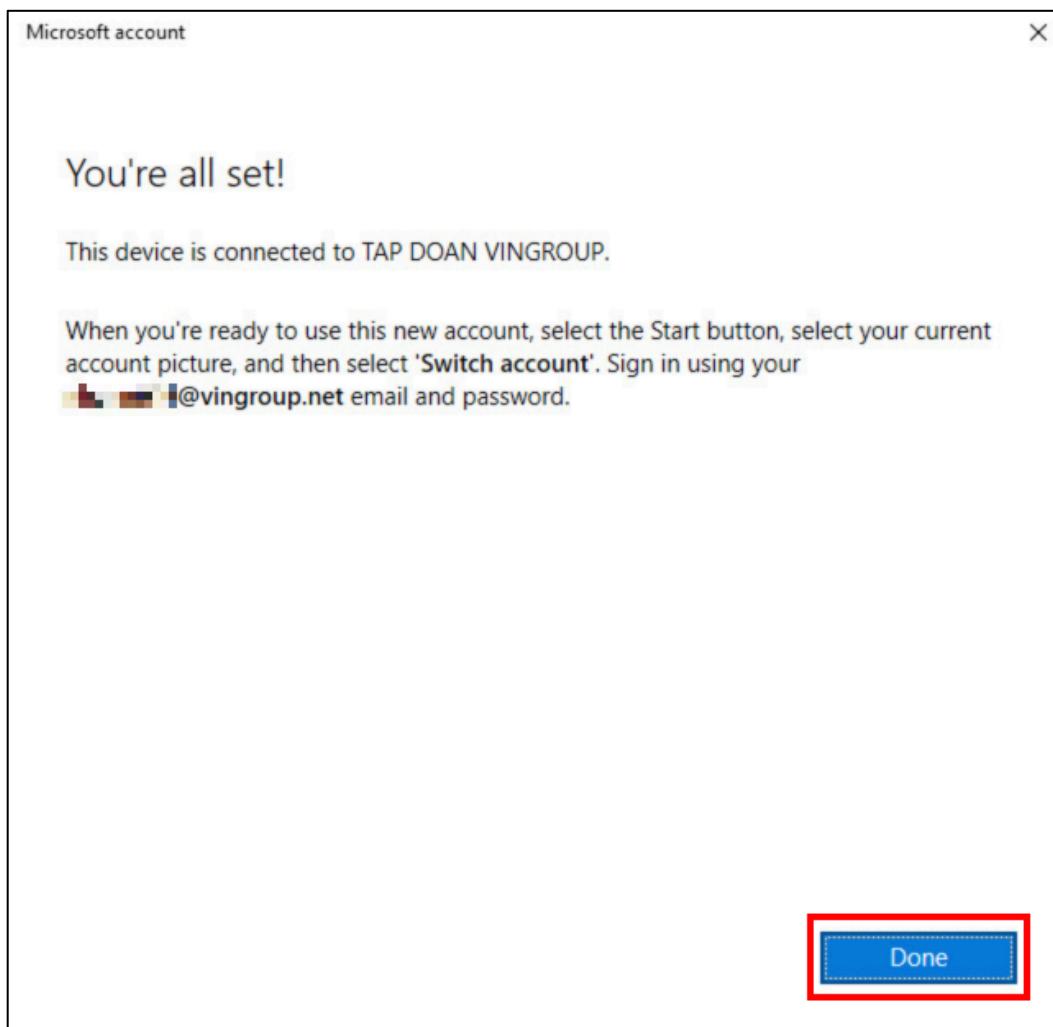
- Xác thực bằng ứng dụng Microsoft Authenticator trên điện thoại.



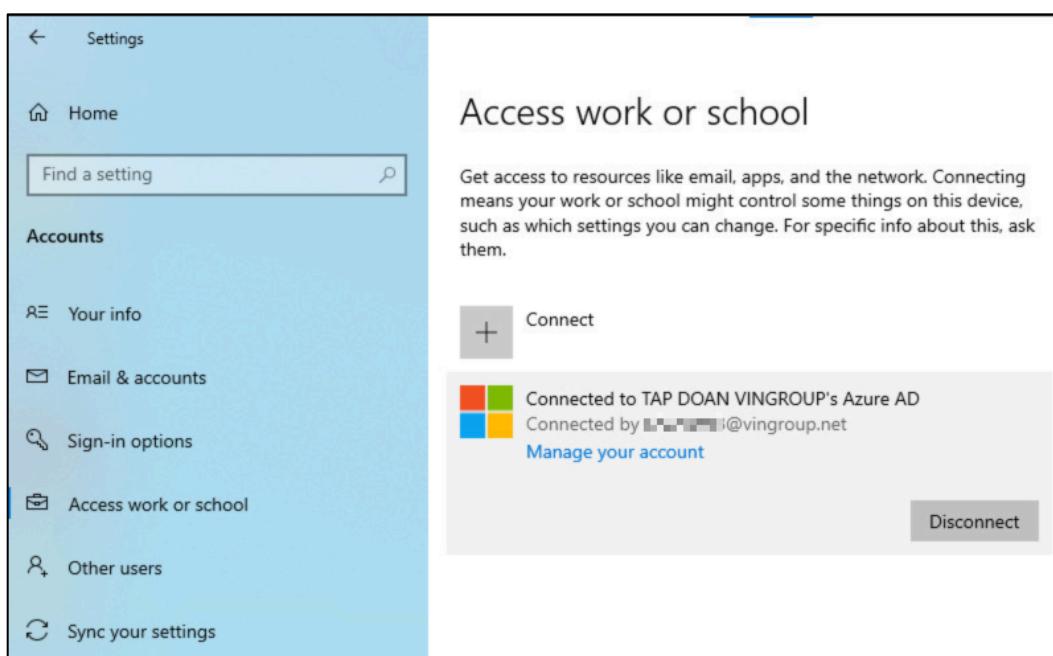
- Kiểm tra thông tin, sau đó nhấn **Join**.



- Nhấn **Done** để kết thúc.

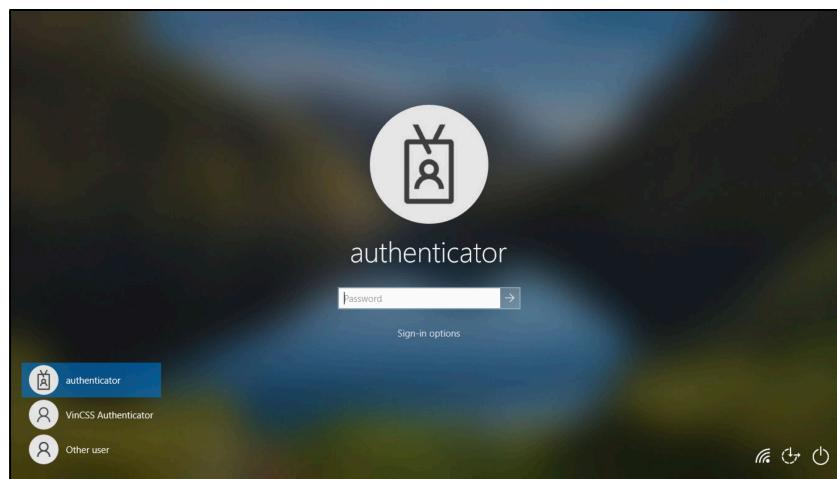


- Kết nối thành công, màn hình hiển thị như hình dưới.

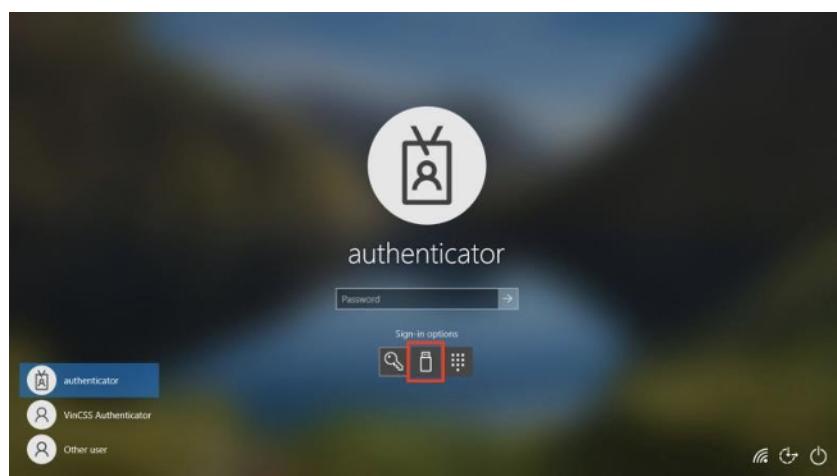


III.1.2. Đăng nhập Windows

- Trên giao diện đăng nhập vào Windows 10, chọn **Sign-in options**.

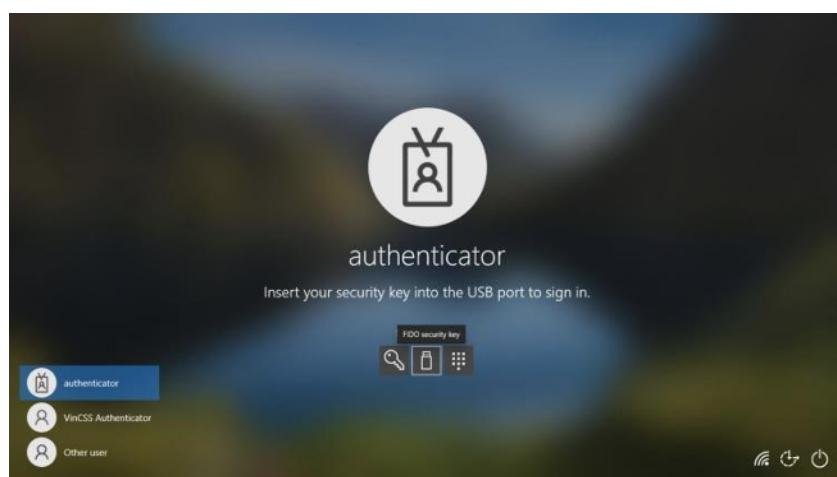


- Để lựa chọn đăng nhập Windows 10 với khoá bảo mật VinCSS FIDO2® Fingerprint thông qua kết nối Bluetooth.



III.1.2.1. Sử dụng qua kết nối Bluetooth.

- Kết nối khoá bảo mật với máy tính thông qua kết nối Bluetooth.



- Quét vân tay khi nhận được thông báo.



III.1.2.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

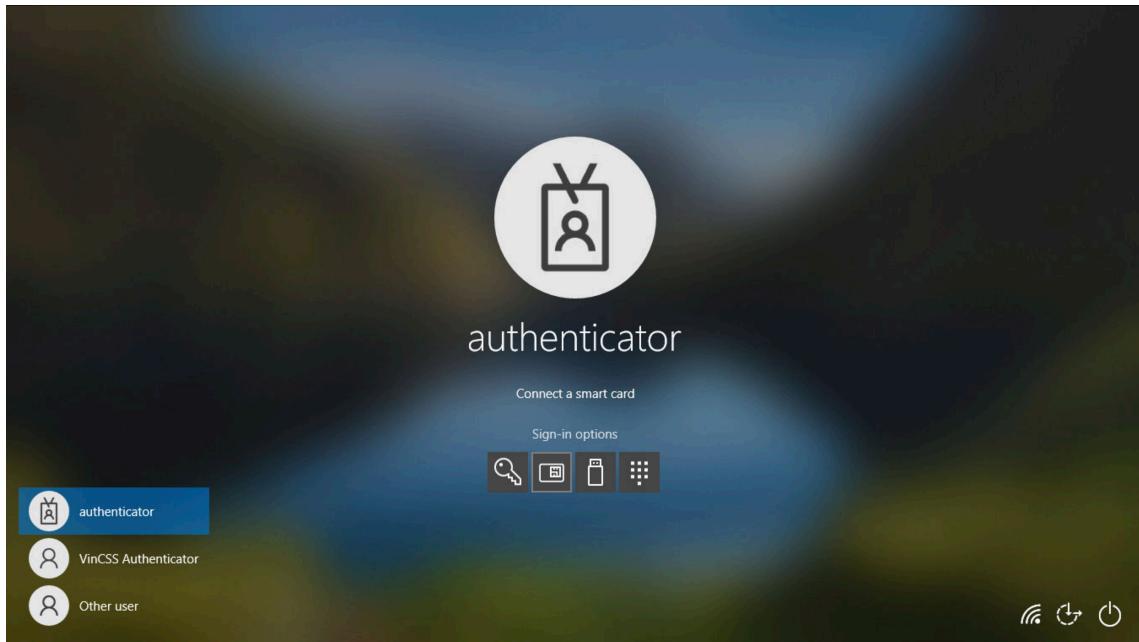


III.1.2.3. Sử dụng qua kết nối NFC

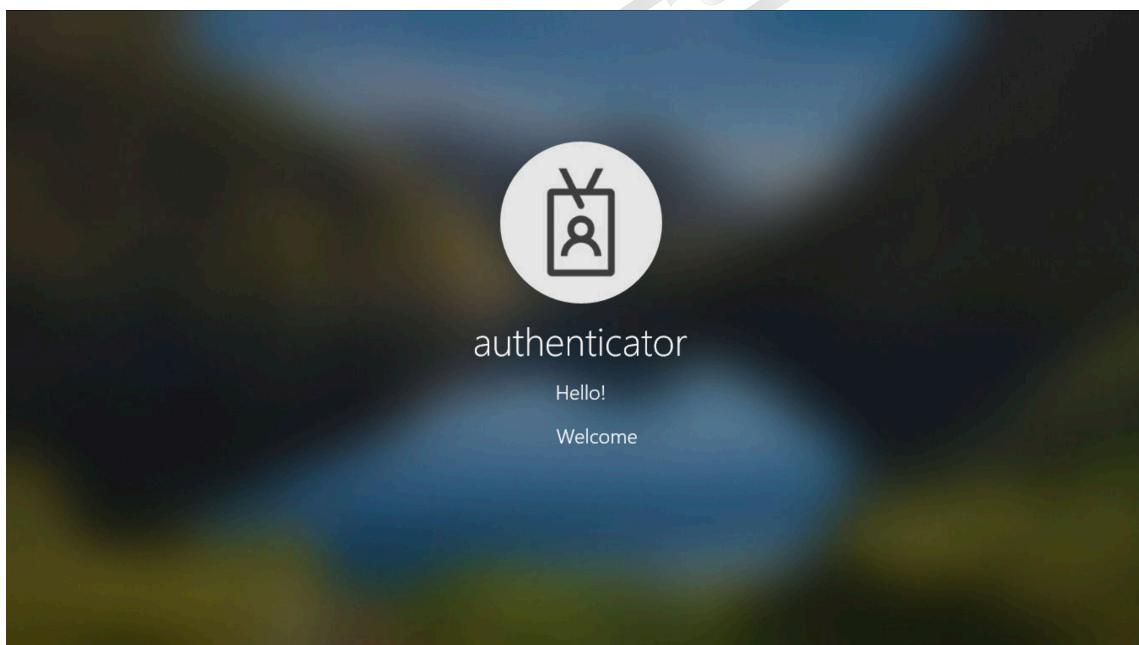
- Để lựa chọn đăng nhập Windows 10 với khoá bảo mật VinCSS FIDO2® Fingerprint thông qua kết nối NFC, chọn biểu tượng smart card.



- Kết nối khoá bảo mật với máy tính thông qua kết nối NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Đăng nhập thành công.



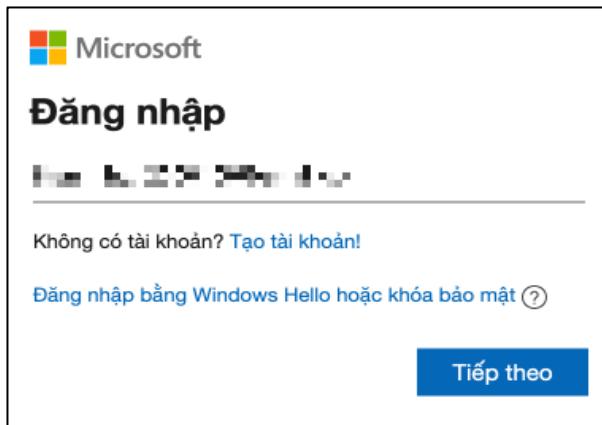
III.2. Xác thực không mật khẩu tài khoản Microsoft

III.2.1. Đăng ký khóa bảo mật

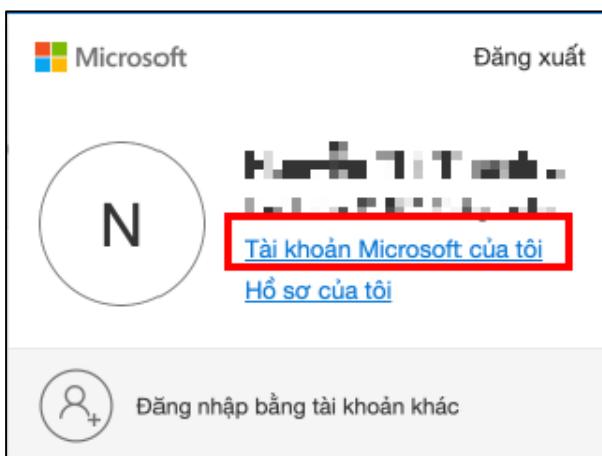
- Truy cập <https://microsoft.com>, chọn Đăng nhập.



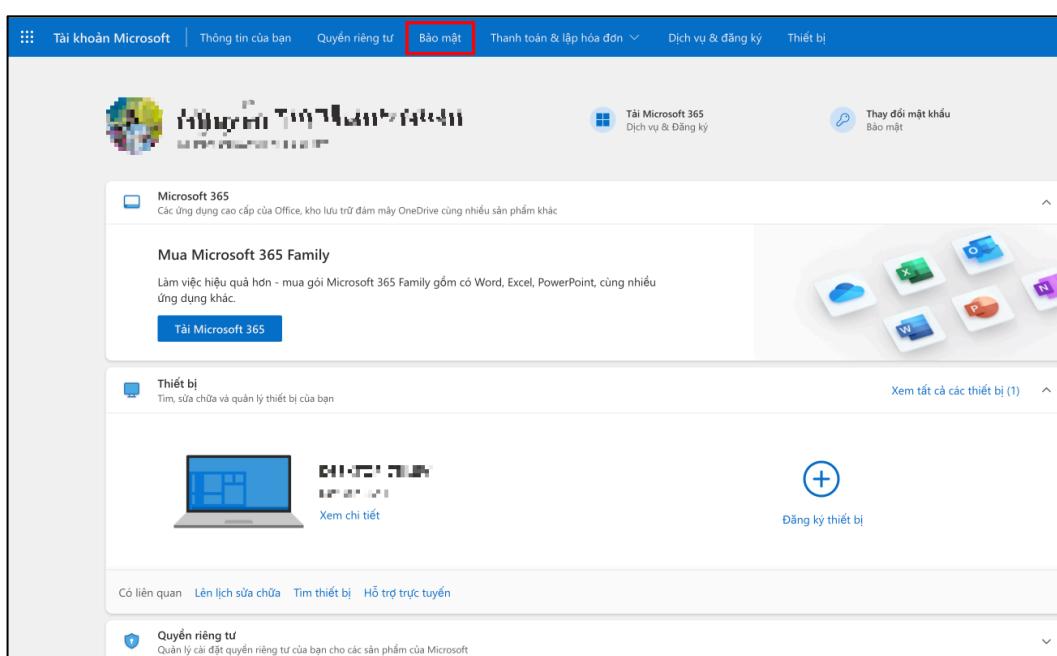
- Nhập thông tin tài khoản/mật khẩu rồi nhấn **Tiếp theo** để đăng nhập.



- Sau khi đăng nhập thành công, Chọn **Tài khoản Microsoft của tôi** để tiến hành cấu hình.

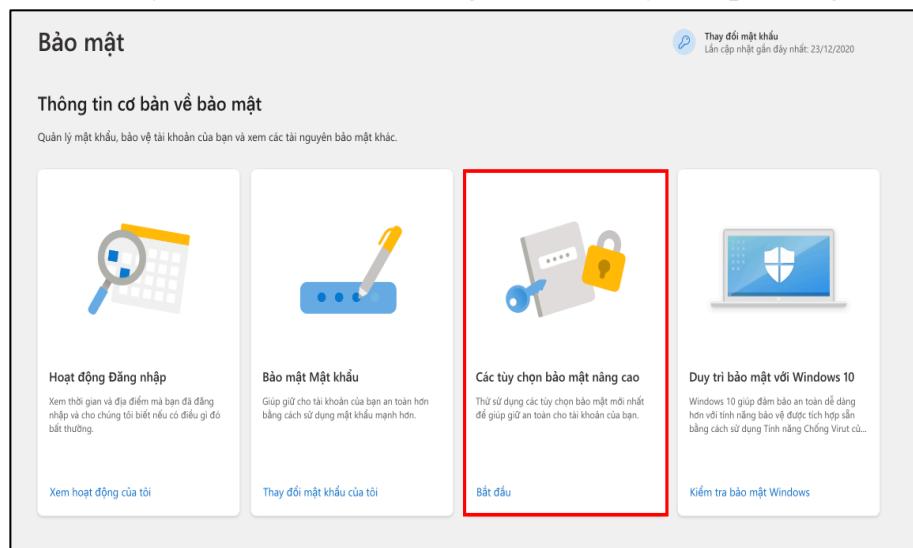


- Chọn mục **Bảo mật**.



The screenshot shows the Microsoft Security settings page. The top navigation bar has tabs: Tài khoản Microsoft, Thông tin của bạn, Quyền riêng tư, **Bảo mật** (highlighted with a red box), Thanh toán & lập hóa đơn, Dịch vụ & đăng ký, and Thiết bị. The main content area includes sections for Microsoft 365 (with a 'Tài Microsoft 365' button), Mua Microsoft 365 Family (with a 'Tài Microsoft 365' button), Thiết bị (with a 'Thay đổi mật khẩu' button), and Quyền riêng tư (with a 'Quản lý cài đặt quyền riêng tư' button). A large blue '+' icon is visible on the right side.

- Chọn **Các tùy chọn bảo mật nâng cao** để thay đổi phương thức bảo mật.



Bảo mật

Thông tin cơ bản về bảo mật

Quản lý mật khẩu, bảo vệ tài khoản của bạn và xem các tài nguyên bảo mật khác.

Hoạt động Đăng nhập
Xem thời gian và địa điểm mà bạn đã đăng nhập và cho chúng tôi biết nếu có điều gì đó bất thường.

Bảo mật Mật khẩu
Giúp giữ cho tài khoản của bạn an toàn hơn bằng cách sử dụng mật khẩu mạnh hơn.

Các tùy chọn bảo mật nâng cao
Thử dùng các tùy chọn bảo mật mới nhất để giúp an toàn cho tài khoản của bạn.

Duy trì bảo mật với Windows 10
Windows 10 giúp đảm bảo an toàn dễ dàng hơn với tính năng bảo vệ được tích hợp sẵn bằng cách sử dụng Tính năng Chống Virus cũ...

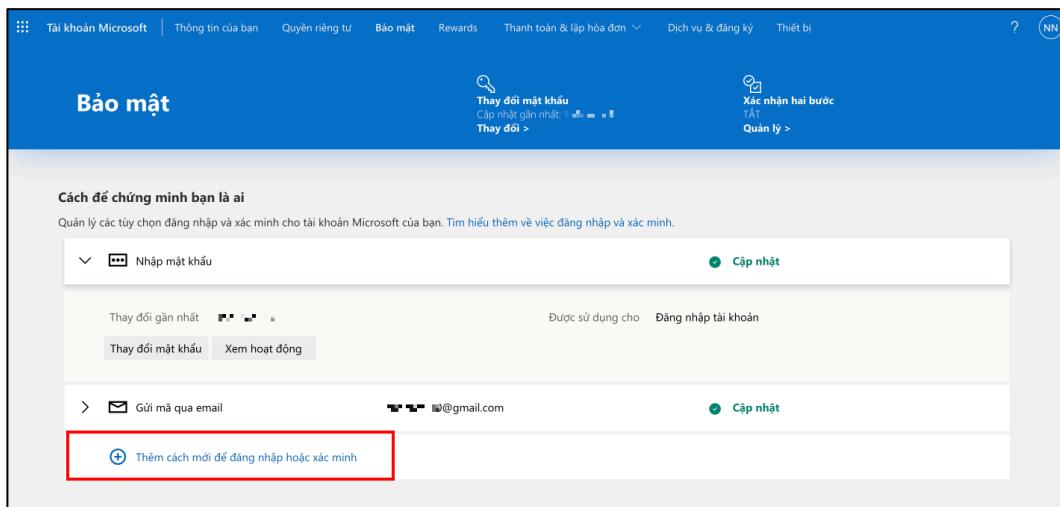
Bắt đầu

Xem hoạt động của tôi

Thay đổi mật khẩu của tôi

Kiểm tra bảo mật Windows

- Chọn **Thêm cách mới để đăng nhập hoặc xác minh**.



Tài khoản Microsoft | Thông tin của bạn | Quyền riêng tư | Bảo mật | Rewards | Thanh toán & lập hóa đơn | Dịch vụ & đăng ký | Thiết bị | ? (NN)

Bảo mật

Thay đổi mật khẩu
Cập nhật gần nhất: 23/12/2020
Thay đổi >

Xác nhận hai bước
Quản lý >

Cách để chứng minh bạn là ai
Quản lý các tùy chọn đăng nhập và xác minh cho tài khoản Microsoft của bạn. [Tim hiểu thêm về việc đăng nhập và xác minh.](#)

Nhập mật khẩu **Cập nhật**

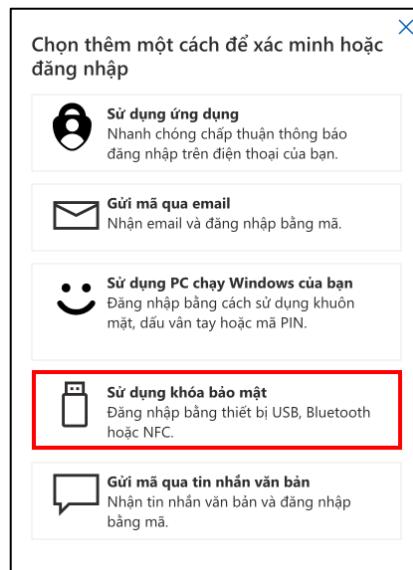
Thay đổi gần nhất: **Đang sử dụng** | **Đăng nhập tài khoản**

Thay đổi mật khẩu | Xem hoạt động

Gửi mã qua email **Cập nhật**

+ Thêm cách mới để đăng nhập hoặc xác minh

- Chọn **Sử dụng khóa bảo mật**.



Chọn thêm một cách để xác minh hoặc đăng nhập

Sử dụng ứng dụng
Nhanh chóng chấp thuận thông báo đăng nhập trên điện thoại của bạn.

Gửi mã qua email
Nhận email và đăng nhập bằng mã.

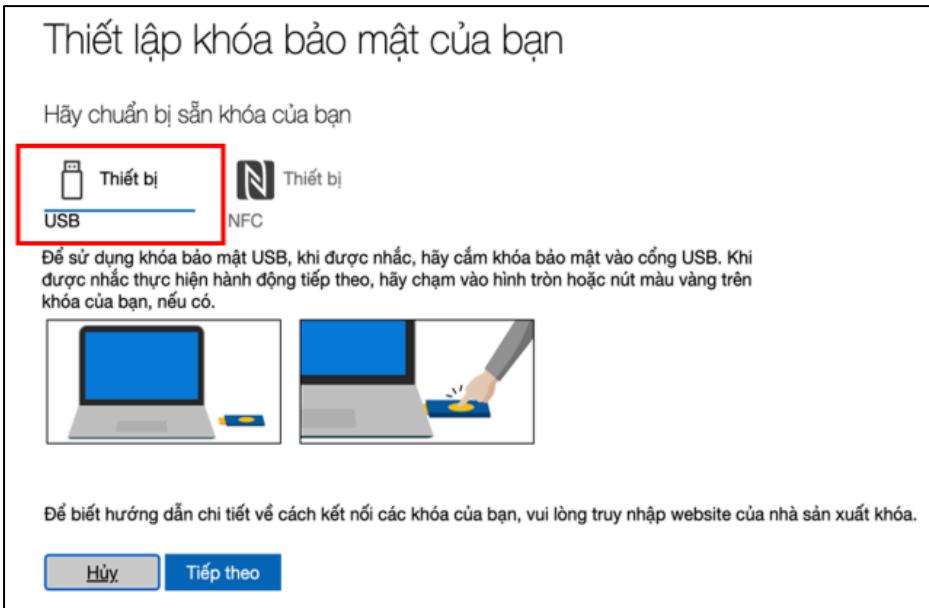
Sử dụng PC chạy Windows của bạn
Đăng nhập bằng cách sử dụng khuôn mặt, dấu vân tay hoặc mã PIN.

Sử dụng khóa bảo mật
Đăng nhập bằng thiết bị USB, Bluetooth hoặc NFC.

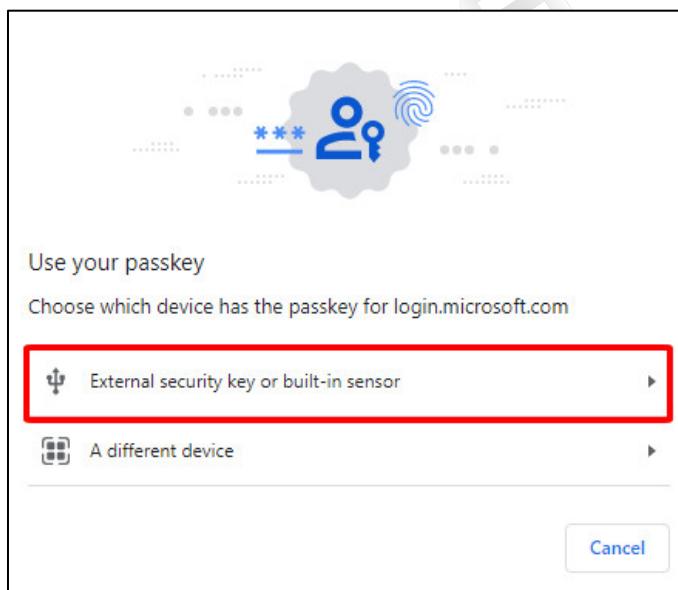
Gửi mã qua tin nhắn văn bản
Nhận tin nhắn văn bản và đăng nhập bằng mã.

III.2.1.1. Sử dụng qua kết nối Bluetooth

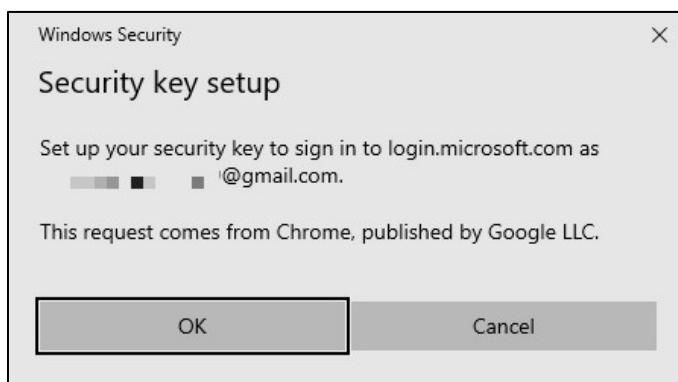
- Chọn **Thiết bị USB**, nhấn Tiếp theo.



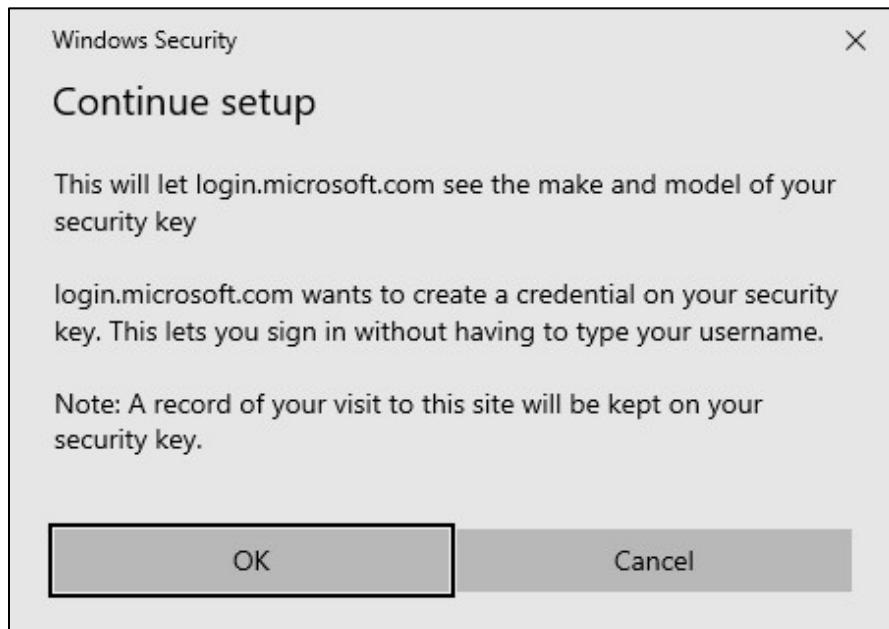
- Chọn **External security key or built-in sensor** để thiết lập khoá bảo mật.



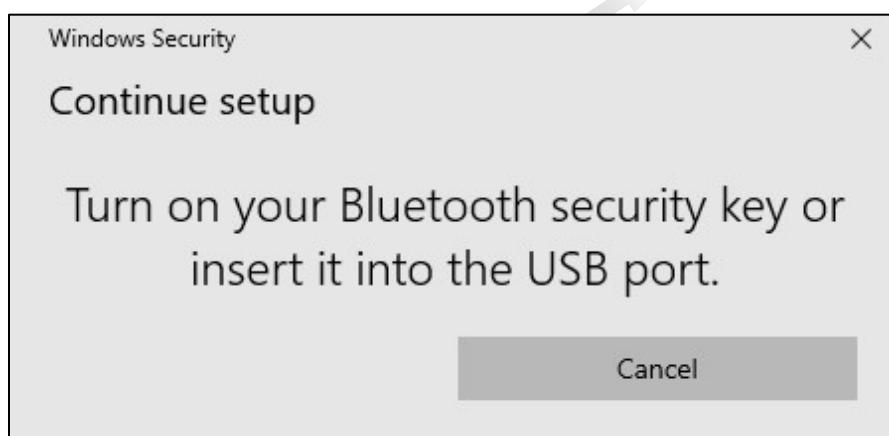
- Nhấn **OK** để tiếp tục thiết lập khoá bảo mật.



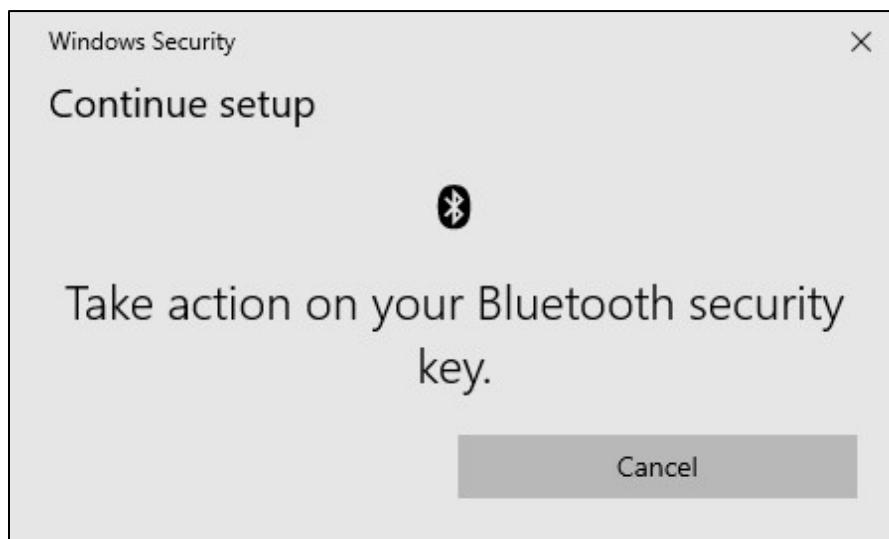
- Nhấn **OK** để tiếp tục.



- Kết nối khoá bảo mật với máy tính thông qua kết nối Bluetooth.

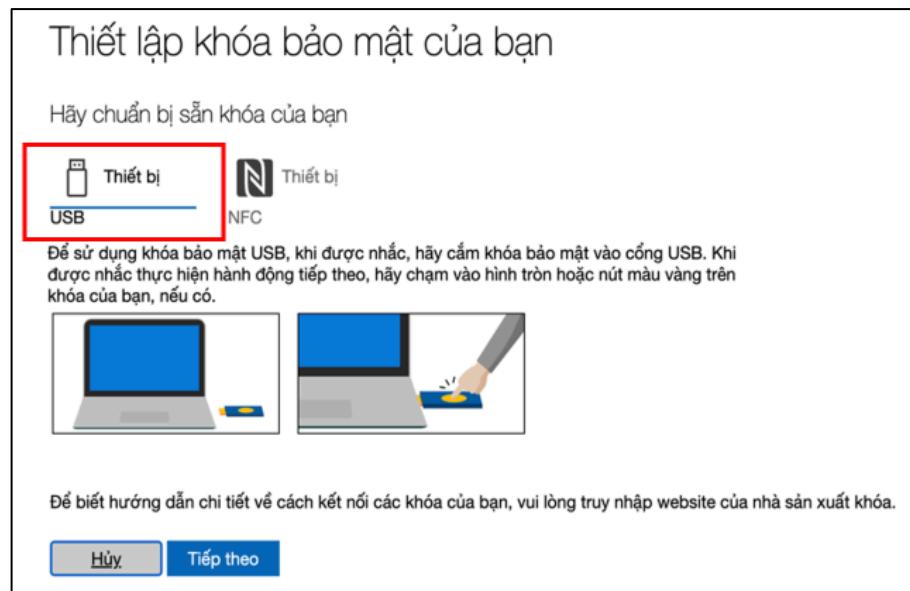


- Quét dấu vân tay khi nhận được thông báo.

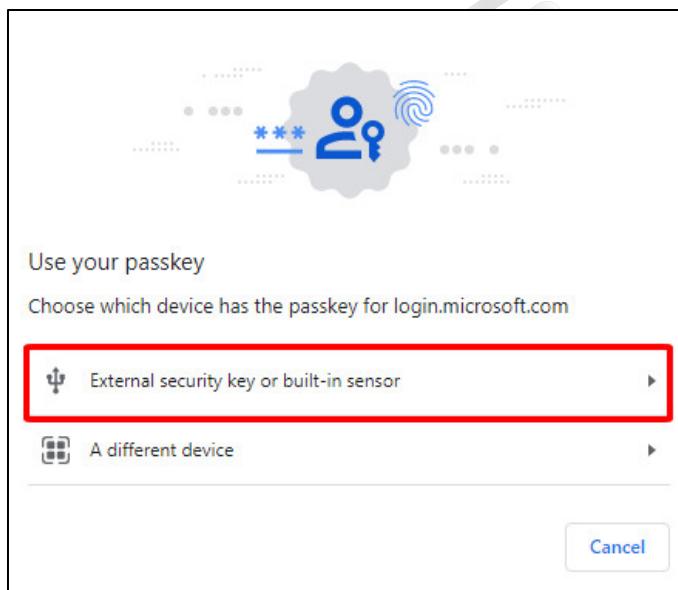


III.2.1.2. Sử dụng qua kết nối USB

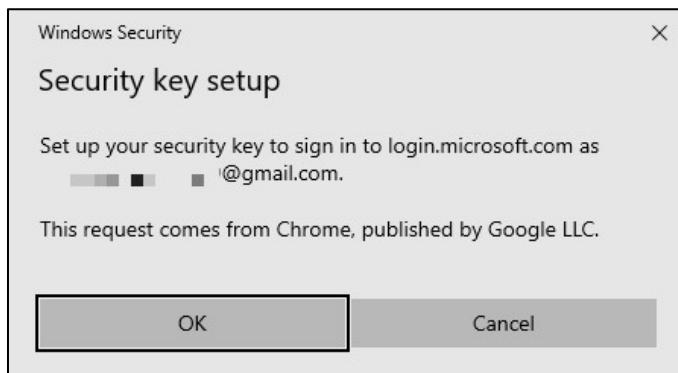
- Chọn **Thiết bị USB**, nhấn Tiếp theo.



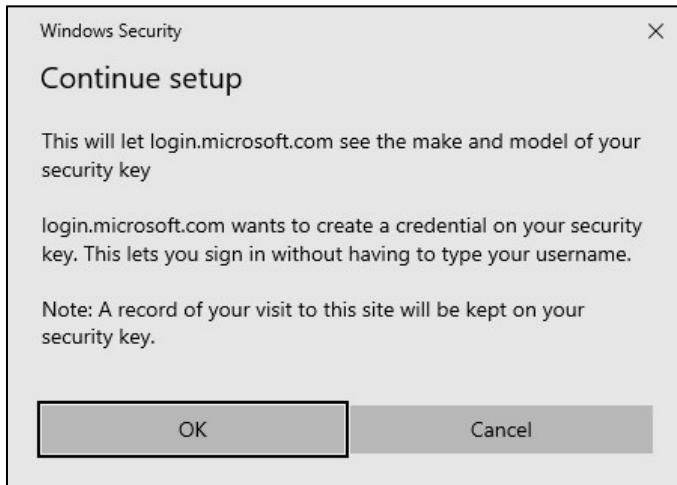
- Chọn **External security key or built-in sensor** để thiết lập khoá bảo mật.



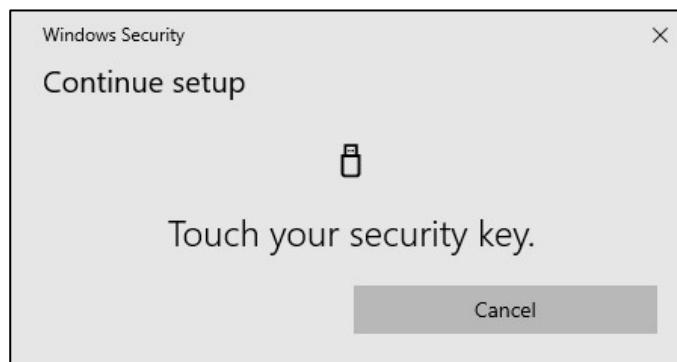
- Nhấn **OK** để tiếp tục thiết lập khoá bảo mật.



- Nhấn **OK** để tiếp tục.



- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

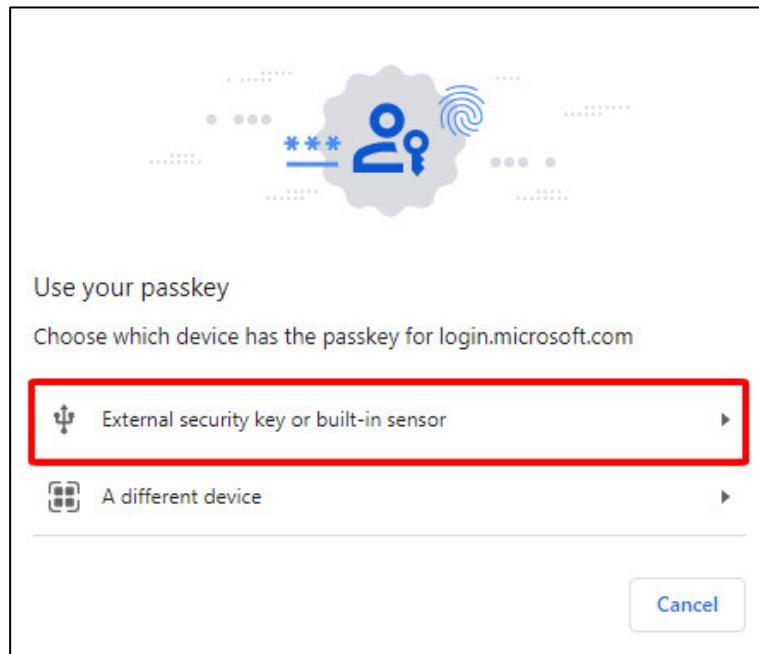


III.2.1.3. Sử dụng qua kết nối NFC

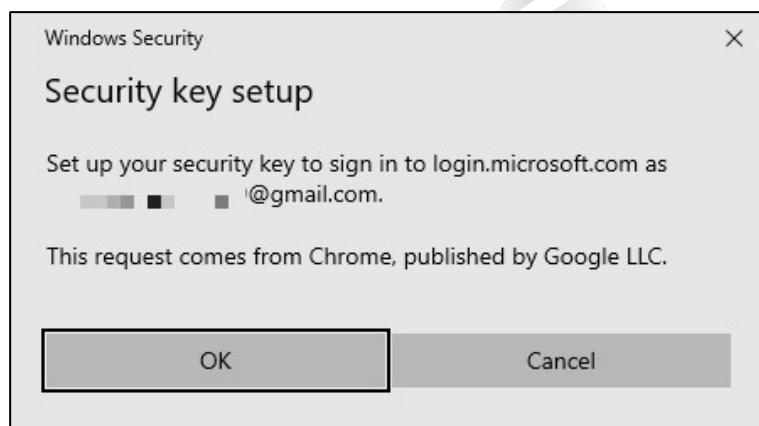
- Chọn **Thiết bị NFC**. nhấn **Tiếp theo**.



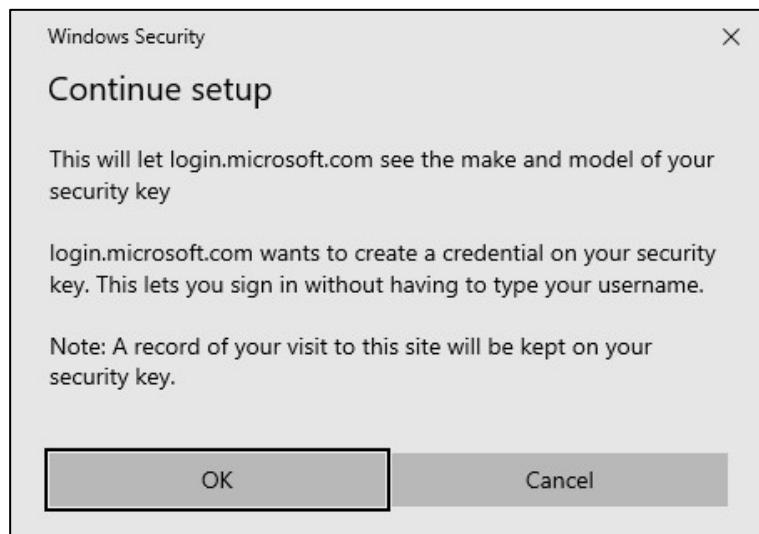
- Chọn **External security key or built-in sensor** để thiết lập khoá bảo mật.



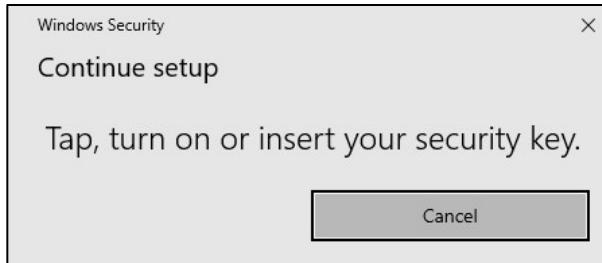
- Nhấn **OK** để tiếp tục thiết lập khoá bảo mật.



- Nhấn **OK** để tiếp tục.



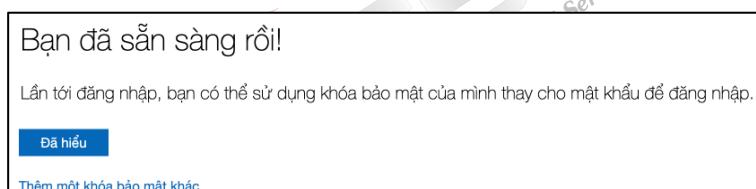
- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Đặt tên cho khoá bảo mật để phân biệt giữa các khoá rồi nhấn **Tiếp theo**.



- Nhấn **Đã hiểu** để hoàn tất đăng ký Security key.

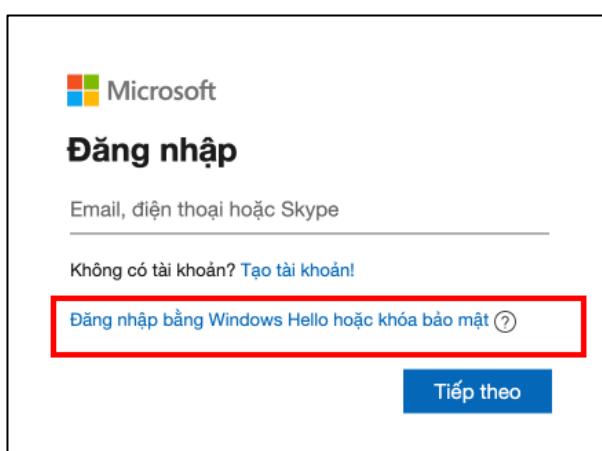


III.2.2. Xác thực không mật khẩu tài khoản Microsoft

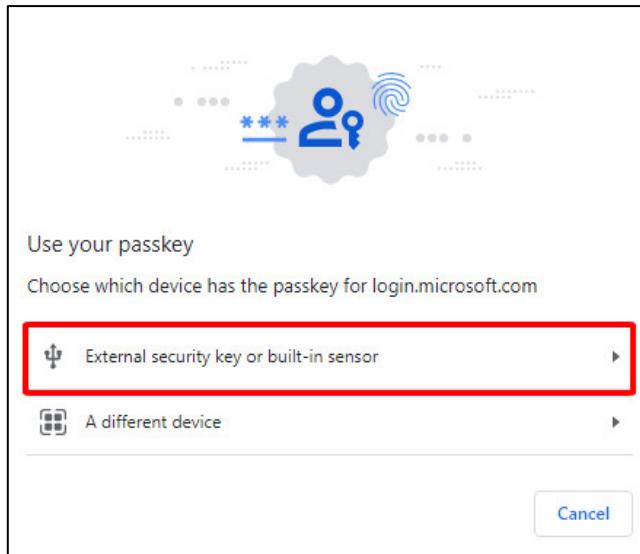
- Truy cập <https://www.microsoft.com/vi-vn/>, chọn **Đăng nhập**.



- Chọn **Đăng nhập bằng Windows Hello hoặc khóa bảo mật**.



- Chọn **External security key or built-in sensor** để đăng nhập bằng khoá bảo mật.



III.2.2.1. Sử dụng qua kết nối Bluetooth

- Kết nối khoá bảo mật với máy tính thông qua kết nối Bluetooth.



- Quét dấu vân tay khi nhận được thông báo.



III.2.2.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

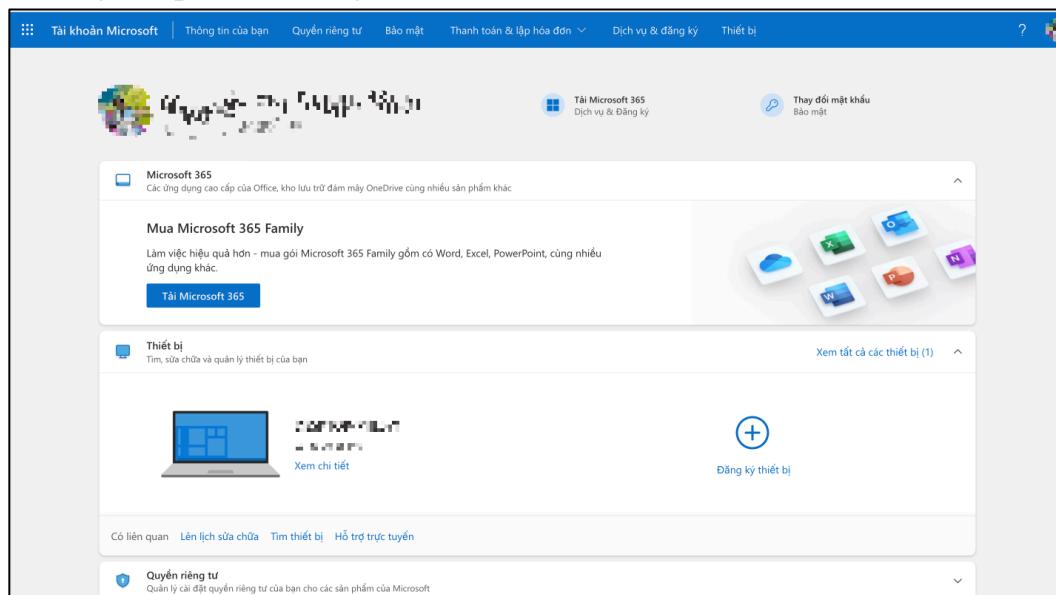


III.2.2.3. Sử dụng qua kết nối NFC

- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Đăng nhập thành công.

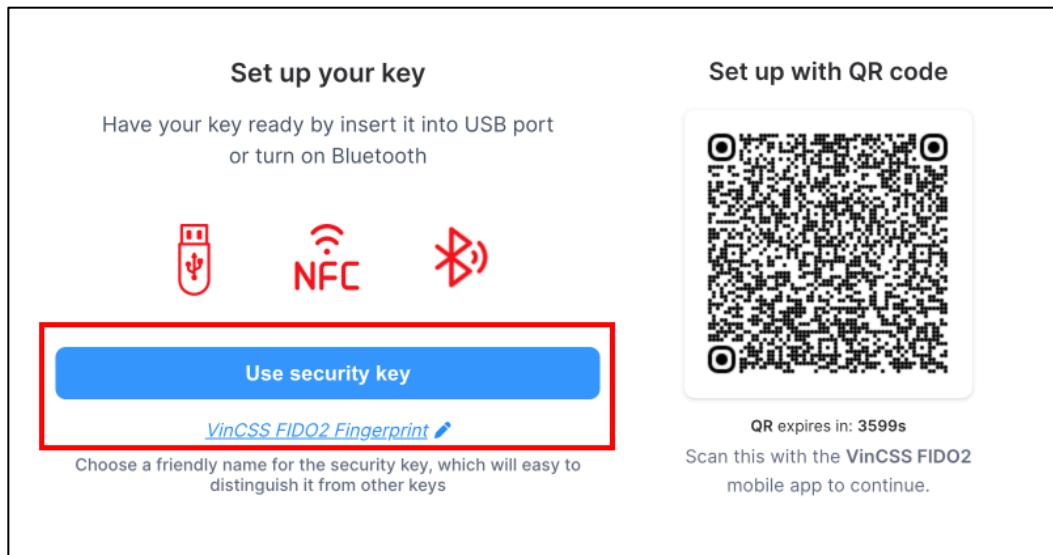


III.3. VinCSS OVPN Client

III.3.1. Windows

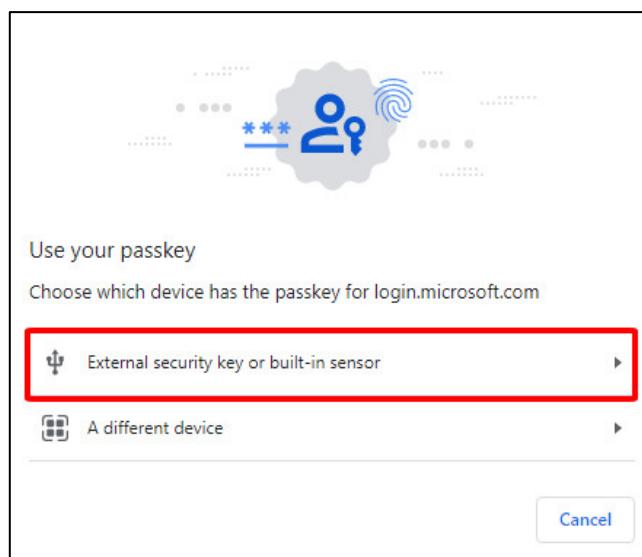
III.3.1.1. Đăng ký khóa bảo mật VinCSS FIDO2® Fingerprint

- Liên hệ người quản trị để lấy đường link đăng ký khoá được gửi cho người dùng qua email hoặc IM (*có hiệu lực trong 1 giờ*). Thay đổi tên khoá bảo mật và chọn **Use security key**.

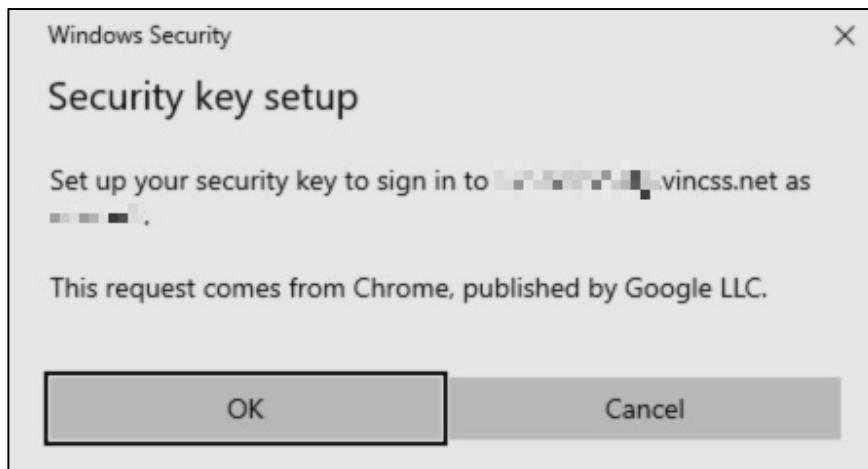


Lưu ý: Mặc định người quản trị sẽ gửi link đăng ký khoá bảo mật sử dụng được với tất cả các hình thức đăng nhập sau khi đăng ký khoá bảo mật thành công (Hình thức xác thực không mật khẩu (Tham khảo mục III.3.1.2.1.) và hình thức xác thực không tên người dùng (Tham khảo mục III.3.1.2.2.)).

- Chọn **External security key or built-in sensor** để đăng ký khoá bảo mật VinCSS FIDO2® Fingerprint.



- Chọn **OK** để tiếp tục quá trình đăng ký khóa bảo mật.

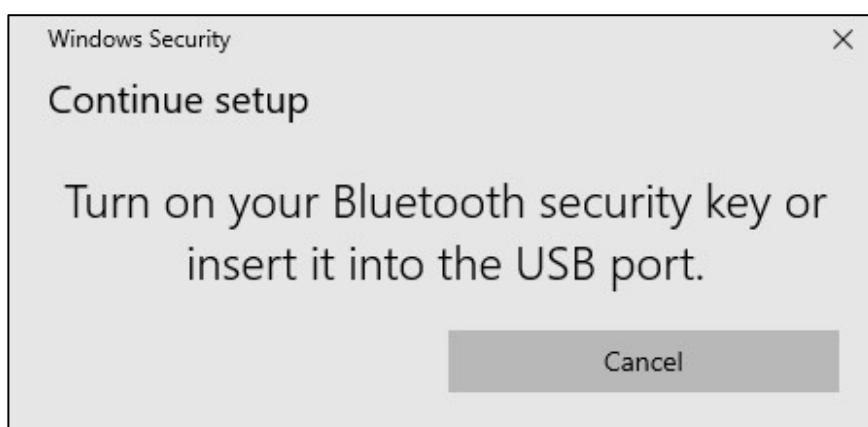


- Nhấn **OK** để tiếp tục.

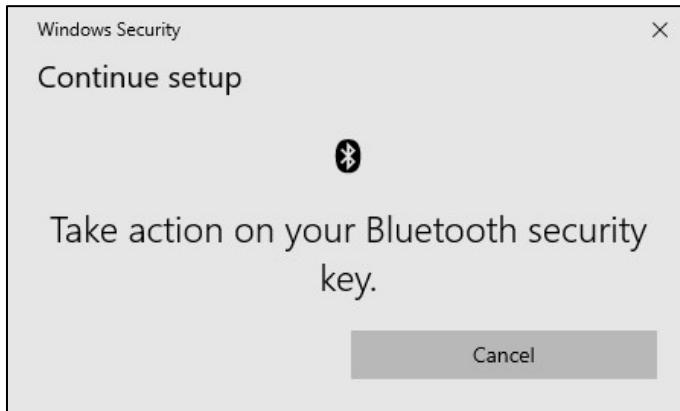


III.3.1.1.1. Sử dụng qua kết nối Bluetooth

- Kết nối khoá bảo mật với máy tính thông qua kết nối Bluetooth.

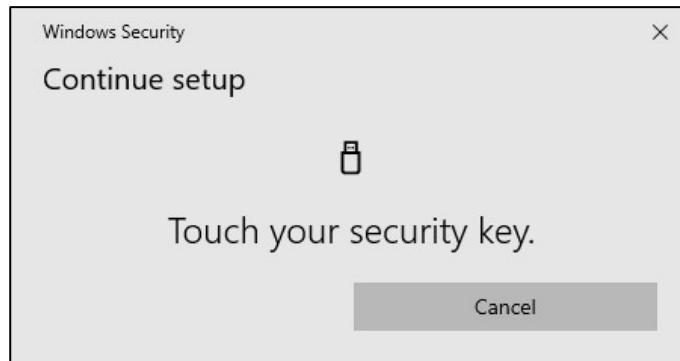


- Quét dấu vân tay khi nhận được thông báo.



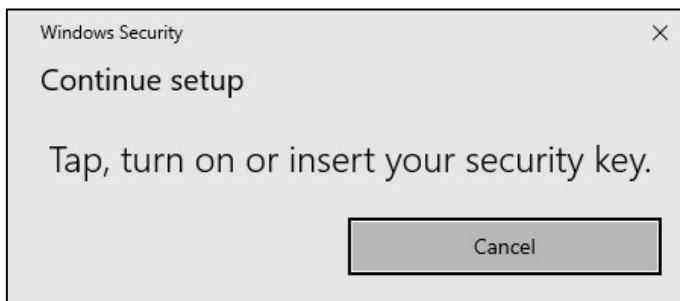
III.3.1.1.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

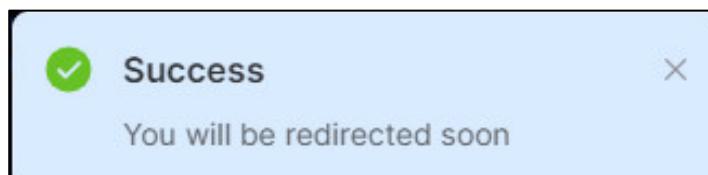


III.3.1.1.3. Sử dụng qua kết nối NFC

- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.

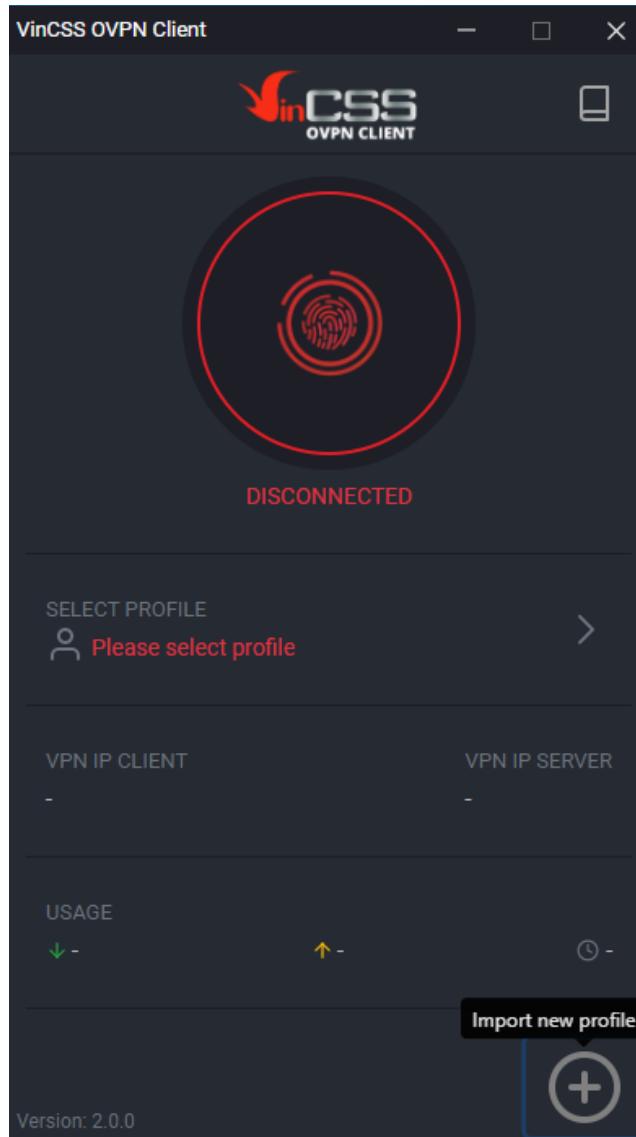


- Trên màn hình máy tính hiện thông báo người dùng đã đăng ký khoá bảo mật thành công.

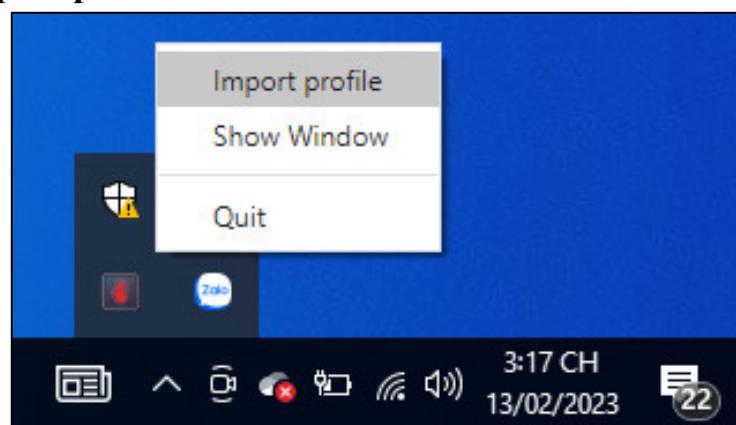


III.3.1.2. Xác thực bằng khoá bảo mật VinCSS FIDO2® Fingerprint

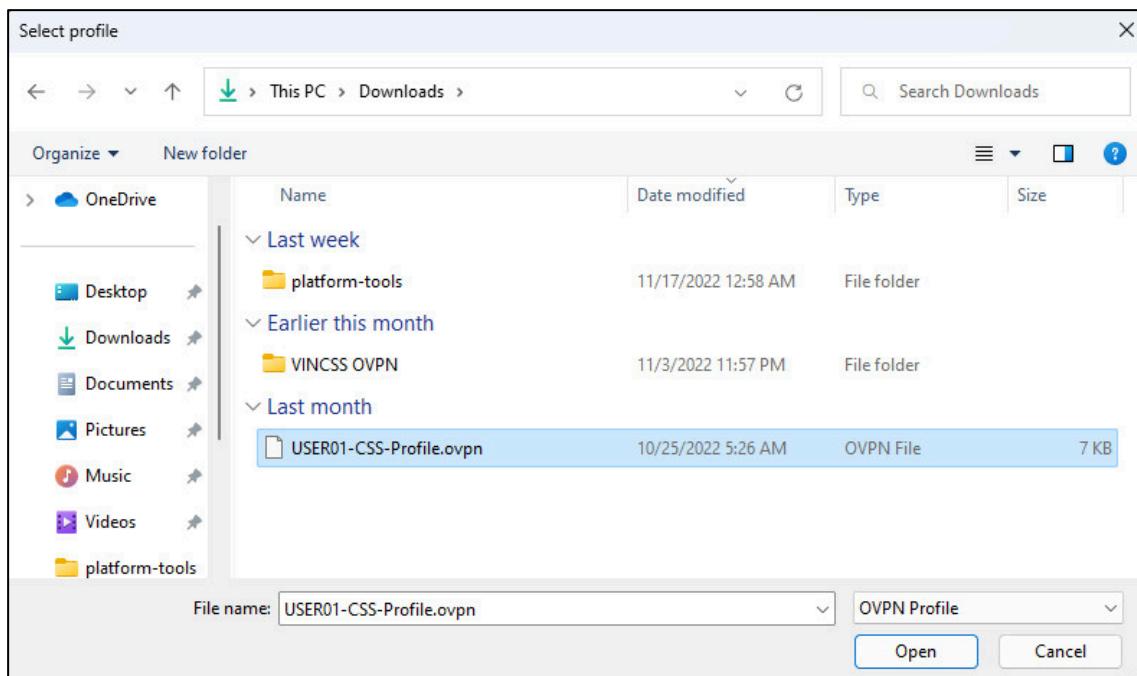
- Mở ứng dụng VinCSS OVPN Client, trên giao diện chọn **Import new profile**.



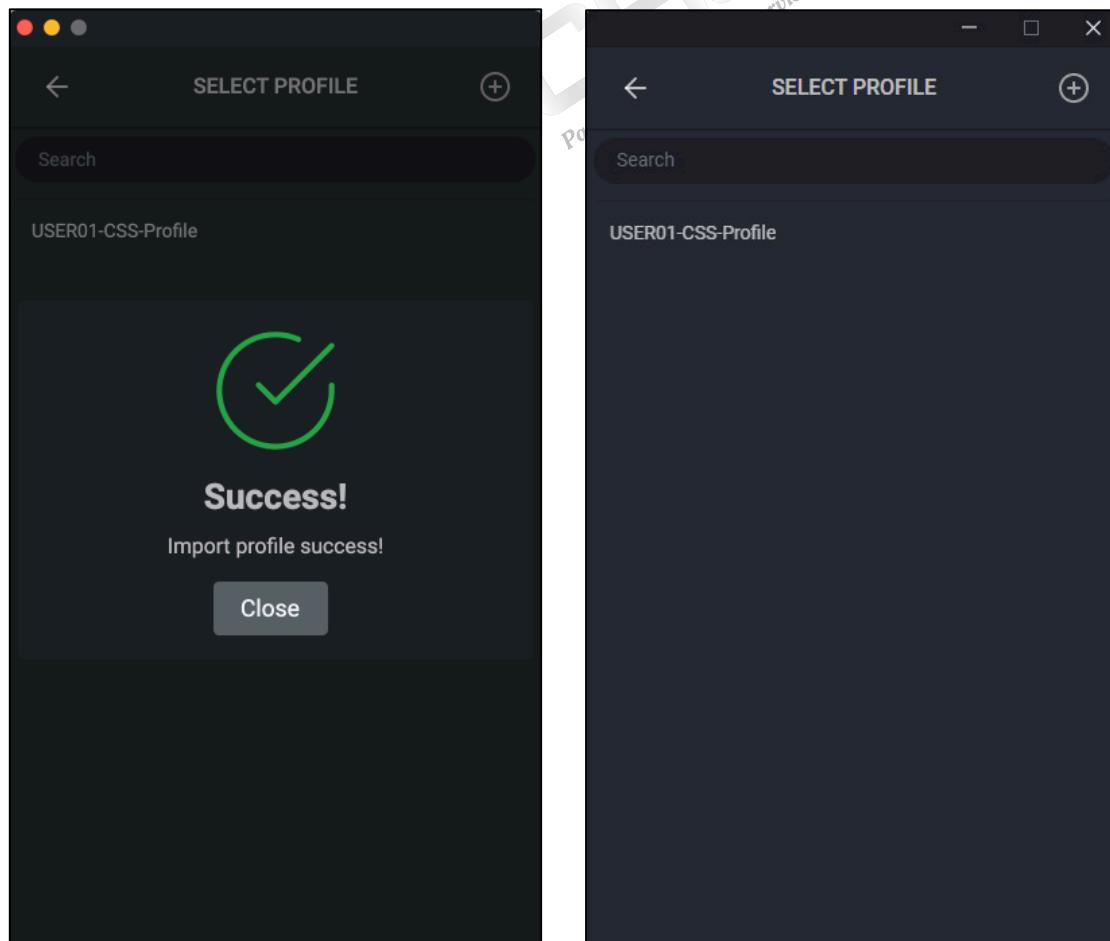
- Hoặc nhấn chuột phải vào biểu tượng VinCSS OVPN Client trên taskbar, chọn **Import profile**.



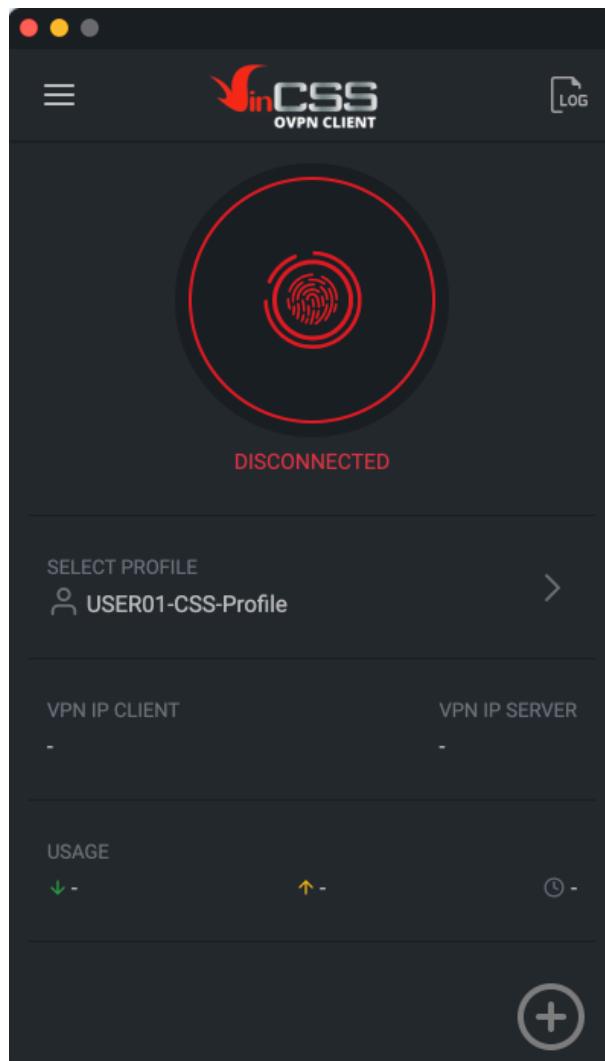
- Chọn profile được gửi bởi quản trị viên (*file .ovpn*) và chọn **Open**.



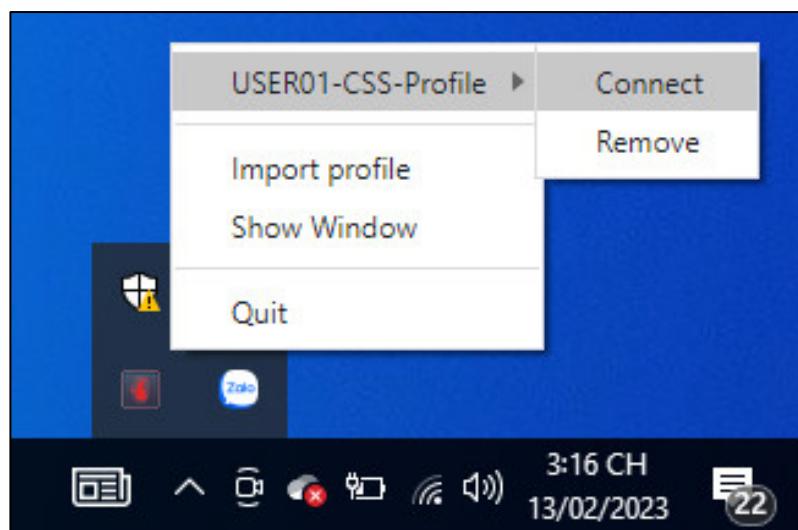
- Profile được thêm thành công. Nhấn **Close** để đóng cửa sổ thông báo. Màn hình hiển danh sách profile đã thêm.



- Nhấn vào biểu tượng vân tay màu đỏ trên giao diện ứng dụng để tiến hành kết nối VPN.

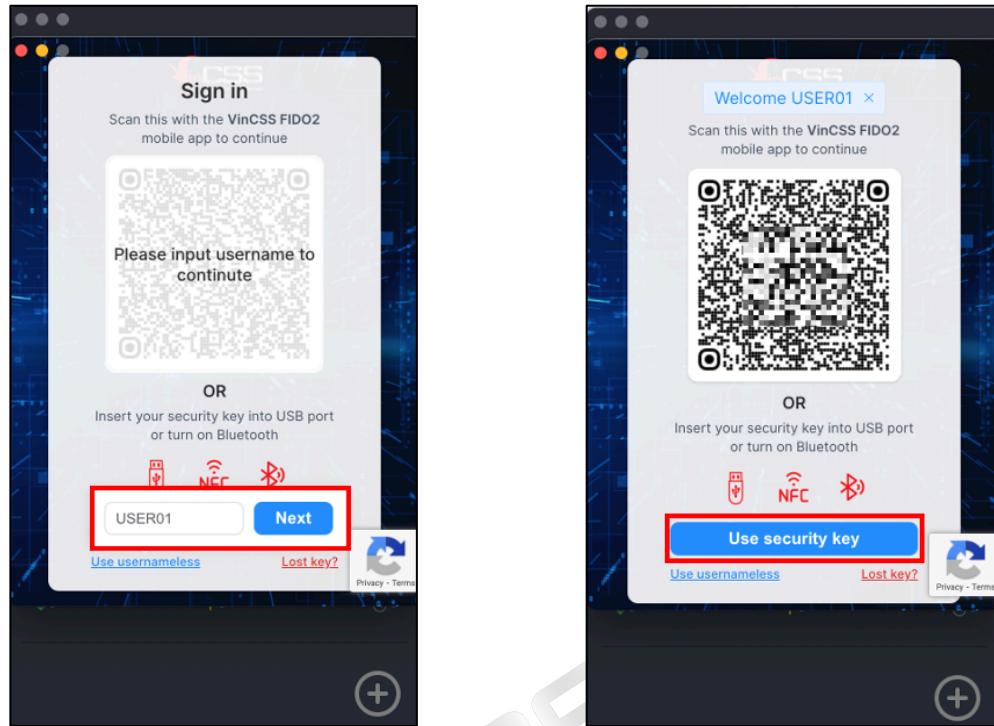


- Hoặc nhấn chuột phải vào biểu tượng VinCSS OVPN Client ở taskbar, chọn VPN profile cần kết nối, sau đó chọn **Connect**.



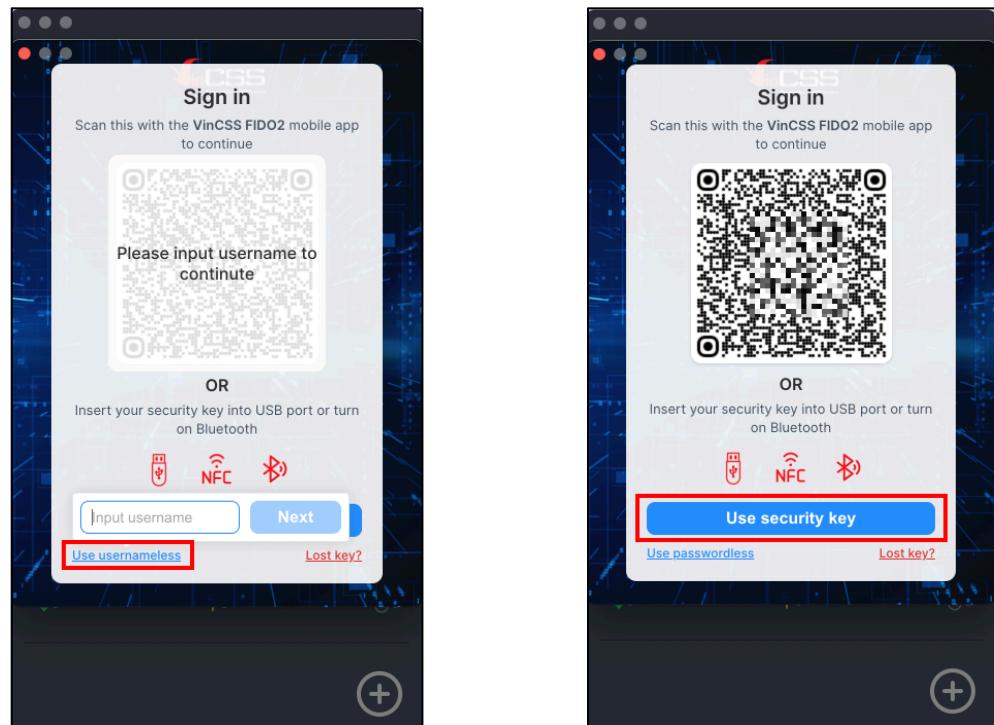
III.3.1.2.1. Xác thực không mật khẩu

- Nhập **Username** (*không phân biệt chữ hoa, chữ thường*) rồi chọn **Next**. Sau đó chọn **Use security key** để tiếp tục.



III.3.1.2.2. Xác thực không tên người dùng

- Người dùng có thể chọn phương thức đăng nhập khác bằng cách chọn **Use usernameless** để thay cho bước nhập **username** rồi chọn **Use security key**.

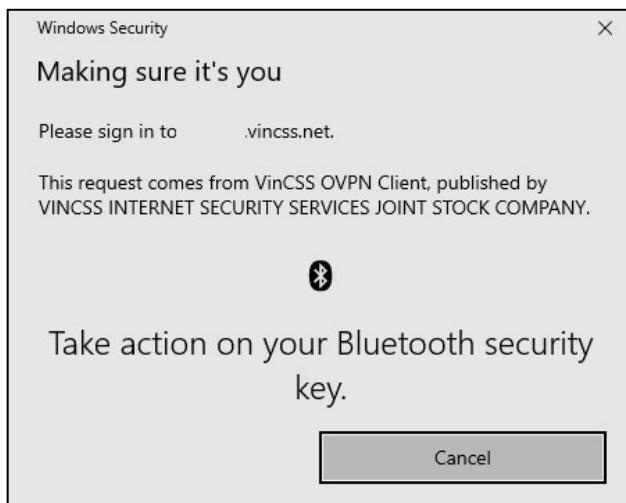


III.3.1.2.2.1. Sử dụng qua kết nối Bluetooth

- Kết nối khoá bảo mật VinCSS FIDO2® Fingerprint với máy tính thông qua kết nối Bluetooth.



- Quét dấu vân tay khi nhận được thông báo.



III.3.1.2.2.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB. Chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

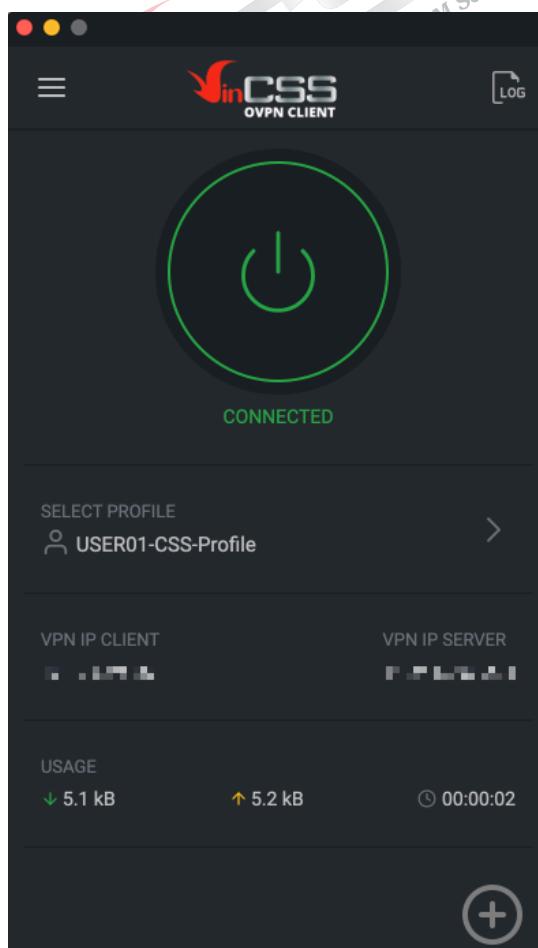


III.3.1.2.2.3. Sử dụng qua kết nối NFC

- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC. Chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



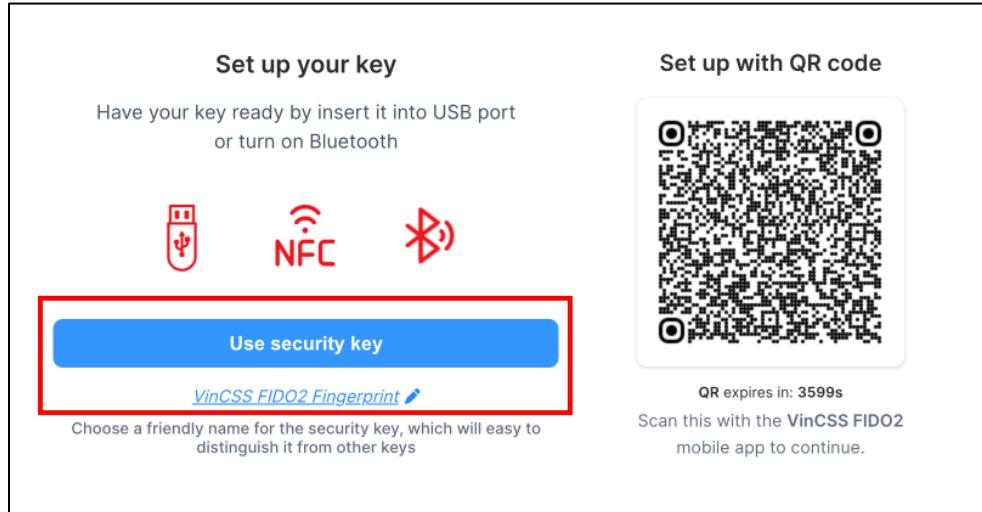
- Quá trình kết nối được tiến hành khi người dùng xác thực thành công. Kết nối VPN thành công, trên giao diện ứng dụng hiển thị trạng thái **CONNECTED**.



III.3.2. macOS

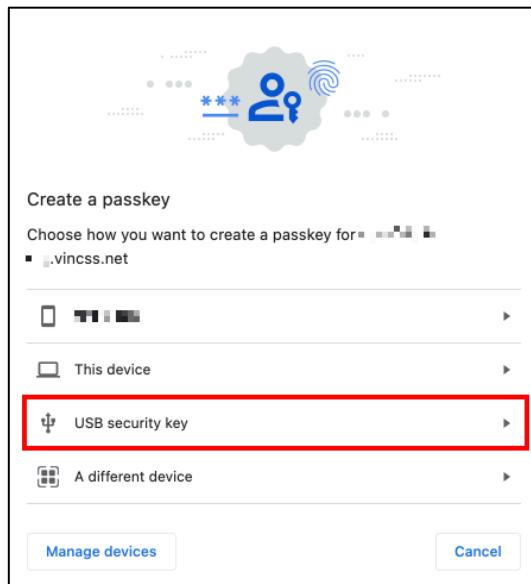
III.3.2.1. Đăng ký khóa bảo mật VinCSS FIDO2® Fingerprint (*Chỉ hỗ trợ kết nối USB*)

- Liên hệ người quản trị để lấy đường link đăng ký khoá được gửi cho người dùng qua email hoặc IM (*có hiệu lực trong 1 giờ*). Thay đổi tên khoá bảo mật và chọn **Use security key**.

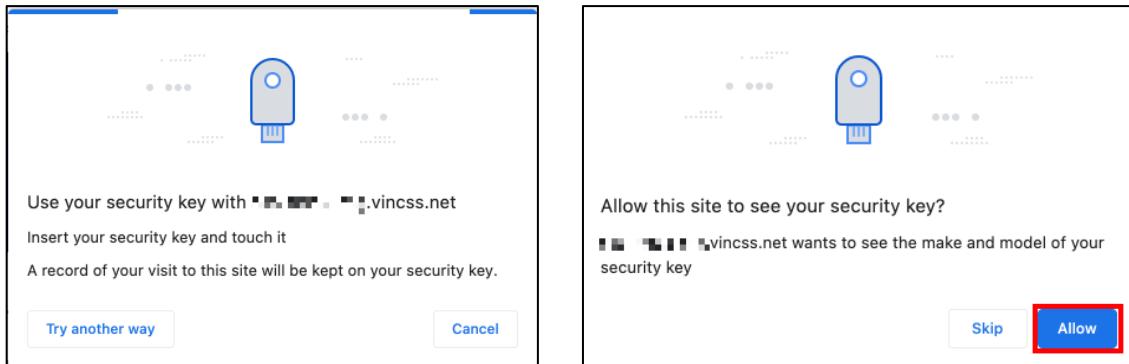


Lưu ý: Mặc định người quản trị sẽ gửi link đăng ký khoá bảo mật sử dụng được với tất cả các hình thức đăng nhập sau khi đăng ký khoá bảo mật thành công (Hình thức xác thực không mật khẩu (Tham khảo mục III.3.2.2.1.) và hình thức xác thực không tên người dùng (Tham khảo mục III.3.2.2.2.)).

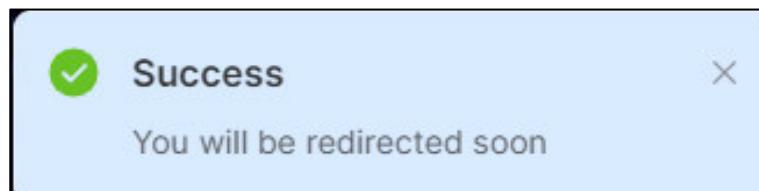
- Chọn **USB security key** để đăng ký bằng khoá bảo mật VinCSS FIDO2® Fingerprint.



- Chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo. Sau đó nhấn **Allow** để tiếp tục.

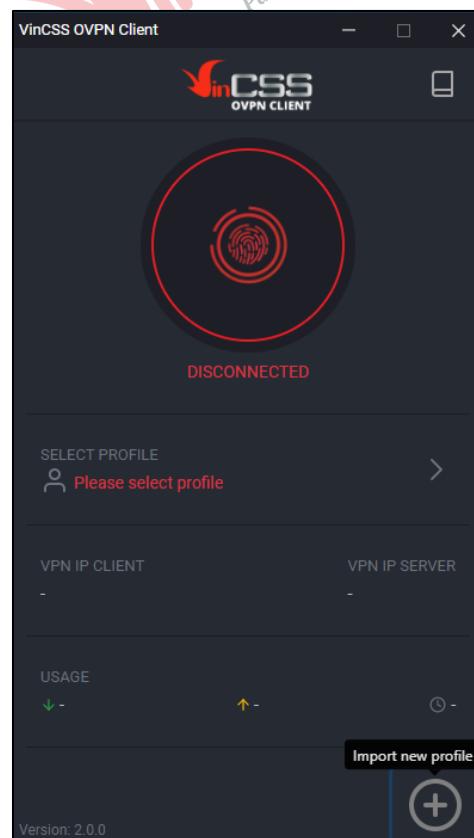


- Trên màn hình máy tính hiện pop-up thông báo người dùng đã đăng ký khoá bảo mật thành công.

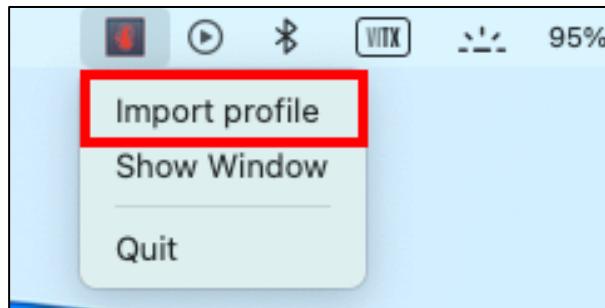


III.3.2.2. Xác thực bằng khoá bảo mật VinCSS FIDO2® Fingerprint

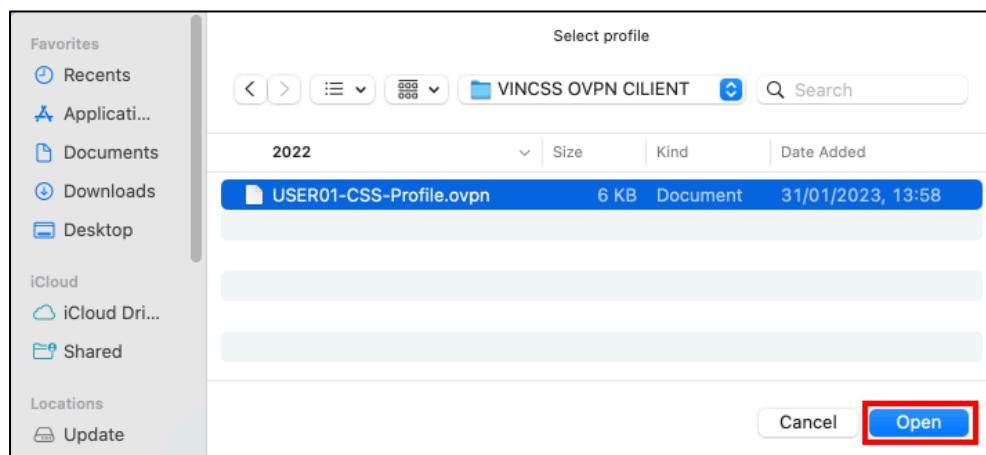
- Mở phần mềm VinCSS OVPN Client đã được cài đặt trong máy. Trên giao diện chính, nhấn vào dấu (+) để thêm mới profile.



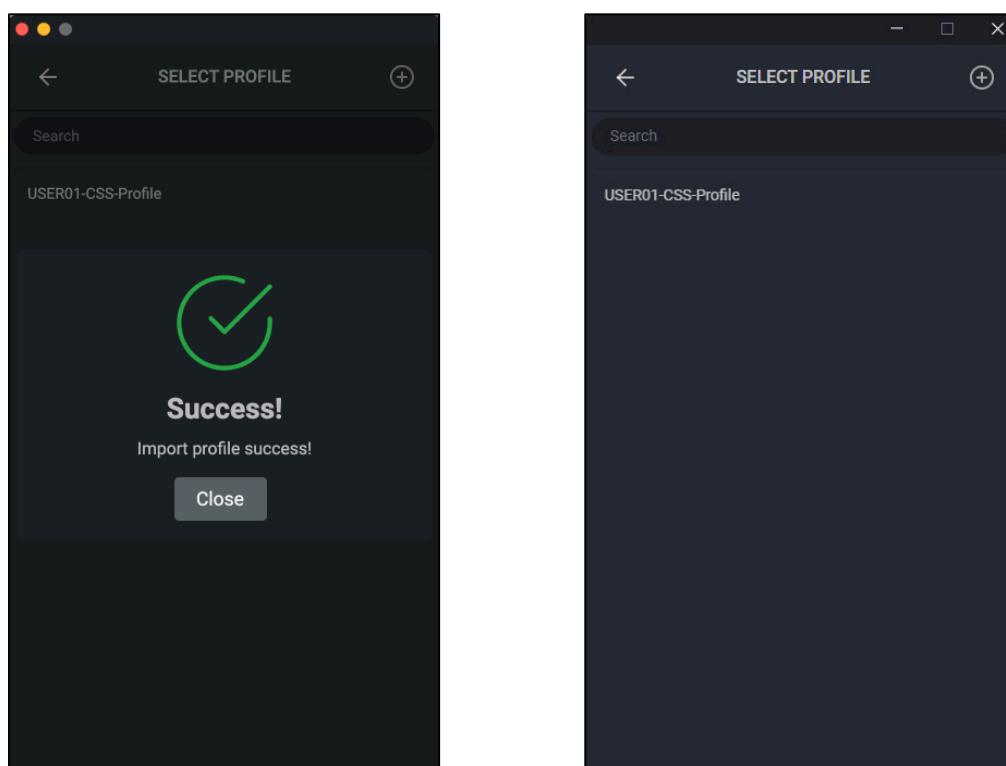
- Hoặc nhấp chuột phải vào biểu tượng VinCSS OVPN Client trên taskbar, chọn **Import profile**.



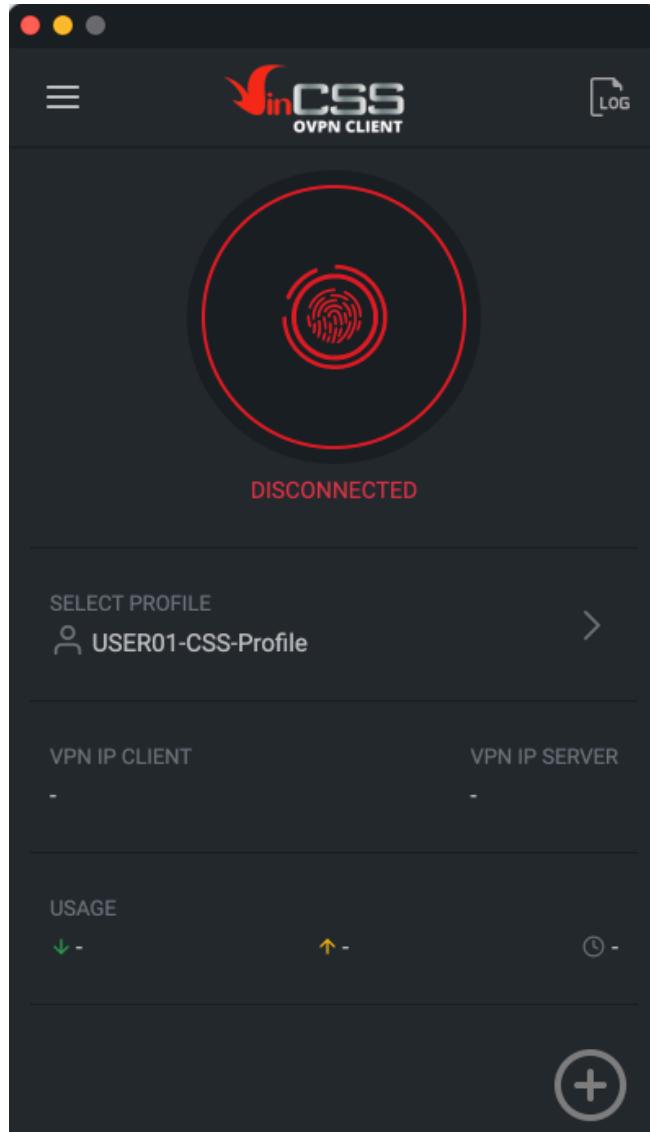
- Chọn profile được gửi bởi người quản trị (*file .ovpn*) và chọn **Open**.



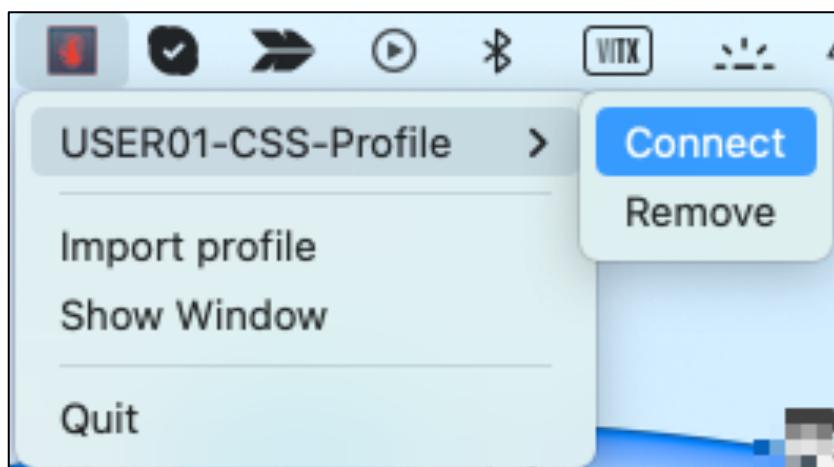
- Profile được thêm thành công, nhấn **Close** để đóng cửa sổ thông báo. Màn hình hiển thị tên profile trong danh sách.



- Nhấn vào biểu tượng vân tay màu đỏ trên giao diện ứng dụng để tiến hành kết nối VPN.

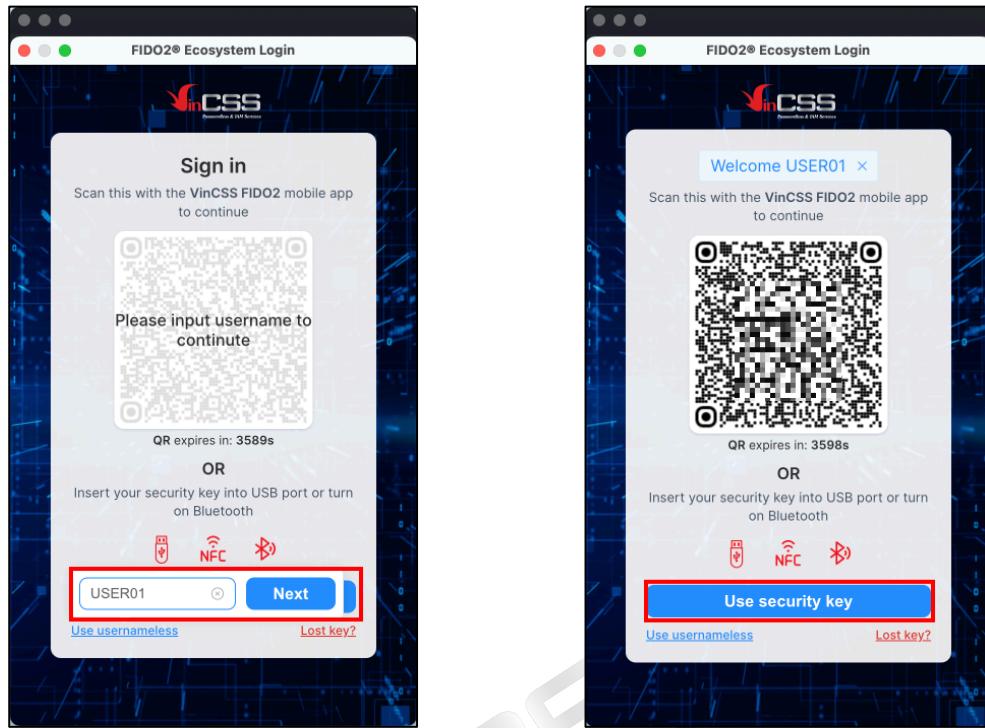


- Hoặc nhấn chuột phải vào biểu tượng VinCSS OVPN Client ở taskbar, chọn VPN profile cần kết nối, sau đó chọn **Connect**.



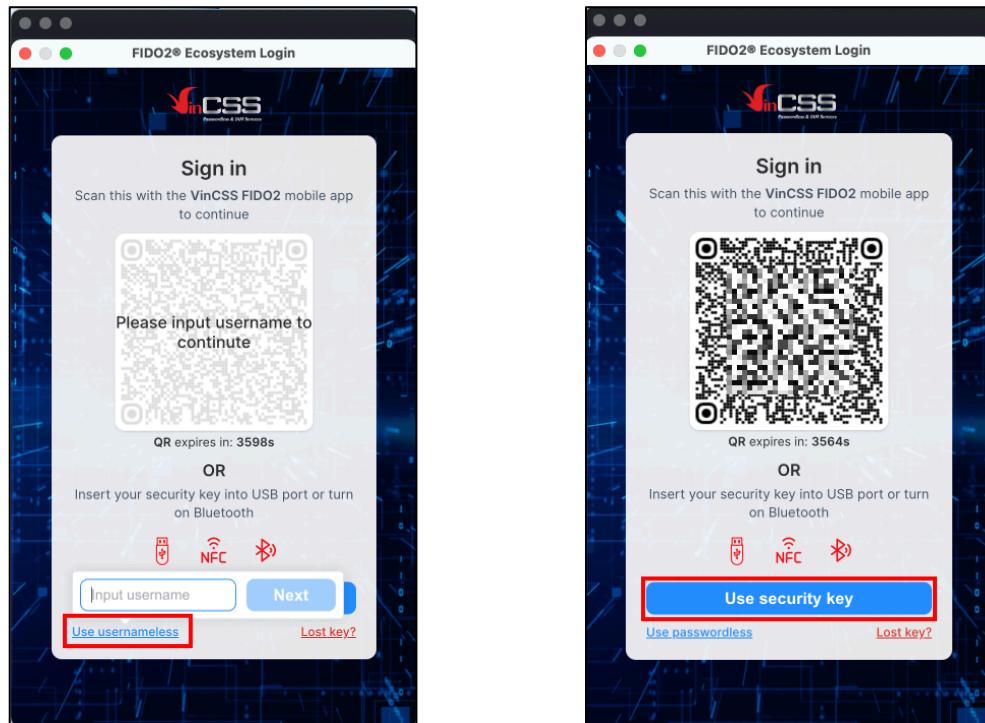
III.3.2.2.1. Xác thực không mật khẩu

- Nhập **Username** (*không phân biệt chữ hoa, chữ thường*) rồi chọn **Next**. Sau đó chọn **Use security key** để tiếp tục.



III.3.2.2.2. Xác thực không tên người dùng

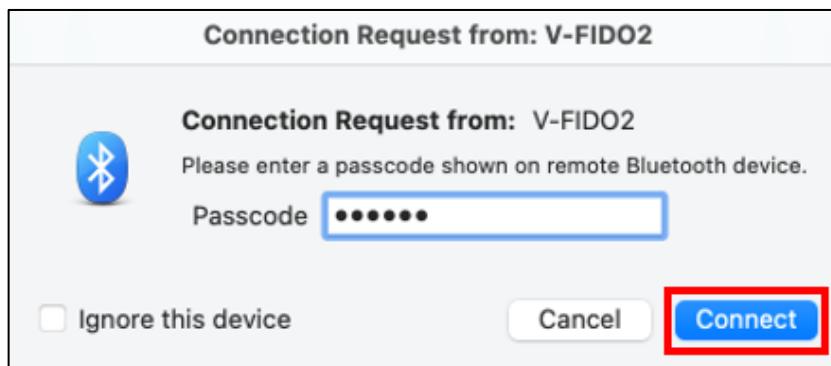
- Hoặc có thể chọn phương thức xác thực khác bằng cách chọn **Use usernameless** để thay cho bước nhập **username** rồi chọn **Use security key**.



III.3.2.2.2.1. Sử dụng qua kết nối Bluetooth

- Chạm và giữ vào phần quét vân tay (*khoảng 5-8 giây*) của khoá bảo mật cho đến khi đèn báo nháy sáng xanh. Khoá bảo mật đang ở trong trạng thái chờ ghép nối. Nhập mã ghép đôi (*Mã ghép đôi được ghi ở mặt sau của khoá bảo mật*) để kết nối rồi chọn **Connect**.

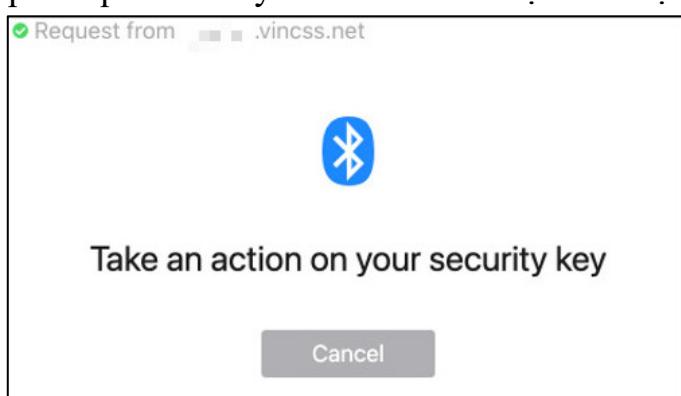
Lưu ý: macOS không hỗ trợ kết nối Bluetooth của khoá bảo mật trước đó. Chỉ có thể hỗ trợ kết nối Bluetooth của khoá bảo mật qua ứng dụng VinCSS OVPN Client tại bước này.



- Người dùng nhấn chọn vào tên của khoá bảo mật để kết nối.

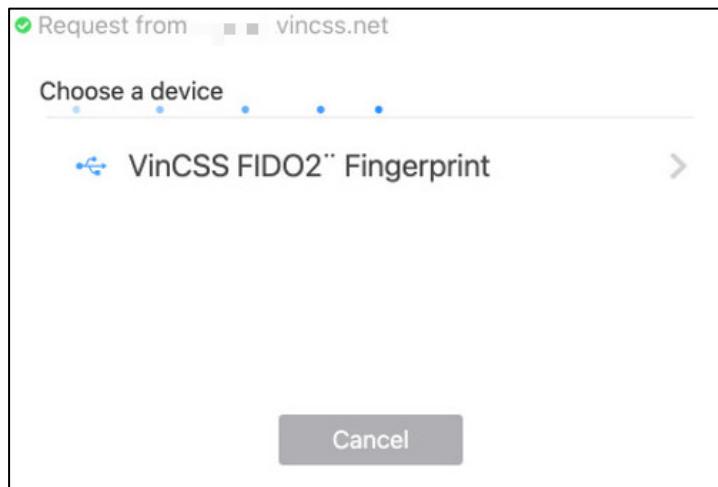


- Chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

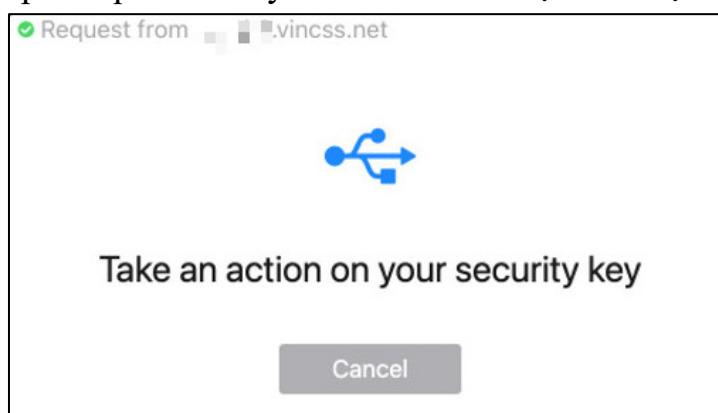


III.3.2.2.2.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB. Chọn thiết bị cần kết nối.



- Chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

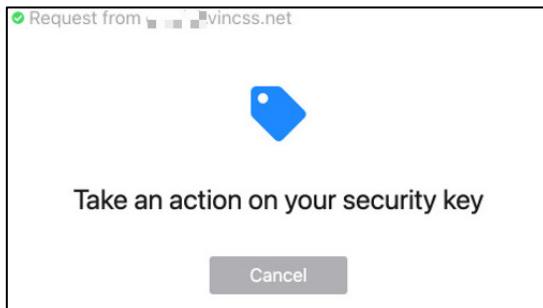


III.3.2.2.2.3. Sử dụng qua kết nối NFC

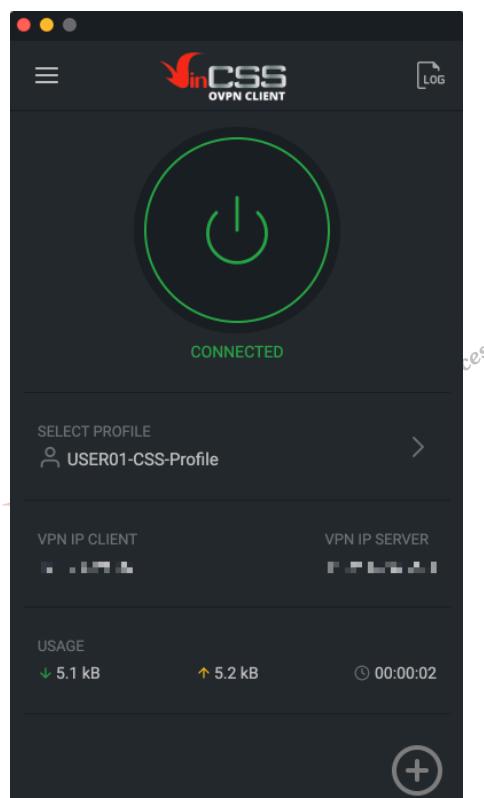
- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chọn thiết bị cần kết nối.



- Chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



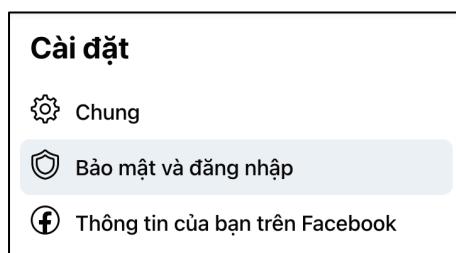
- Kết nối VPN thành công, trên giao diện ứng dụng hiển thị trạng thái **CONNECTED**.



III.4. Xác thực 2 yếu tố tài khoản Facebook

III.4.1. Đăng ký khoá bảo mật

- Đăng nhập vào <https://www.facebook.com/>, sau đó vào phần **Cài đặt > Bảo mật và đăng nhập** bên menu trái.



- Tại mục **Xác thực 2 yếu tố**, chọn **Chỉnh sửa** ở phần **Dùng tính năng xác thực 2 yếu tố**.

The screenshot shows the 'Bảo mật và đăng nhập' (Security and Login) settings in Facebook. Under the 'Đăng nhập' (Login) section, there is a 'Xác thực 2 yếu tố' (Two-factor authentication) subsection. This subsection contains two items: 'Dùng tính năng xác thực 2 yếu tố' (Use two-factor authentication feature) and 'Đăng nhập hợp lệ' (Valid login). Both items have a 'Chỉnh sửa' (Edit) button next to them. The 'Chỉnh sửa' button for the first item is highlighted with a red box.

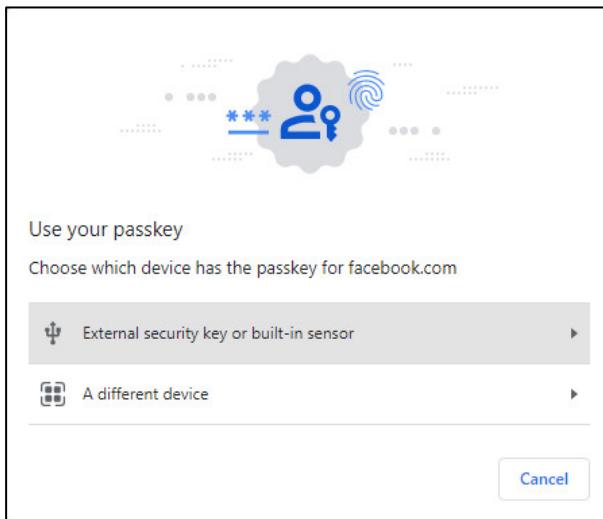
- Từ danh sách **Chọn phương thức bảo mật**, chọn **Sử dụng khóa bảo mật**.

The screenshot shows the 'Chọn phương thức bảo mật' (Select security method) screen. It lists three options: 'Ứng dụng xác thực' (Authenticator app), 'Tin nhắn văn bản (SMS)' (Text message (SMS)), and 'Khóa bảo mật' (Security key). The 'Khóa bảo mật' option is selected and highlighted with a red box around its 'Sử dụng khóa bảo mật' (Use security key) button.

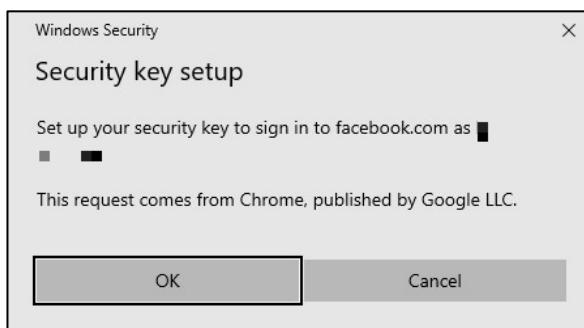
- Ở hộp thoại **Xác thực hai yếu tố**, chọn **Đăng ký khóa bảo mật**.

The screenshot shows the 'Xác thực 2 yếu tố' (Two-factor authentication) setup screen. It displays a 'Cắm khóa bảo mật' (Insert security key) section with an icon of a USB drive. Below it, there is a note: 'Nếu có khóa bảo mật USB, bạn có thể dùng khóa để bảo vệ tài khoản Facebook của mình.' (If you have a USB security key, you can use it to protect your Facebook account.) At the bottom, there are two buttons: 'Quay lại' (Back) and 'Đăng ký khóa bảo mật' (Register security key), which is highlighted with a red box.

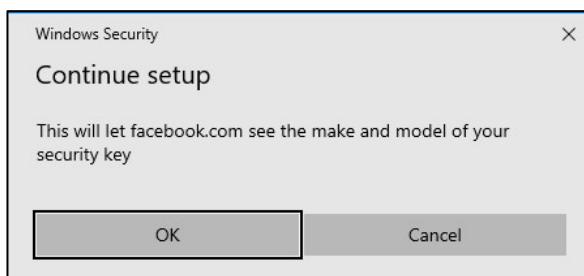
- Chọn **External security key or built-in sensor** để thiết lập khoá bảo mật.



- Để tiếp tục quá trình đăng ký, nhấn **OK**.

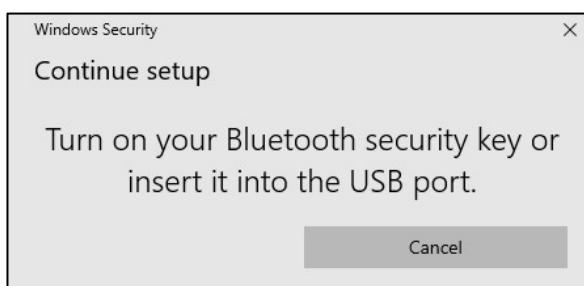


- Nhấn **OK** để tiếp tục.

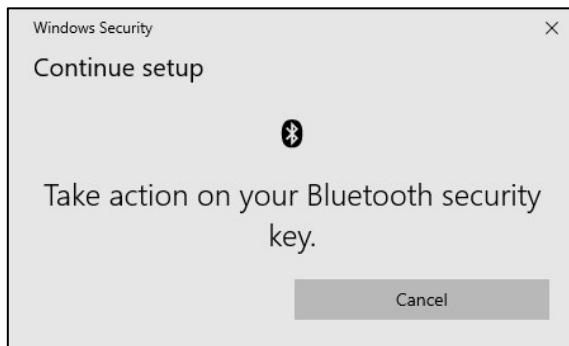


III.4.1.1. Sử dụng qua kết nối Bluetooth

- Kết nối khoá bảo mật VinCSS FIDO2® Fingerprint vào máy tính thông qua Bluetooth.



- Quét vân tay khi nhận được thông báo.



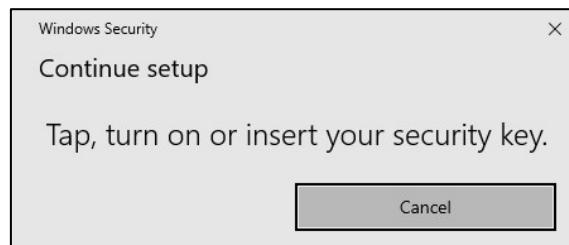
III.4.1.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB. Chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.



III.4.1.3. Sử dụng qua kết nối NFC

- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Đặt tên cho khoá bảo mật để phân biệt giữa các khoá, sau đó nhấn **Lưu** để lưu lại thông tin khoá.



- Thông tin khoá bảo mật đã được đăng ký thành công.

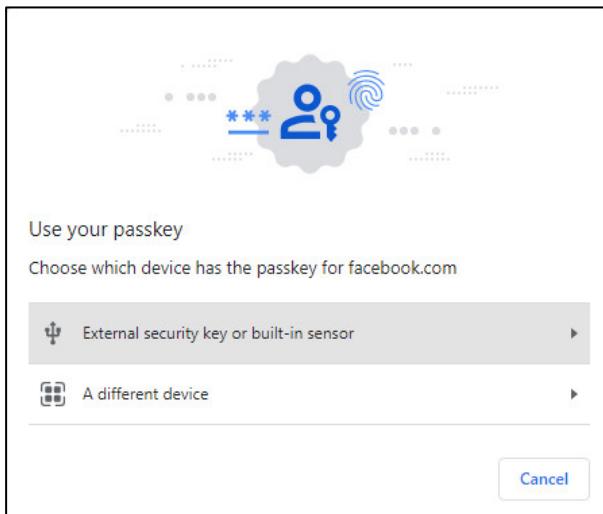


III.4.2. Xác thực 2 yếu tố với dịch vụ Facebook

- Truy cập <https://www.facebook.com/>, đăng nhập với tài khoản và mật khẩu.



- Sau khi nhập mật khẩu, trình duyệt yêu cầu người dùng thực hiện xác thực bằng khoá bảo mật. Chọn **External security key or built-in sensor**.



III.4.2.1. Sử dụng qua kết nối Bluetooth

- Kết nối khoá bảo mật với máy tính thông qua kết nối Bluetooth.



- Quét vân tay khi nhận được thông báo.



III.4.2.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

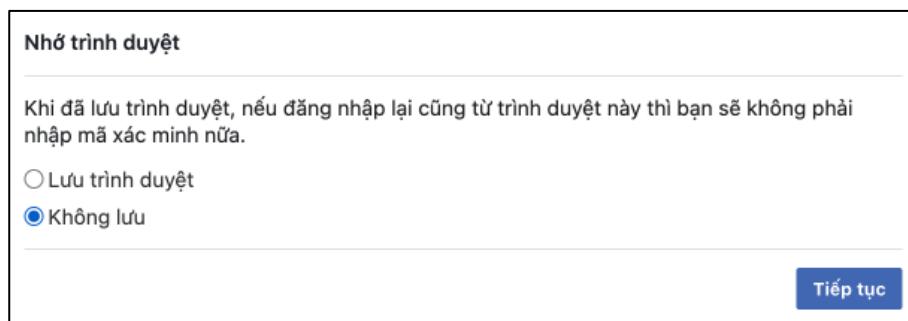


III.4.2.3. Sử dụng qua kết nối NFC

- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



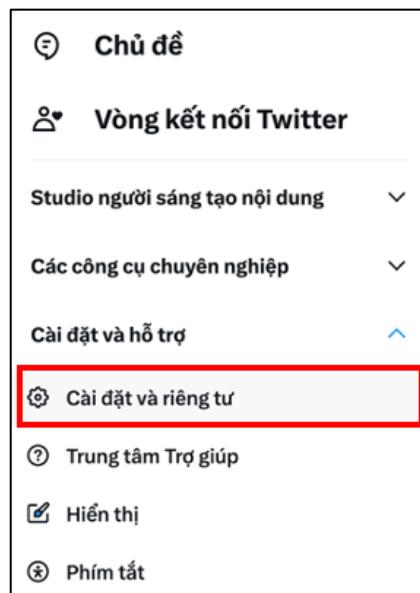
- Xác thực thành công. Chọn **Không lưu** rồi nhấn **Tiếp tục**.



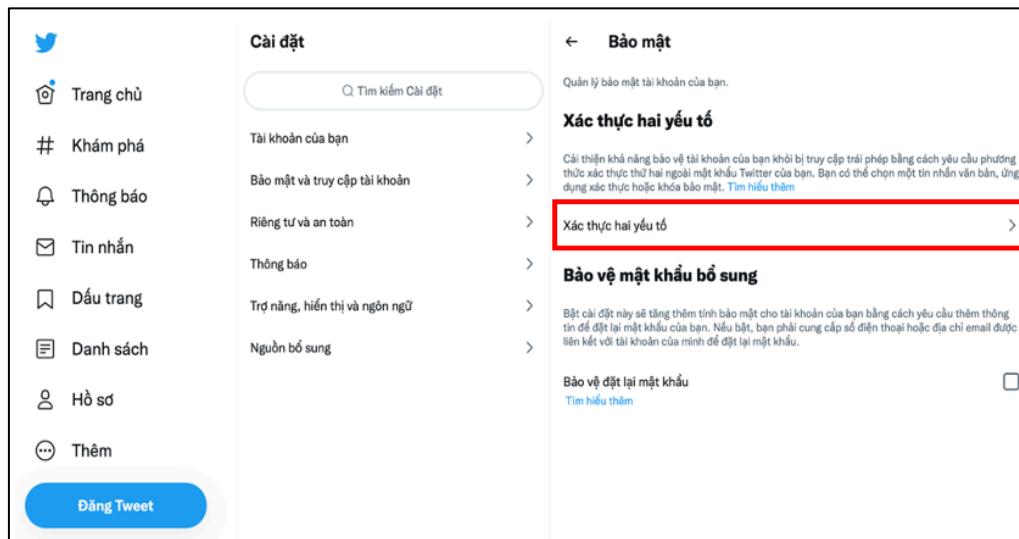
III.5. Xác thực 2 yếu tố với Twitter

III.5.1. Đăng ký khoá bảo mật

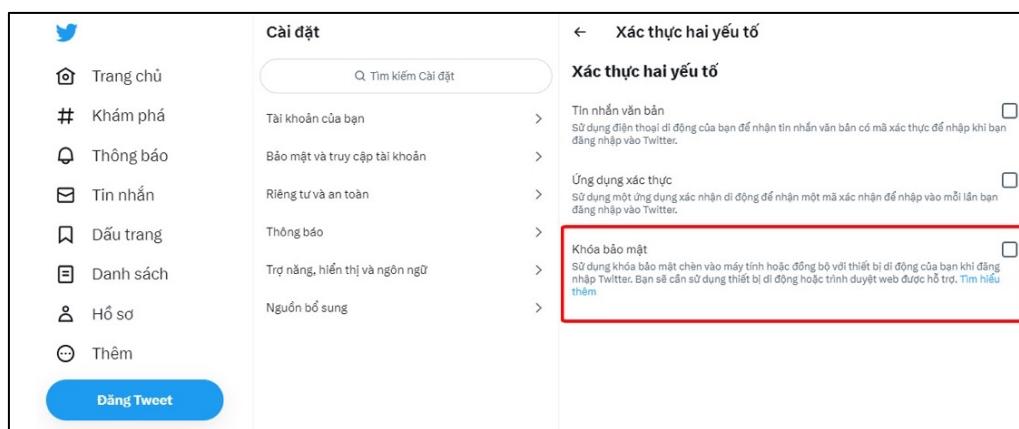
- Đăng nhập vào <https://twitter.com>, sau đó chọn **Thêm > Cài đặt và hỗ trợ > Cài đặt và riêng tư**.



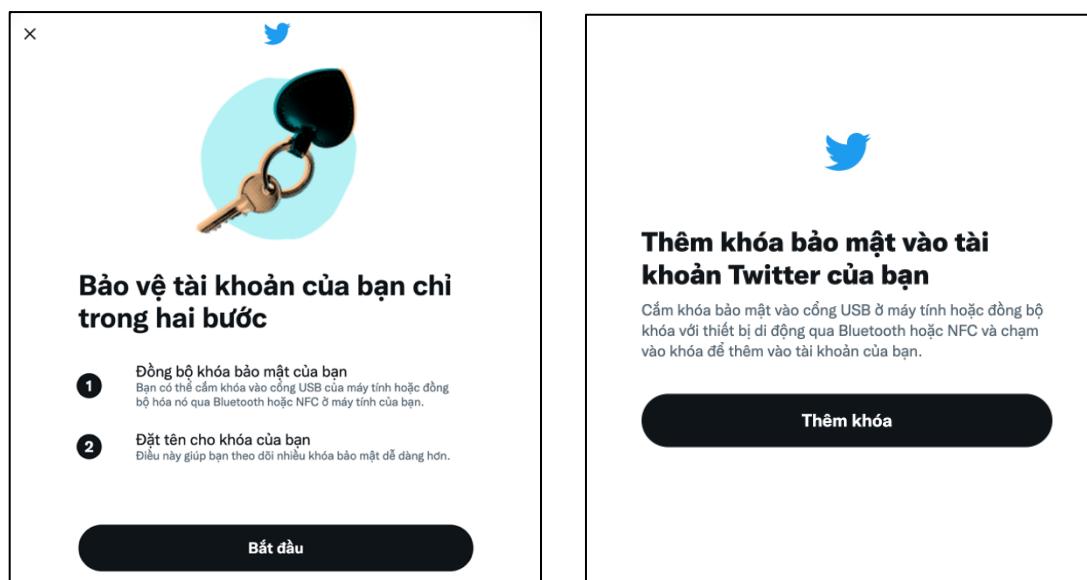
- Chọn **Bảo mật và truy cập tài khoản > Bảo mật > Xác thực hai yếu tố.**



- Tại mục **Xác thực hai yếu tố**, chọn tính năng **Khoá bảo mật**.



- Ở bảng thông báo, chọn **Bắt đầu > Thêm khoá** để bắt đầu quá trình đăng ký khoá bảo mật.

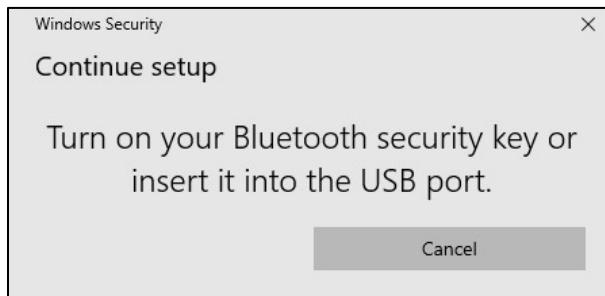


- Nhấn **OK** để tiếp tục.

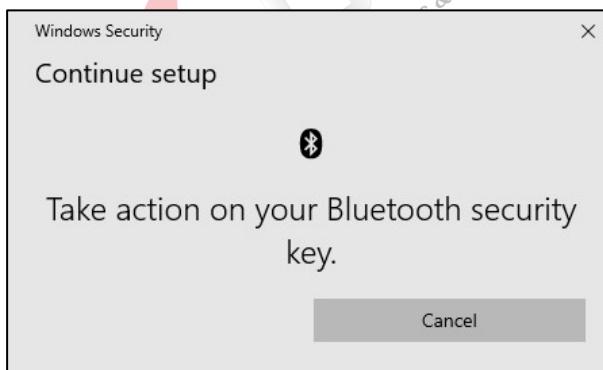


III.5.1.1. Sử dụng qua kết nối Bluetooth

- Kết nối khoá bảo mật với máy tính thông qua Bluetooth.

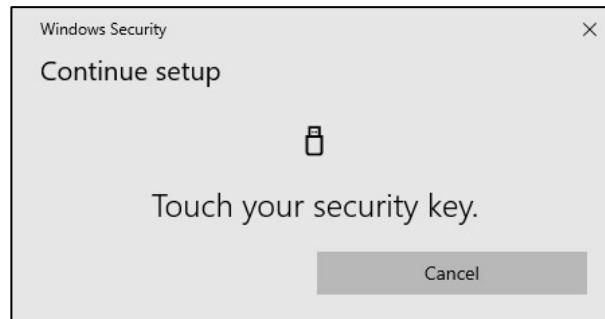


- Quét vân tay khi nhận được thông báo.



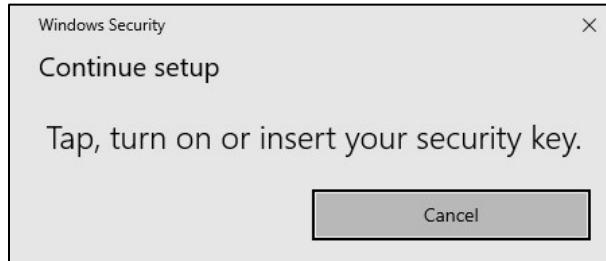
III.5.1.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

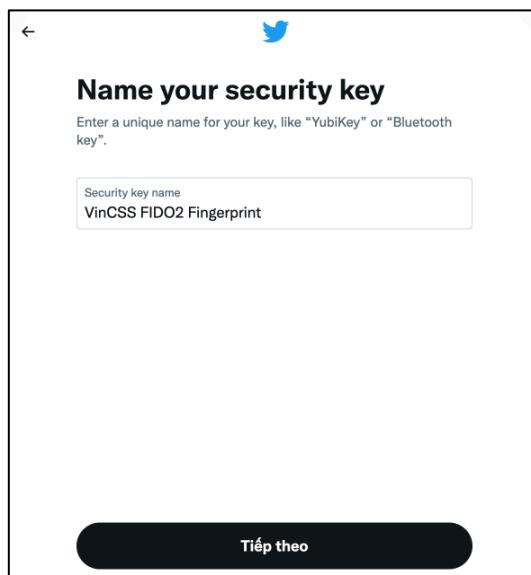


III.5.1.3. Sử dụng qua kết nối NFC

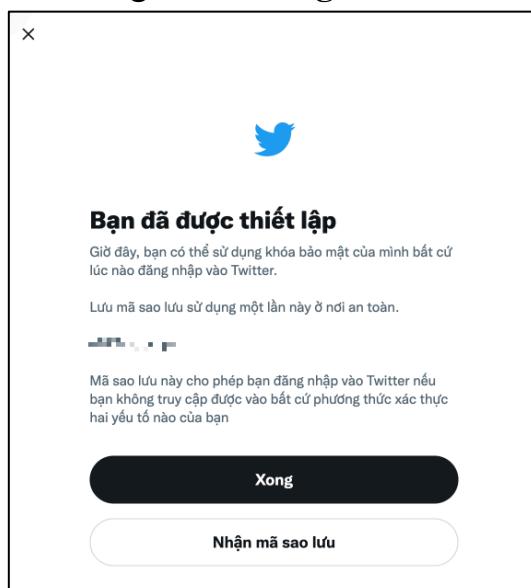
- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Đặt tên cho khoá bảo mật để phân biệt giữa các khoá, sau đó nhấn **Tiếp theo** để lưu lại thông tin khoá.

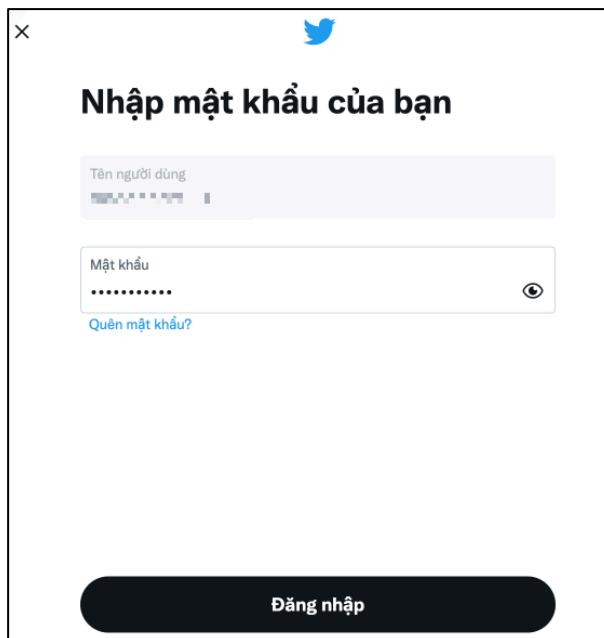


- Đăng ký khoá thành công, nhấn **Xong** để hoàn thành.



III.5.2. Xác thực 2 yếu tố với dịch vụ Twitter

- Truy cập <https://twitter.com> rồi đăng nhập với tài khoản và mật khẩu.

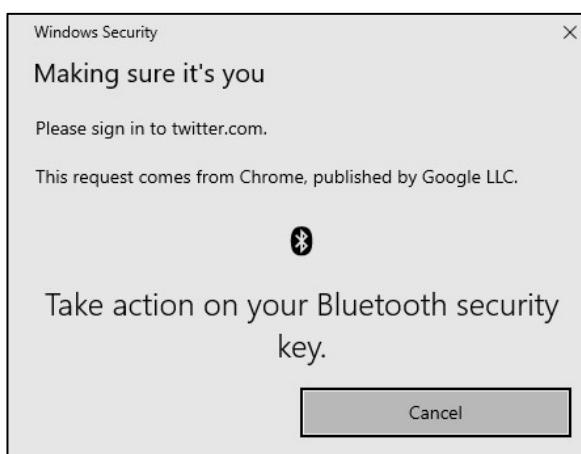


III.5.2.1. Sử dụng qua kết nối Bluetooth

- Người dùng kết nối khoá bảo mật với máy tính thông qua Bluetooth.



- Quét vân tay khi nhận được thông báo.



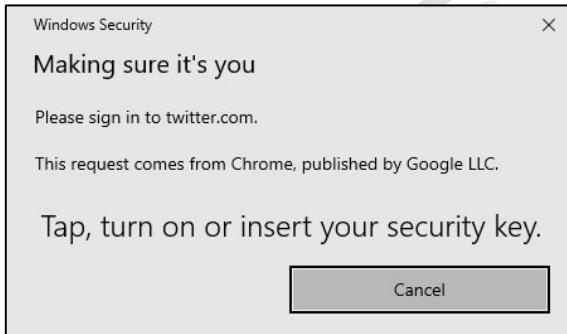
III.5.2.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.



III.5.2.3. Sử dụng qua kết nối NFC

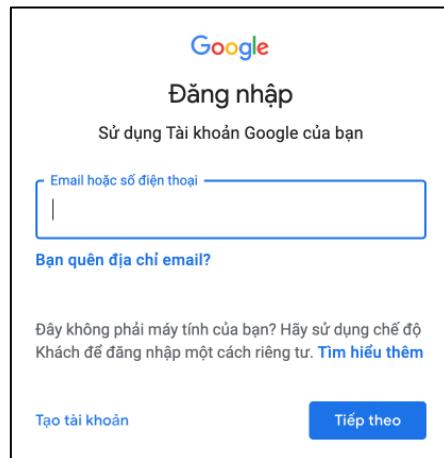
- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



III.6. Xác thực 2 yếu tố với Google

III.6.1. Đăng ký khoá bảo mật

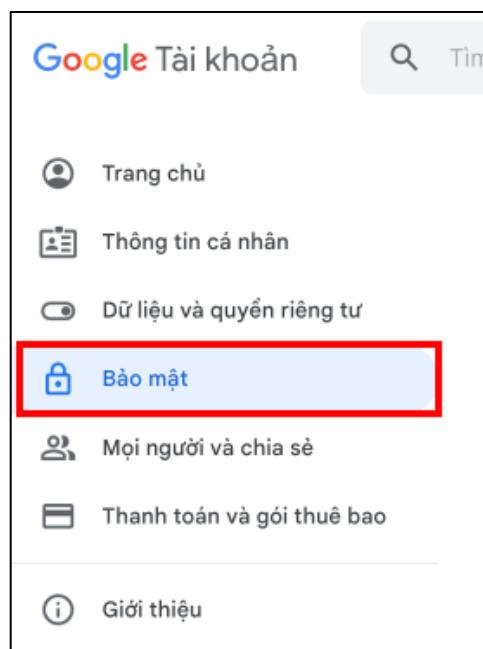
- Truy cập vào <https://accounts.google.com/>, đăng nhập với tài khoản và mật khẩu.



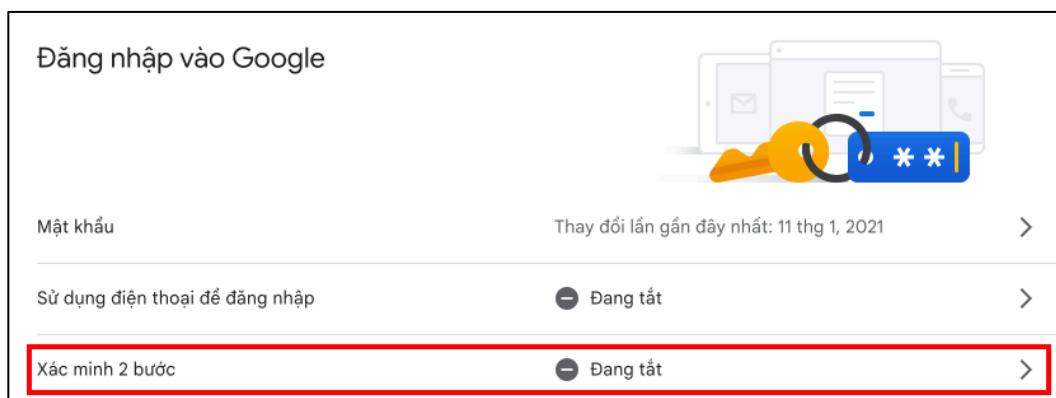
- Bấm vào biểu tượng account góc trên bên phải, chọn **Quản lý Tài khoản Google của bạn**.



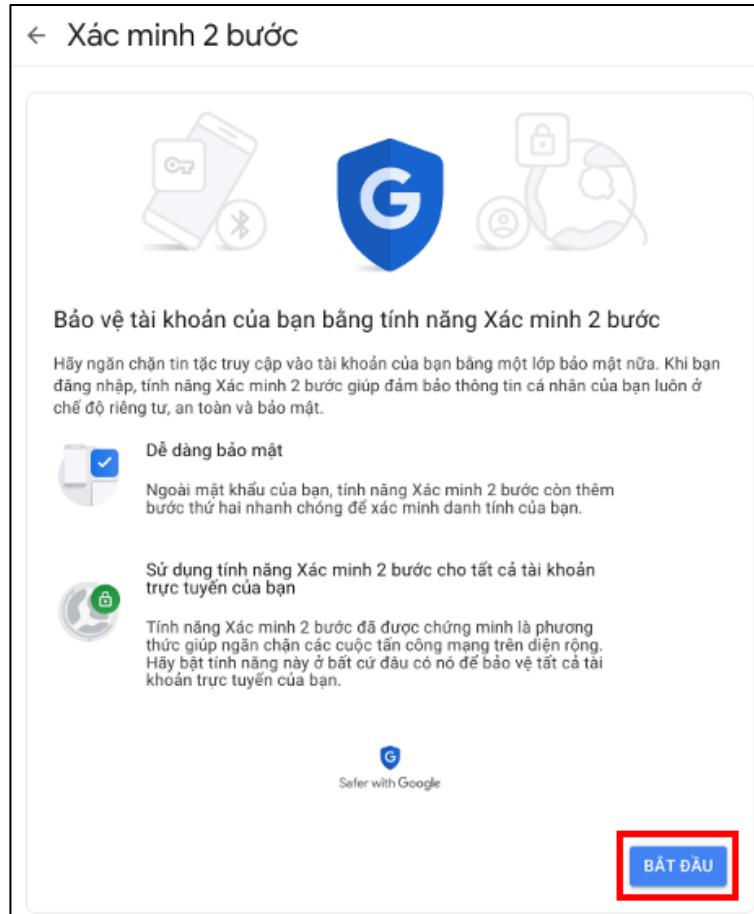
- Chọn mục **Bảo mật** tại menu bên trái.



- Chọn mục **Xác minh 2 bước** để thiết lập xác thực hai yếu tố.



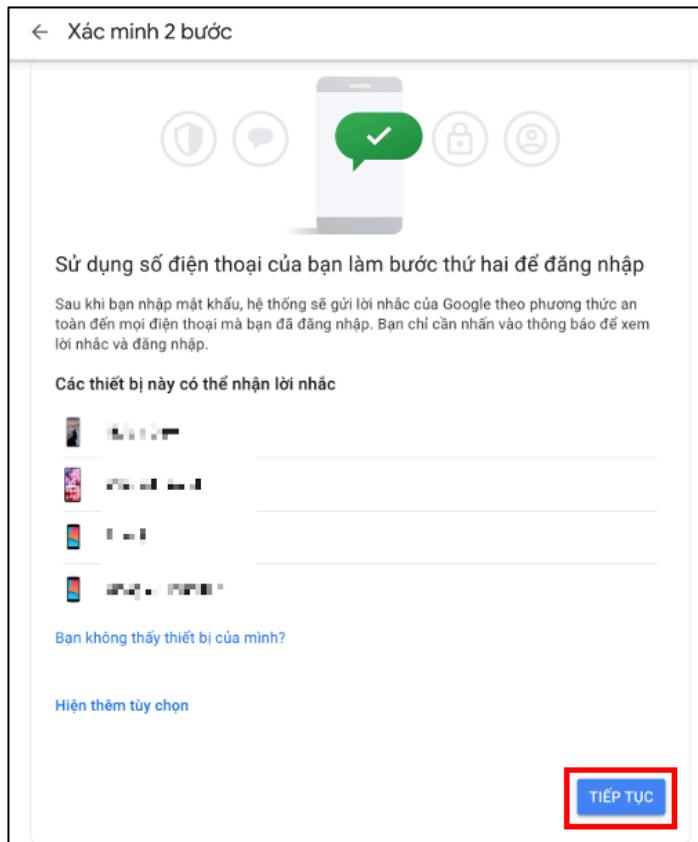
- Trong trường hợp chưa đăng ký xác thực 2 bước trước đó, cần xác minh danh tính của người dùng trước khi thiết lập khoá bảo mật. Nhấn **Bắt đầu**.



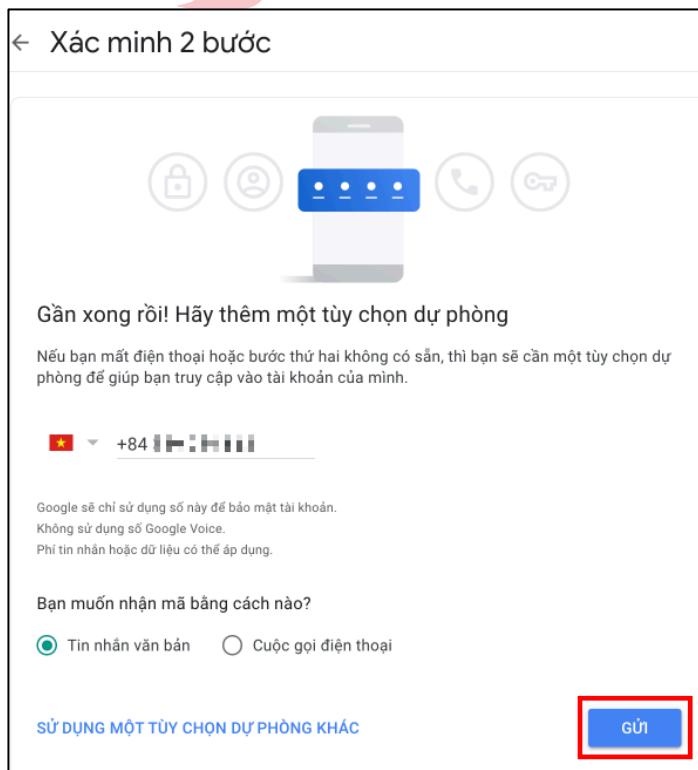
- Nhập mật khẩu để xác minh danh tính và nhấn **Tiếp theo**.



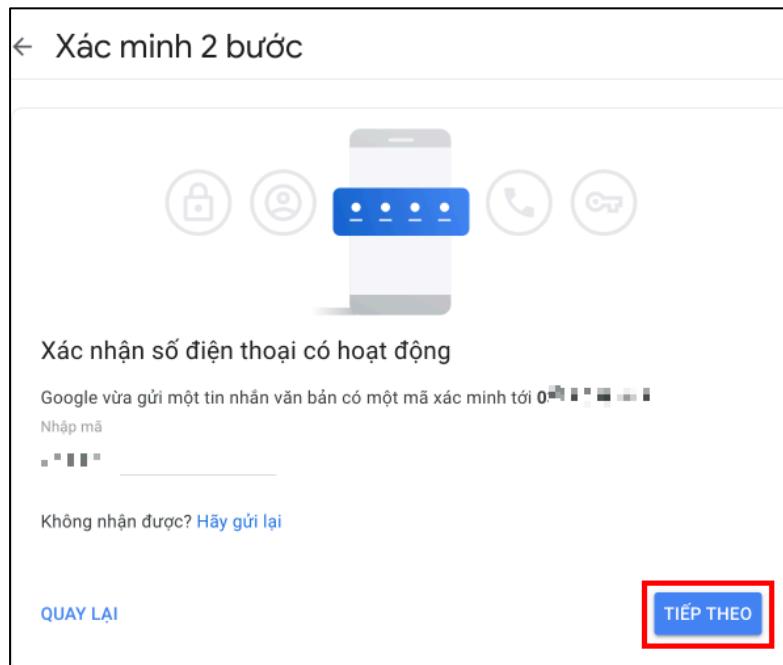
- Nhấn **Tiếp tục** để sử dụng số điện thoại làm bước thứ 2 để đăng nhập.



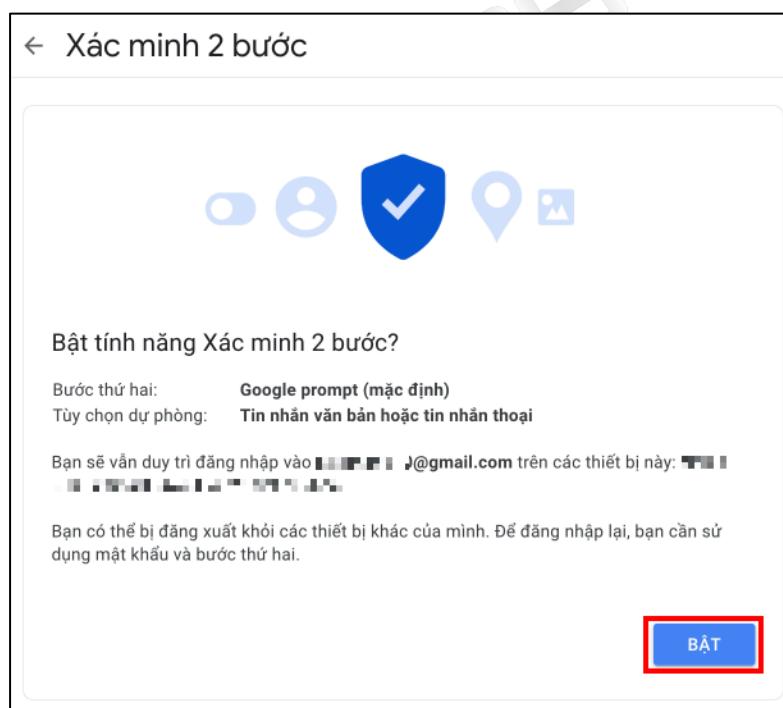
- Nhập số điện thoại và lựa chọn cách nhận mã rồi nhấn **Gửi** (**mặc định nhận bằng tin nhắn văn bản**).



- Nhập mã xác minh được gửi về điện thoại và nhấn **Tiếp theo**.



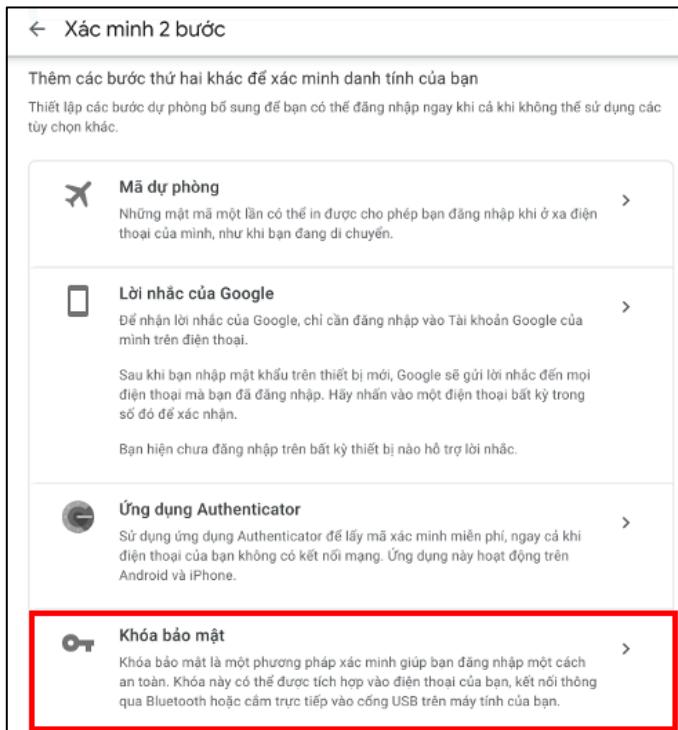
- Nhấn vào **Bật** để bật Xác minh 2 bước.



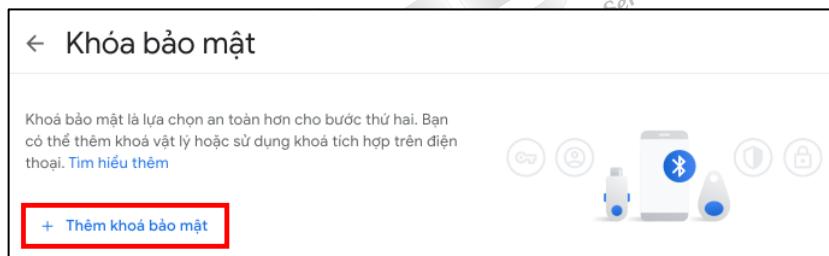
- Hoàn thành bước xác minh.



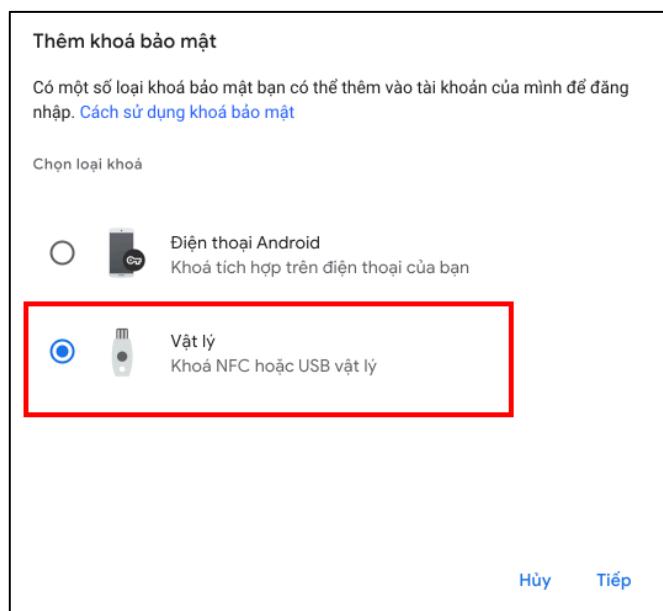
- Ở mục xác minh 2 bước, chọn **Khoá bảo mật**.



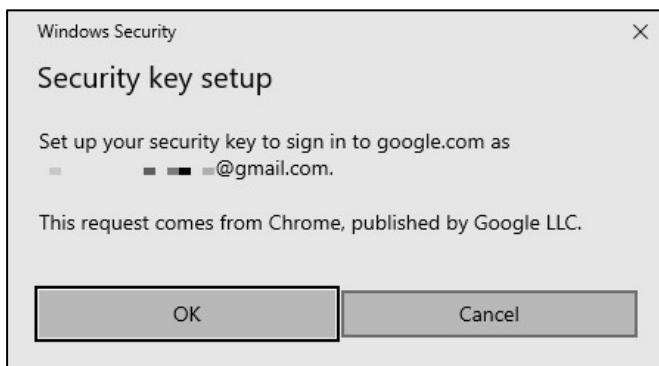
- Ở mục Khoá bảo mật chọn **Thêm khoá bảo mật**.



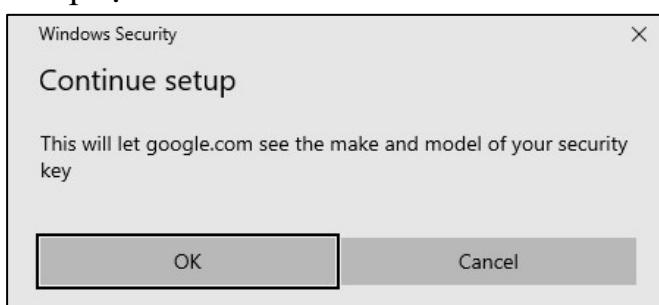
- Chọn **Vật lý** rồi nhấn **Tiếp** để thêm khóa bảo mật.



- Nhấn **OK** để tiếp tục quá trình đăng ký.

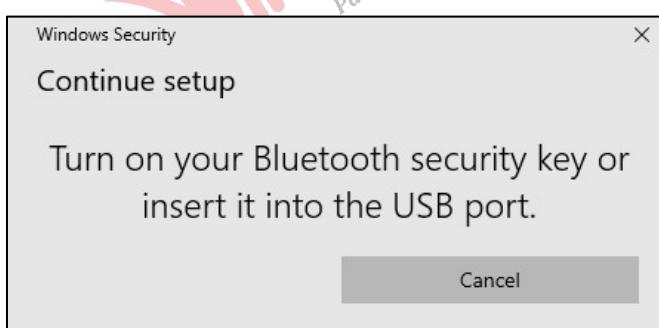


- Nhấn **OK** để tiếp tục.

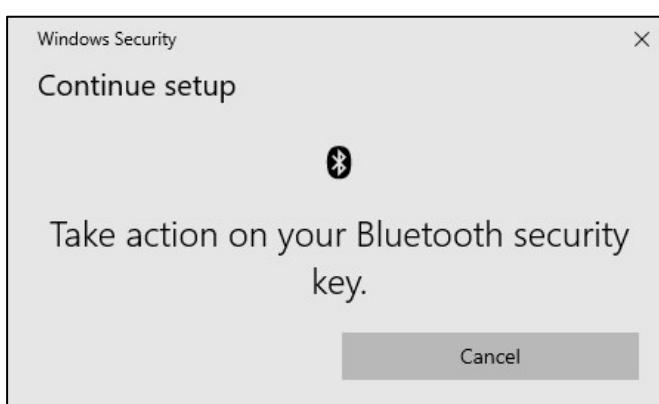


III.6.1.1. Sử dụng qua kết nối Bluetooth

- Người dùng kết nối khoá bảo mật VinCSS FIDO2® Fingerprint với máy tính thông qua Bluetooth.

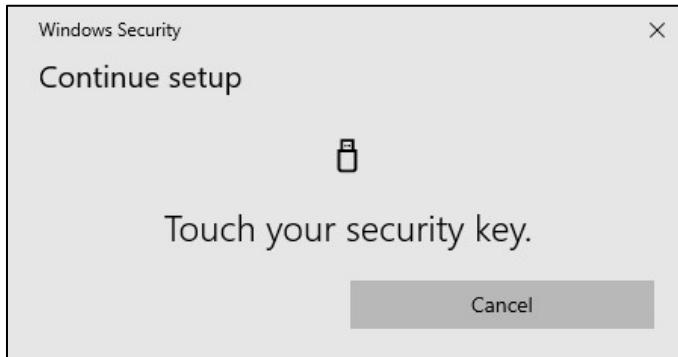


- Quét vân tay khi nhận được thông báo.



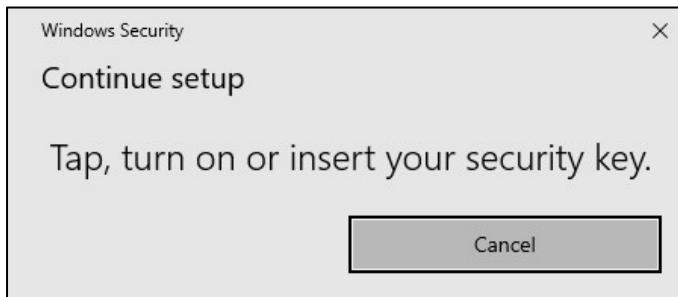
III.6.1.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.



III.6.1.3. Sử dụng qua kết nối NFC

- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



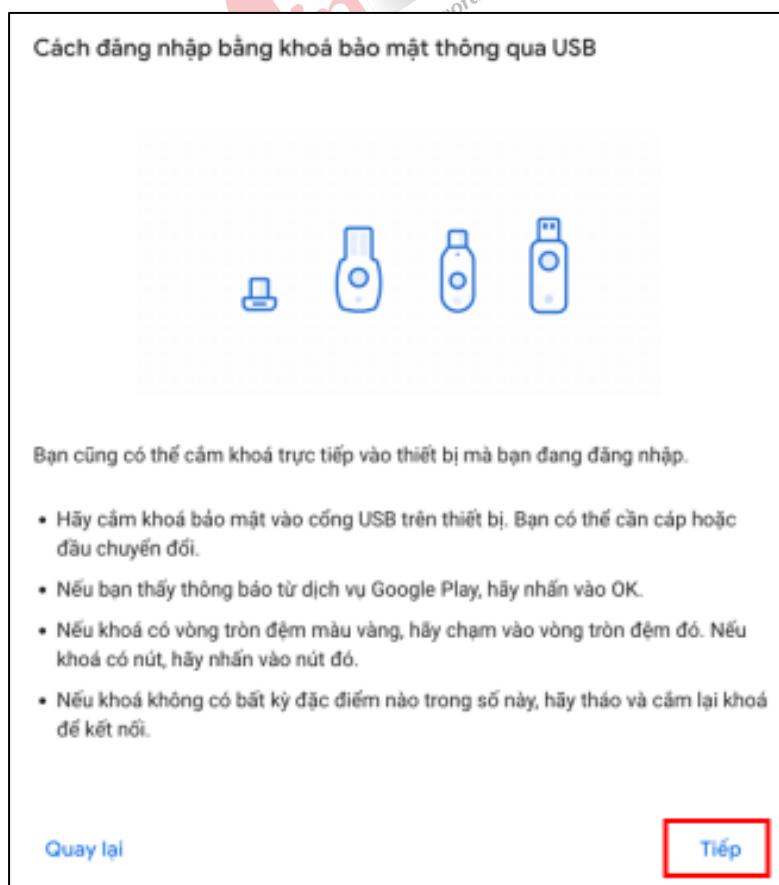
- Đặt tên cho thiết bị khoá bảo mật để dễ phân biệt trong trường hợp người dùng sử dụng đồng thời nhiều khóa (*tối đa 20 ký tự*), sau đó nhấn **Tiếp**.



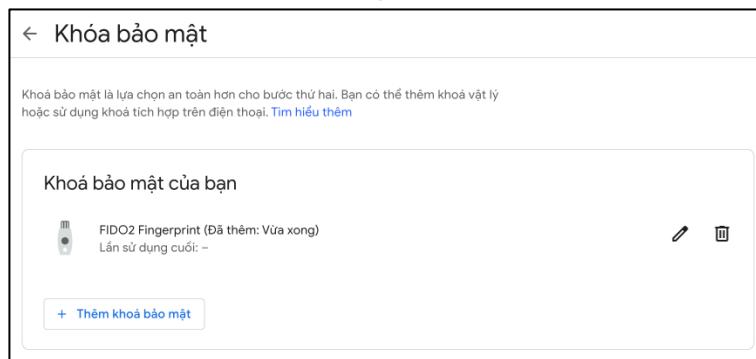
- Chọn **Tiếp** để hoàn thành quá trình đăng ký khoá bảo mật.



- Chọn **Tiếp** để hoàn tất đăng ký. Từ thời điểm này mọi dịch vụ của Google yêu cầu người dùng đăng nhập phải xác thực với cả mật khẩu và khóa bảo mật.

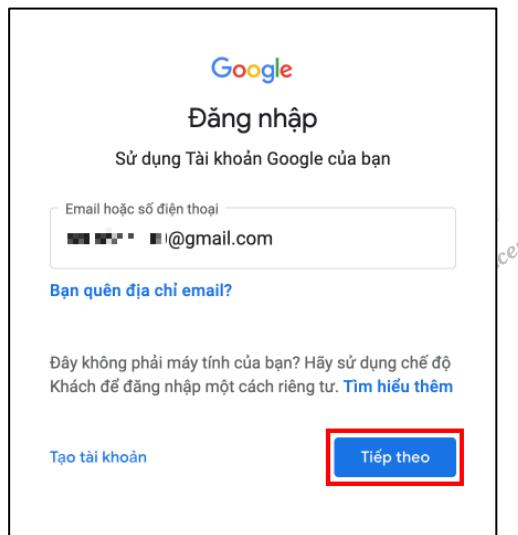


- Đăng ký khoá bảo mật thành công.



III.6.2. Xác thực 2 yếu tố với dịch vụ Google

- Truy cập vào <https://accounts.google.com/> rồi đăng nhập bằng tài khoản và mật khẩu.



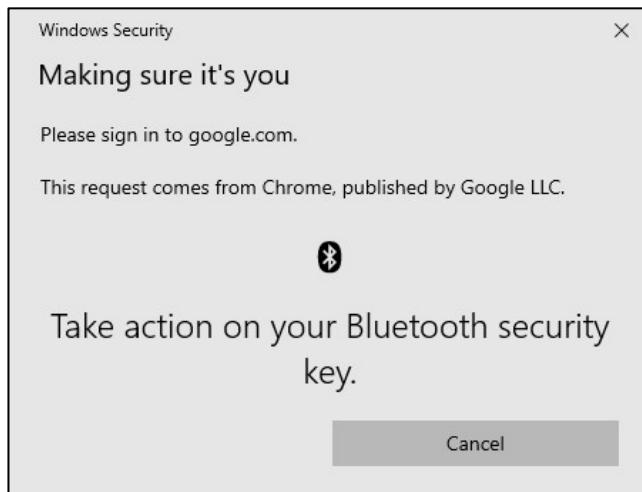
- Sau khi xác thực với mật khẩu, trình duyệt yêu cầu người dùng thực hiện xác thực bằng khóa bảo mật.

III.6.2.1. Sử dụng qua kết nối Bluetooth

- Kết nối khoá bảo mật VinCSS FIDO2® Fingerprint với máy tính thông qua Bluetooth.



- Quét vân tay khi nhận được thông báo.



III.6.2.2. Sử dụng qua kết nối USB

- Kết nối VinCSS FIDO2® Fingerprint vào máy tính thông qua dây USB. Chạm vào phần quét vân tay trên khoá bảo mật VinCSS FIDO2® Fingerprint khi nhận được thông báo.

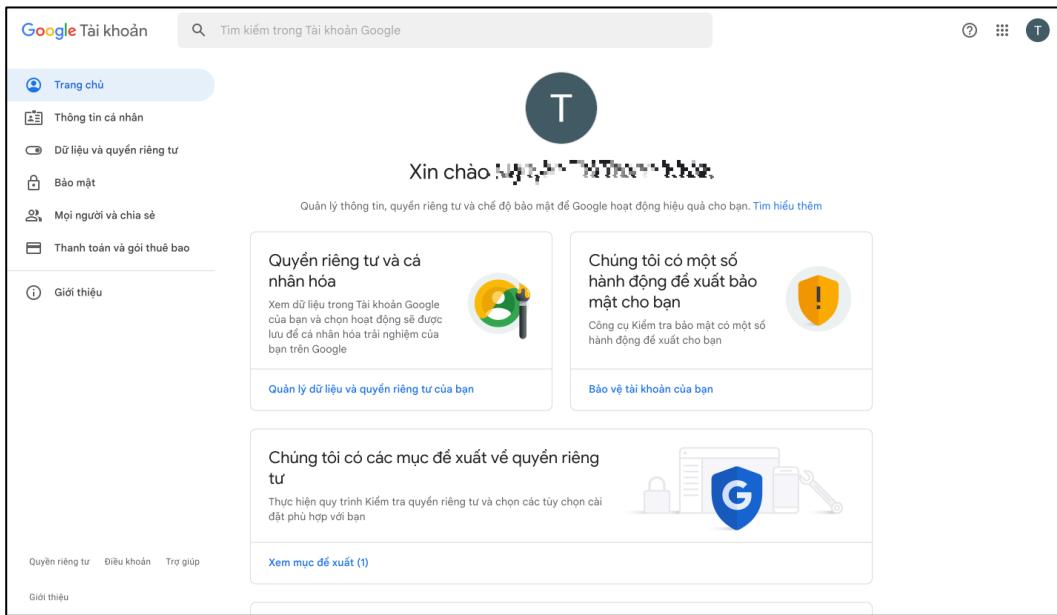


III.6.2.3. Sử dụng qua kết nối NFC

- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Quá trình đăng nhập thành công, người dùng vào được tài khoản.



The screenshot shows a Google Account page with a blue circular profile picture containing a white letter 'T'. The greeting says 'Xin chào **TuanThienHue**'. Below it, there's a link to 'Quản lý thông tin, quyền riêng tư và chế độ bảo mật để Google hoạt động hiệu quả cho bạn' and a 'Tim hiểu thêm' button. On the left, a sidebar lists: Trang chủ, Thông tin cá nhân, Dữ liệu và quyền riêng tư, Bảo mật, Mọi người và chia sẻ, Thanh toán và gói thuê bao, and Giới thiệu. The 'Giới thiệu' option is highlighted with a blue border. The main content area has three sections: 'Quyền riêng tư và cá nhân hóa' (with a green and yellow icon), 'Chúng tôi có một số hành động để xuất bảo mật cho bạn' (with an orange shield icon), and 'Chúng tôi có các mục để xuất về quyền riêng tư' (with a blue icon). At the bottom, there are links for 'Quyền riêng tư', 'Điều khoản', 'Trợ giúp', and 'Giới thiệu'.

THAM KHẢO

- Hệ sinh thái VinCSS FIDO2®:

<https://passwordless.vincss.net>

- Kênh Youtube VinCSS:

https://www.youtube.com/channel/UCNtS_7d4GtyecE2HCpJSr7g

- Các câu hỏi thường gặp:

<https://passwordless.vincss.net/hotro>

- Hướng dẫn sử dụng ứng dụng VinCSS OVPN Client:

<https://github.com/VinCSS-Public-Projects/FIDO2-Public-Documents/tree/main/VinCSS-OVPN-Client>

