

HƯỚNG DẪN SỬ DỤNG CÁC PHƯƠNG THỨC XÁC THỰC ĐỂ TRUY CẬP HỆ THỐNG VINCSS FIDO2 ECOSYSTEM

Ngày: 24/04/2024

Mã số: CSS-PRD-PQMC-INT-230424-015

Phiên bản: 1.0

Phân loại tài liệu: Tài liệu công bố

Thực hiện: TT. 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 thực hiện	Vị trí	Liên hệ	Ghi chú
1.1	24/04/2024				Cập nhật tài liệu



MỤC LỤC

THEO DÕI PHIÊN BẢN	2
MỤC LỤC	3
I. KHỞI TẠO TÀI KHOẢN VÀ ĐĂNG KÝ KHOÁ BẢO MẬT	5
I.1. TRUY CẬP TRÊN MÁY TÍNH.....	5
I.1.1. Đăng ký khoá bảo mật sử dụng khoá vật lý	6
I.1.2. Đăng ký khoá bảo mật sử dụng khoá mềm với ứng dụng VinCSS FIDO2	11
I.1.3. Đăng ký khoá bảo mật sử dụng Passkey	14
I.2. TRUY CẬP BẰNG ĐIỆN THOẠI	18
I.2.1. Đăng ký khoá bảo mật sử dụng Passkey trên điện thoại di động.....	19
I.2.2. Đăng ký khoá bảo mật sử dụng VinCSS FIDO2® Touch 1/ VinCSS FIDO2® Fingerprint hoặc các khoá bảo mật có tính năng tương tự	21
II. ĐĂNG NHẬP VÀO HỆ THỐNG	23
II.1. Truy cập trên máy tính.....	24
II.1.1. Đăng nhập bằng khoá bảo mật sử dụng khoá vật lý.....	24
II.1.2. Đăng nhập bằng ứng dụng VinCSS FIDO2	27
II.1.3. Đăng nhập hệ thống bằng passkey	30
II.2. Truy cập bằng điện thoại thông minh	35
II.2.1. Đăng nhập bằng passkey trên thiết bị.....	36
II.2.2. Đăng nhập bằng khoá bảo mật vật lý VinCSS FIDO2® Touch 1/ VinCSS FIDO2® Fingerprint hoặc các khoá bảo mật có tính năng tương tự.....	37
III. ĐĂNG KÝ THÊM KHOÁ BẢO MẬT MỚI.....	40

Để sử dụng tính năng xác thực mạnh, an toàn, không mật khẩu thông qua hệ thống hệ thống VinCSS FIDO2 Ecosystem, người dùng cần **khởi tạo tài khoản và đăng ký khoá bảo mật**, sau đó có thể sử dụng khoá đã đăng ký để **đăng nhập vào hệ thống**. Tài liệu này hướng dẫn người dùng đăng ký và đăng nhập vào hệ thống hệ thống VinCSS FIDO2 Server Enterprise.

Để truy cập hệ thống VinCSS FIDO2 Server Enterprise trên các trình duyệt, người dùng có thể truy cập theo các phương thức sau đây:

- Truy cập trên máy tính.
- Truy cập trên điện thoại thông minh.



I. KHỞI TẠO TÀI KHOẢN VÀ ĐĂNG KÝ KHOÁ BẢO MẬT

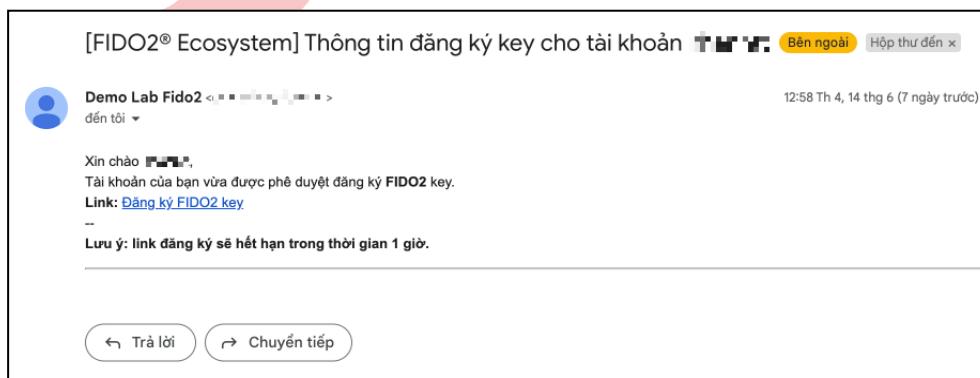
- Người dùng mới cần phải được quản trị viên hệ thống tạo tài khoản trước khi có thể khởi tạo khoá bảo mật và đăng nhập vào hệ thống.
- Khi quản trị hệ thống tạo khoá bảo mật cho người dùng, một đường dẫn đăng ký khoá bảo mật sẽ được gửi cho người dùng qua email hoặc IM (*tùy cấu hình của từng hệ thống*) để tiến hành đăng ký khoá bảo mật cho lần đầu tiên sử dụng.

Ví dụ:

- *Hình dưới đây người dùng sẽ nhận thông báo qua Element (một ứng dụng IM):*



- *Hình dưới đây người dùng sẽ nhận thông báo qua Email.*



I.1. TRUY CẬP TRÊN MÁY TÍNH

Lưu ý: Các bước thực hiện để đăng ký khoá bảo mật sử dụng khoá vật lý trên máy tính sử dụng hệ điều hành Windows, Linux và macOS tương tự nhau. Dưới đây là hướng dẫn minh họa các bước thực hiện trên hệ điều hành Windows.

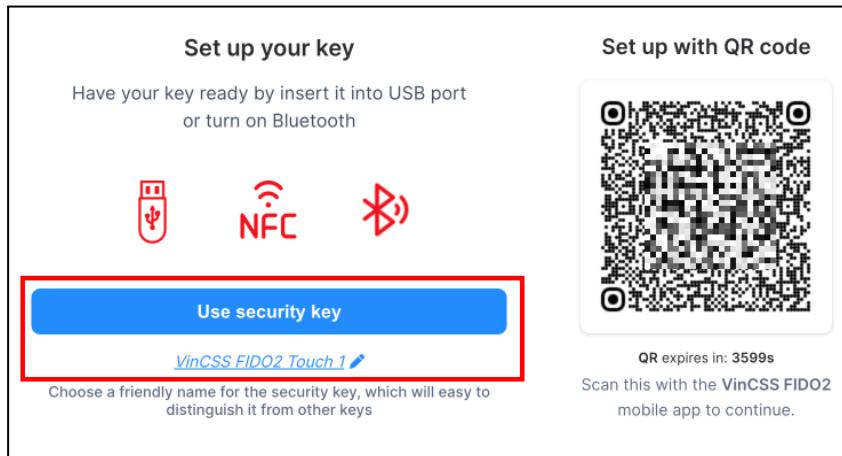
I.1.1. Đăng ký khoá bảo mật sử dụng khoá vật lý

I.1.1.1. Đăng ký khoá bảo mật sử dụng VinCSS FIDO2® Touch 1 hoặc các khoá bảo mật có tính năng tương tự



Lưu ý: Vui lòng thiết lập mã PIN cho khoá bảo mật trước khi tiến hành đăng ký. Chi tiết tham khảo tại: <https://github.com/VinCSS-Public-Projects/FIDO2-Public-Documents/blob/main/VinCSS-FIDO2-Touch-1>

- Sau khi nhấp vào đường link, người dùng sẽ được chuyển hướng đến trang đăng ký khoá bảo mật. Trên giao diện đăng ký khoá bảo mật, điền tên khoá bảo mật sau đó chọn “Use security key”.



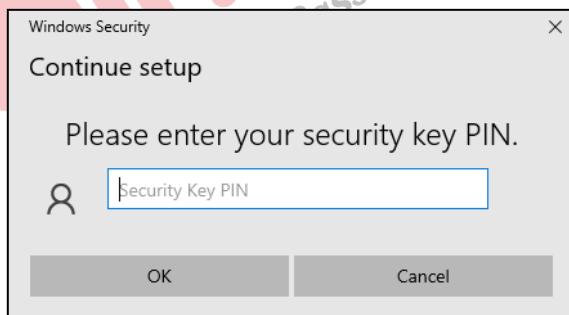
- Kết nối khoá bảo mật với máy tính, nhấn **OK**.



- Nhấn **OK** để tiếp tục.



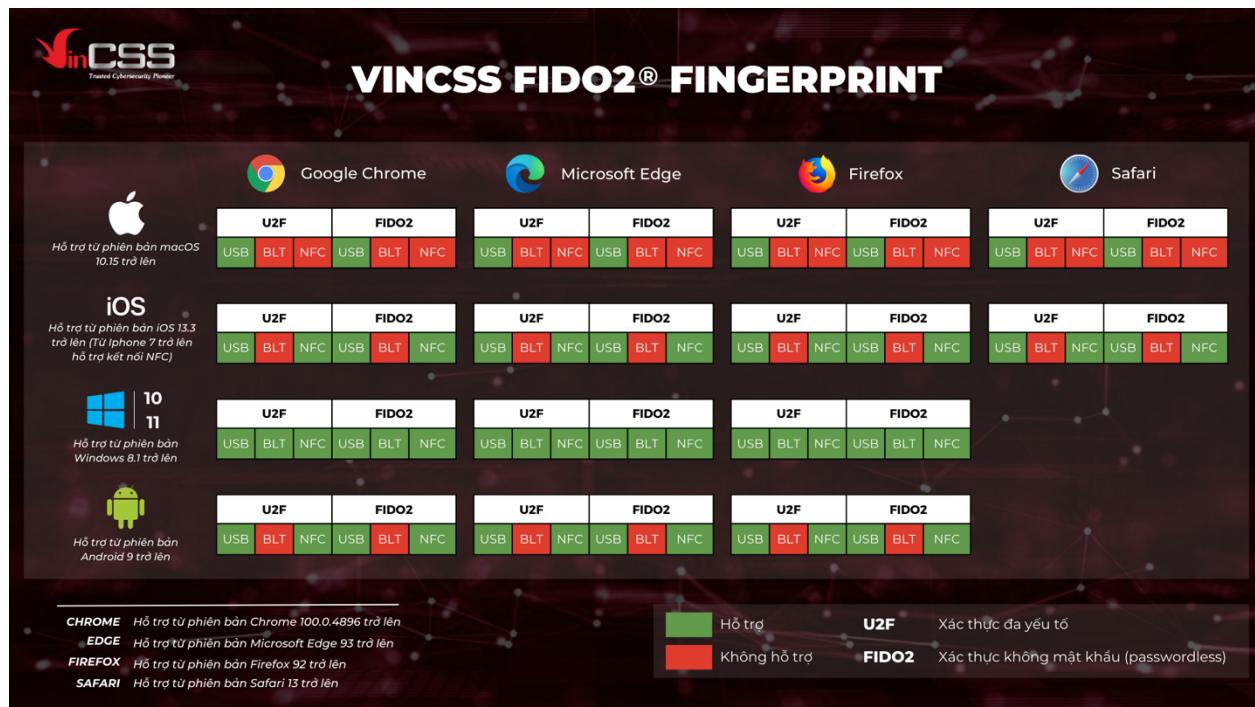
- Nhập mã PIN của khoá bảo mật.



- Chạm vào khoá bảo mật để hoàn tất quá trình đăng ký khoá.

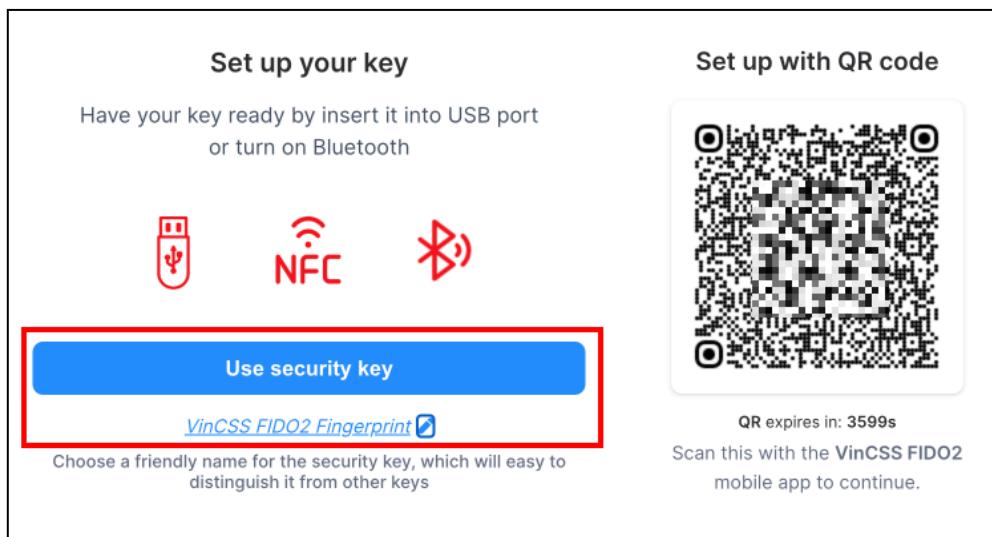


I.1.1.2. Đăng ký khoá bảo mật sử dụng VinCSS FIDO2® Fingerprint hoặc các khoá bảo mật có hỗ trợ sinh trắc học

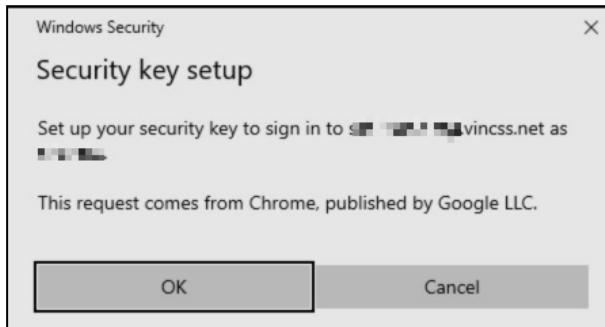


Lưu ý: Vui lòng thiết lập mã PIN cho khoá bảo mật trước khi tiến hành đăng ký. Chi tiết tham khảo tại: <https://github.com/VinCSS-Public-Projects/FIDO2-Public-Documents/blob/main/VinCSS-FIDO2-Fingerprint>

- Sau khi nhấp vào đường link, người dùng sẽ được chuyển hướng đến trang đăng ký khoá bảo mật. Trên giao diện đăng ký khoá bảo mật, điền tên khoá bảo mật sau đó chọn “Use security key”.



- Nhấn **OK** để bắt đầu tiến hành đăng ký khoá bảo mật.

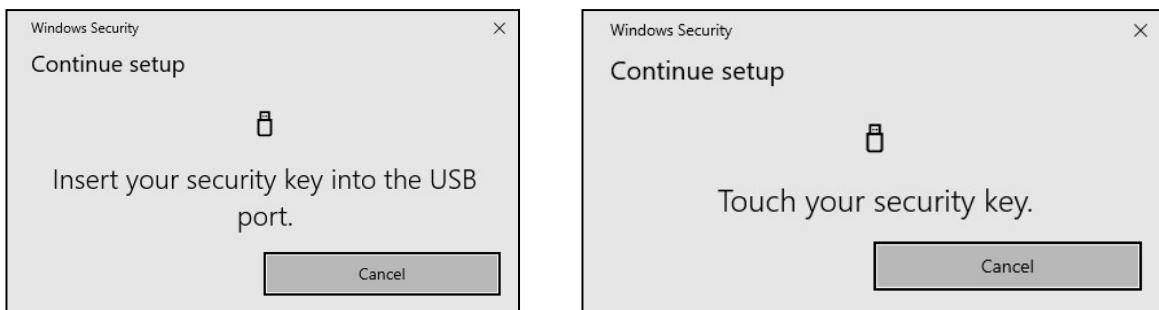


- Nhấn **OK** để tiếp tục.



I.1.1.2.1. Sử dụng kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB. Quét vân tay khi nhận được thông báo.



I.1.1.2.2. Sử dụng kết nối Bluetooth

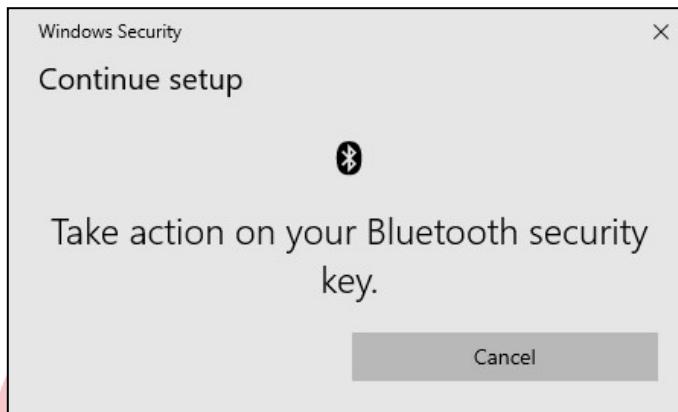
Lưu ý: Vui lòng kết nối khoá bảo mật với máy tính trước khi sử dụng.

Chi tiết tham khảo tại: <https://github.com/VinCSS-Public-Projects/FIDO2-Public-Documents/blob/main/VinCSS-FIDO2-Fingerprint>

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



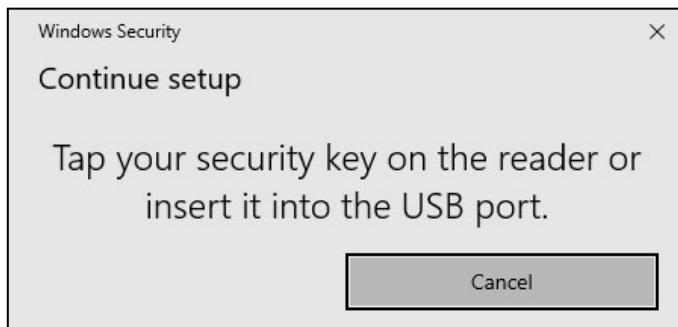
- Quét vân tay khi nhận được thông báo.



I.1.1.2.3. Sử dụng kết nối NFC

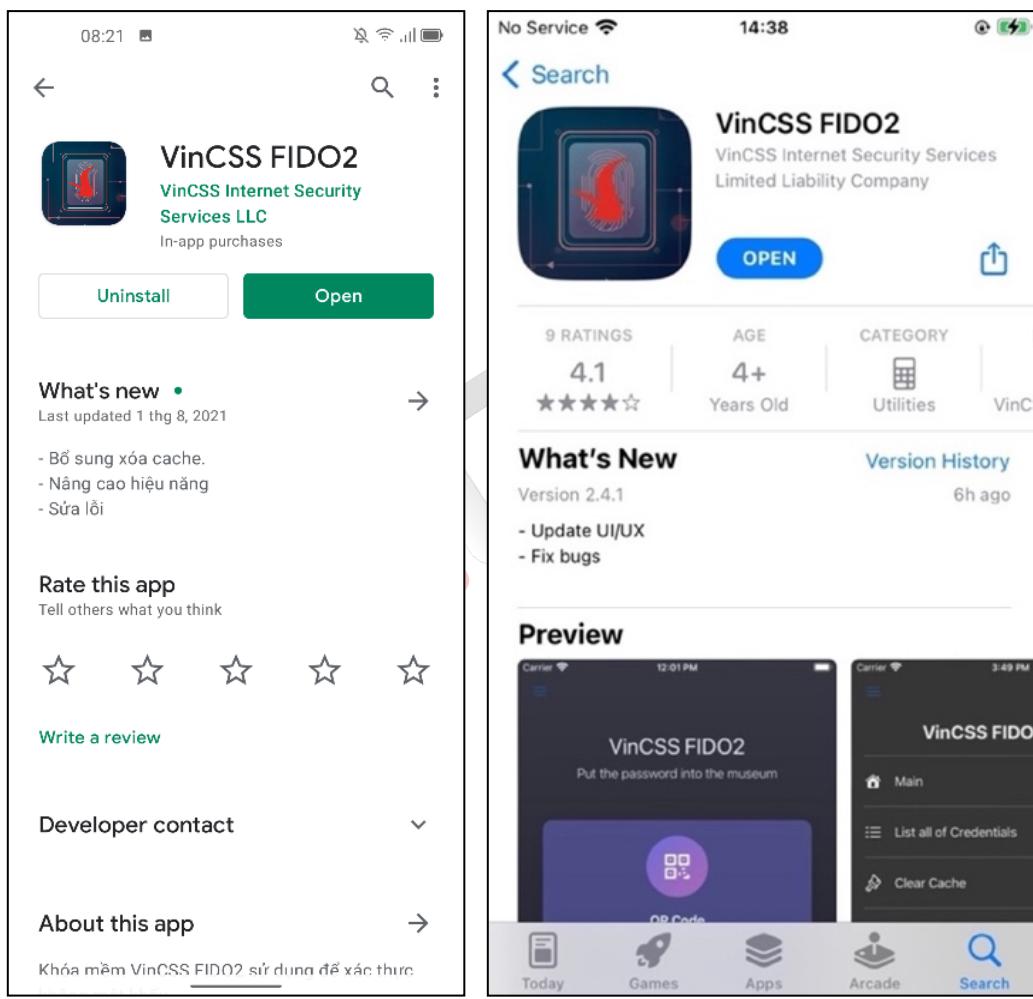
Lưu ý: Máy tính cần có phần cứng hỗ trợ kết nối NFC hoặc đã kết nối với đầu đọc NFC.

- 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.



I.1.2. Đăng ký khoá bảo mật sử dụng khoá mềm với ứng dụng VinCSS FIDO2

- Cài đặt ứng dụng VinCSS FIDO2 trên điện thoại thông minh.
 - o **Android:** Trên **Play Store** tìm kiếm từ khóa “**VinCSS FIDO2**”, chọn **Install** để tải về và cài đặt ứng dụng.
 - o **iOS:** Trên **App Store** tìm kiếm từ khóa ”**VinCSS FIDO2**”, chọn biểu tượng  để tải về và cài đặt ứng dụng.

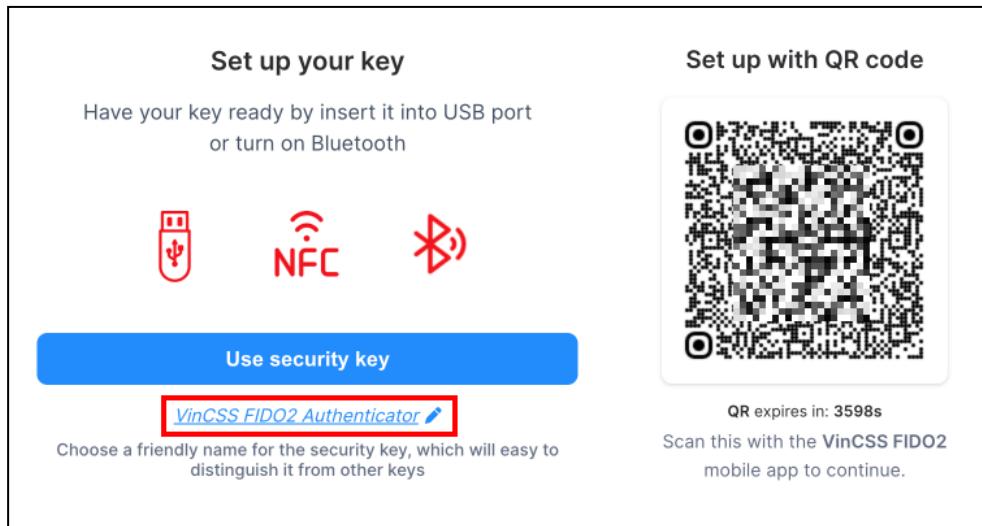


Android

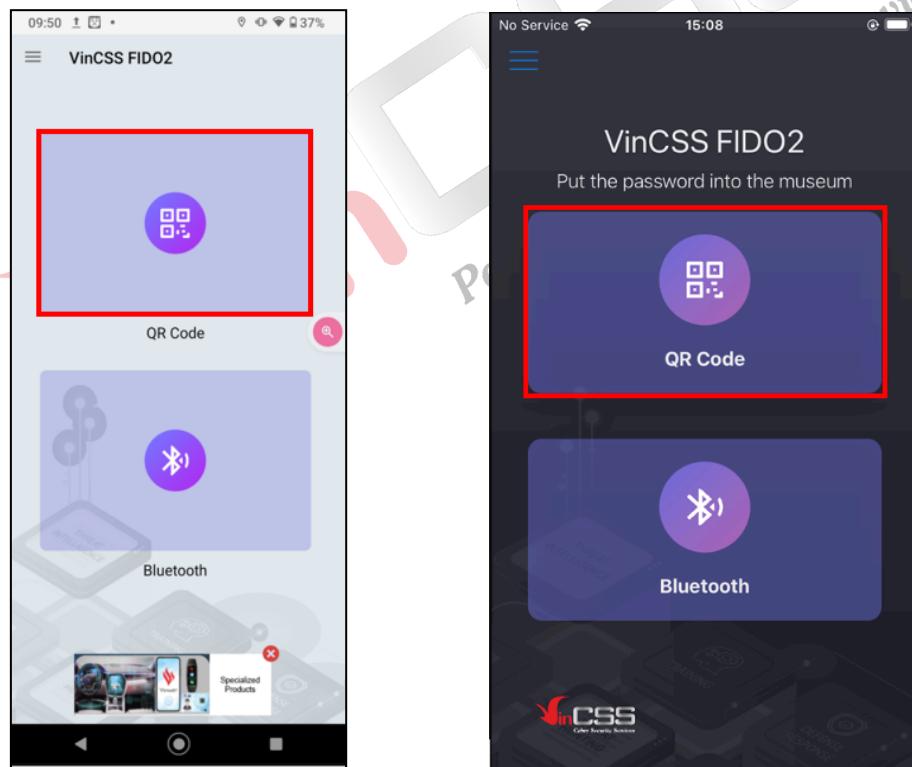
iOS

Lưu ý: Để sử dụng các hình thức trên để đăng ký khoá bảo mật, điện thoại phải thiết lập xác thực bằng sinh trắc học hoặc bật chế độ sử dụng mã PIN tại ứng dụng VinCSS FIDO2 (đối với hệ điều hành Android) hoặc xác thực bằng FaceID/TouchID (đối với hệ điều hành iOS) và ứng dụng được cấp quyền truy cập.

- Trên giao diện đăng ký khoá, điền tên khóa bảo mật.



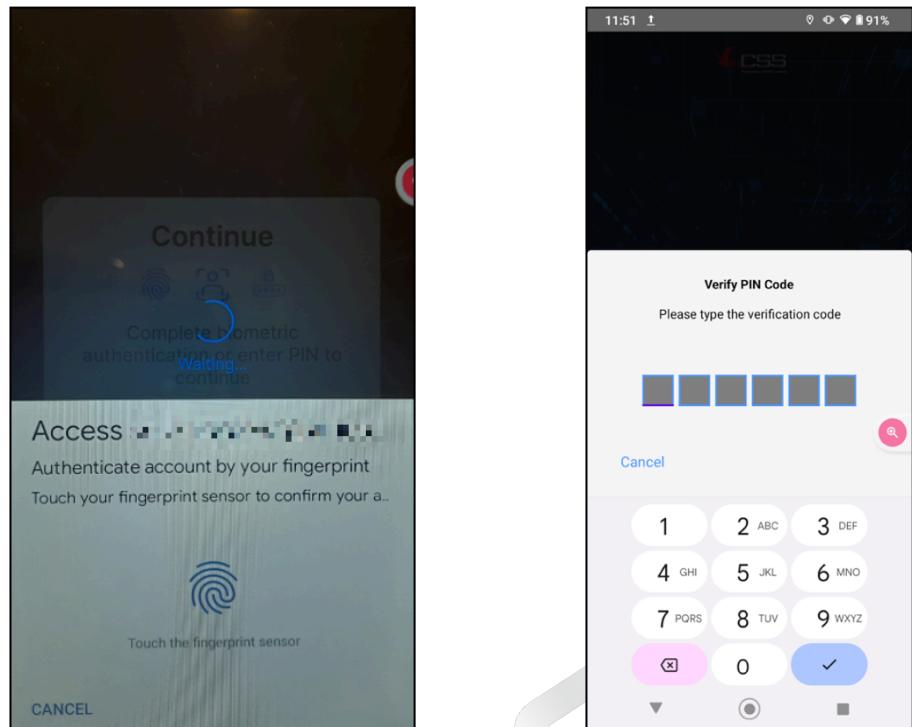
- Trên giao diện ứng dụng VinCSS FIDO2, chọn **QR code**. Sau đó tiến hành quét mã QR trên giao diện đăng ký khoá (*Mã QR này có hiệu lực trong 1 giờ*).



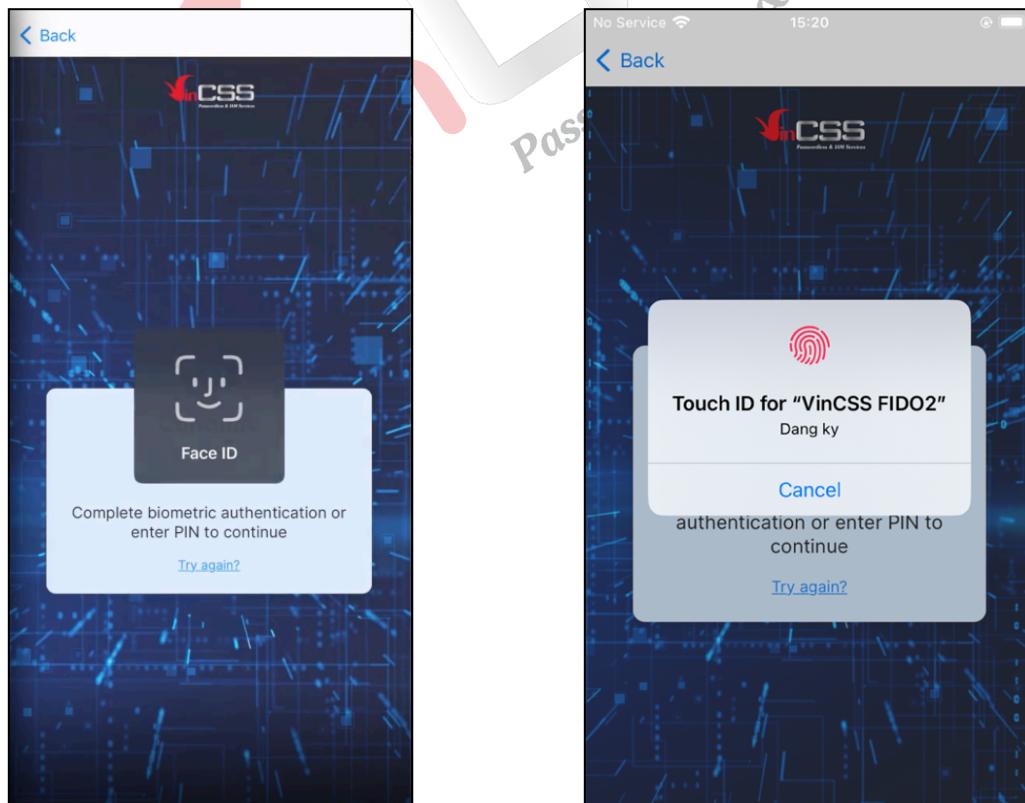
Android

iOS

- Đối với hệ điều hành **Android**: Xác nhận bằng sinh trắc học hoặc nhập mã PIN (*theo yêu cầu của thiết bị*).



- Đối với hệ điều hành iOS: chọn **Register** sau đó xác nhận FaceID/TouchID trên điện thoại (*theo yêu cầu của thiết bị*).

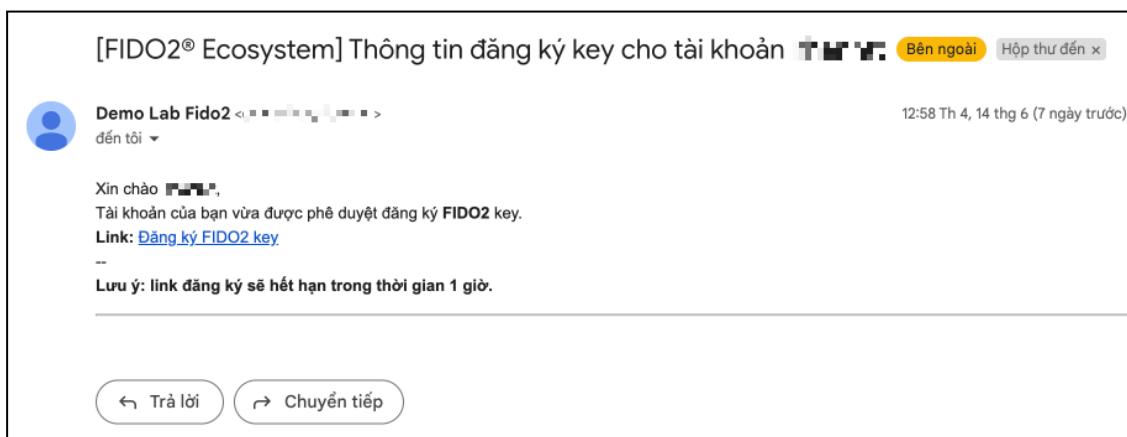


I.1.3. Đăng ký khoá bảo mật sử dụng Passkey

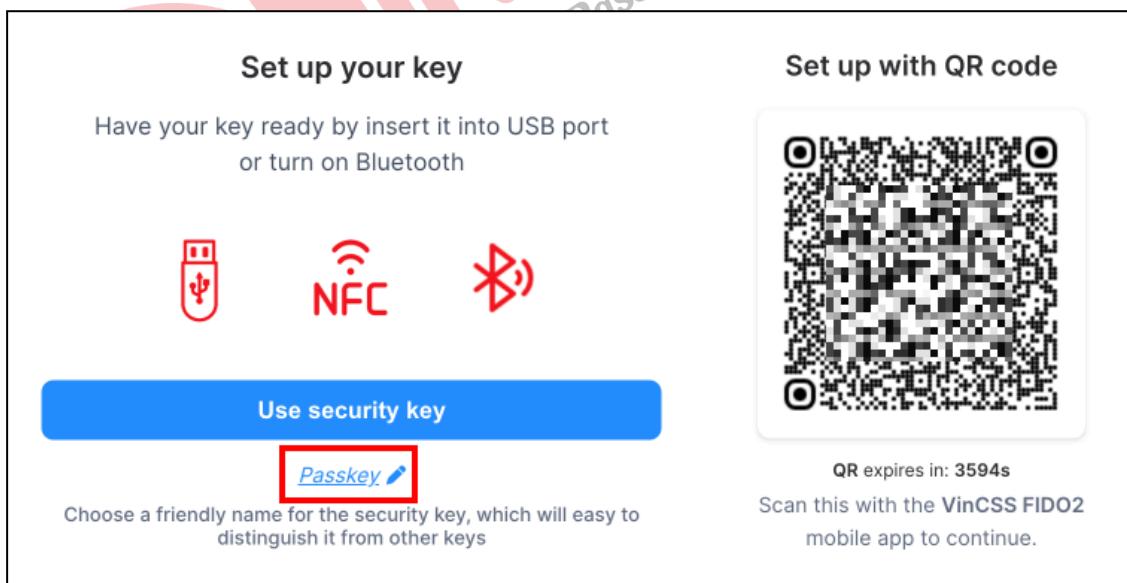
I.1.3.1. Passkey trên điện thoại thông minh

Lưu ý: Passkey hỗ trợ Android 9+, đã đăng nhập Google Account hoặc iOS 16+. Passkey sẽ được lưu trên điện thoại thông minh.

- Liên hệ quản trị viên để lấy link đăng ký Passkey khi xác thực không mật khẩu. Một đường dẫn được gửi tới người dùng qua email hoặc IM (có hiệu lực trong 1 giờ, tùy cấu hình của từng hệ thống) để tiến hành đăng ký khoá bảo mật cho lần đầu sử dụng (Ví dụ nhận link đăng ký qua email).

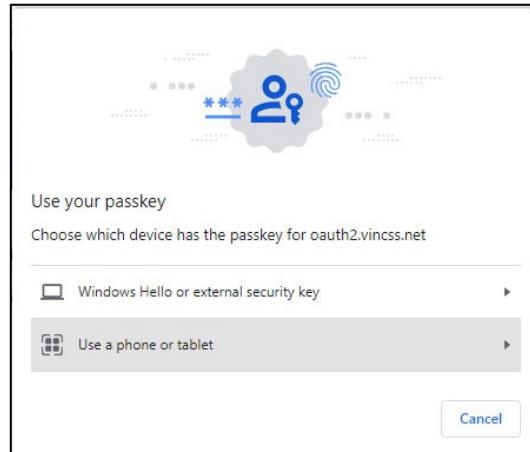


- Nhấn vào link đăng ký khoá bảo mật sau đó đổi tên khoá bảo mật.

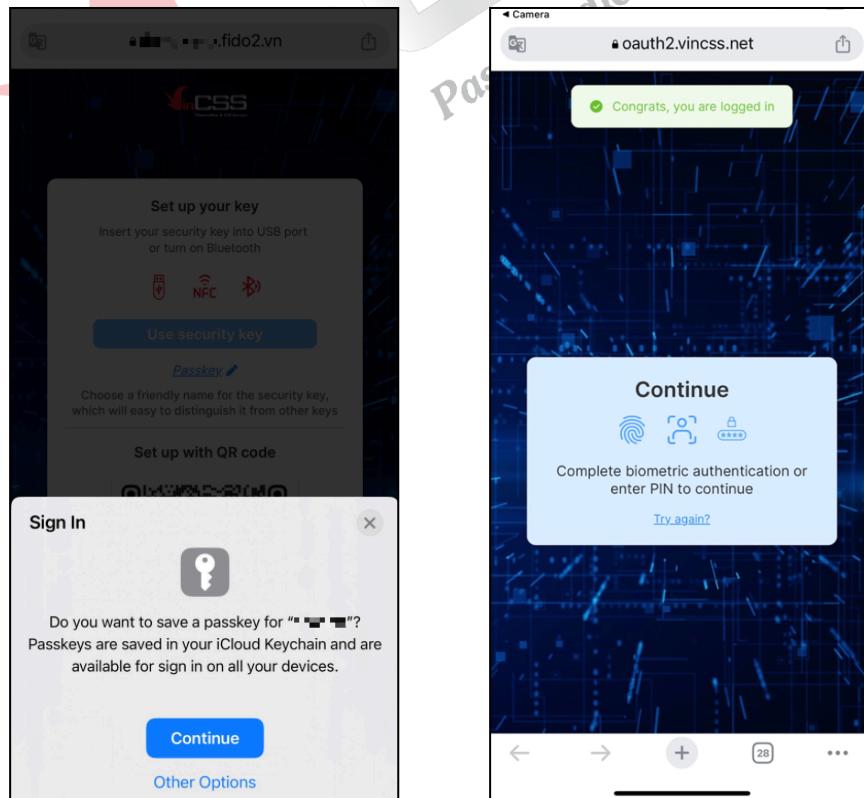


- Người dùng có thể đăng ký Passkey bằng cách quét trực tiếp QR Code hiện trên màn hình đăng ký theo hướng dẫn phía dưới.

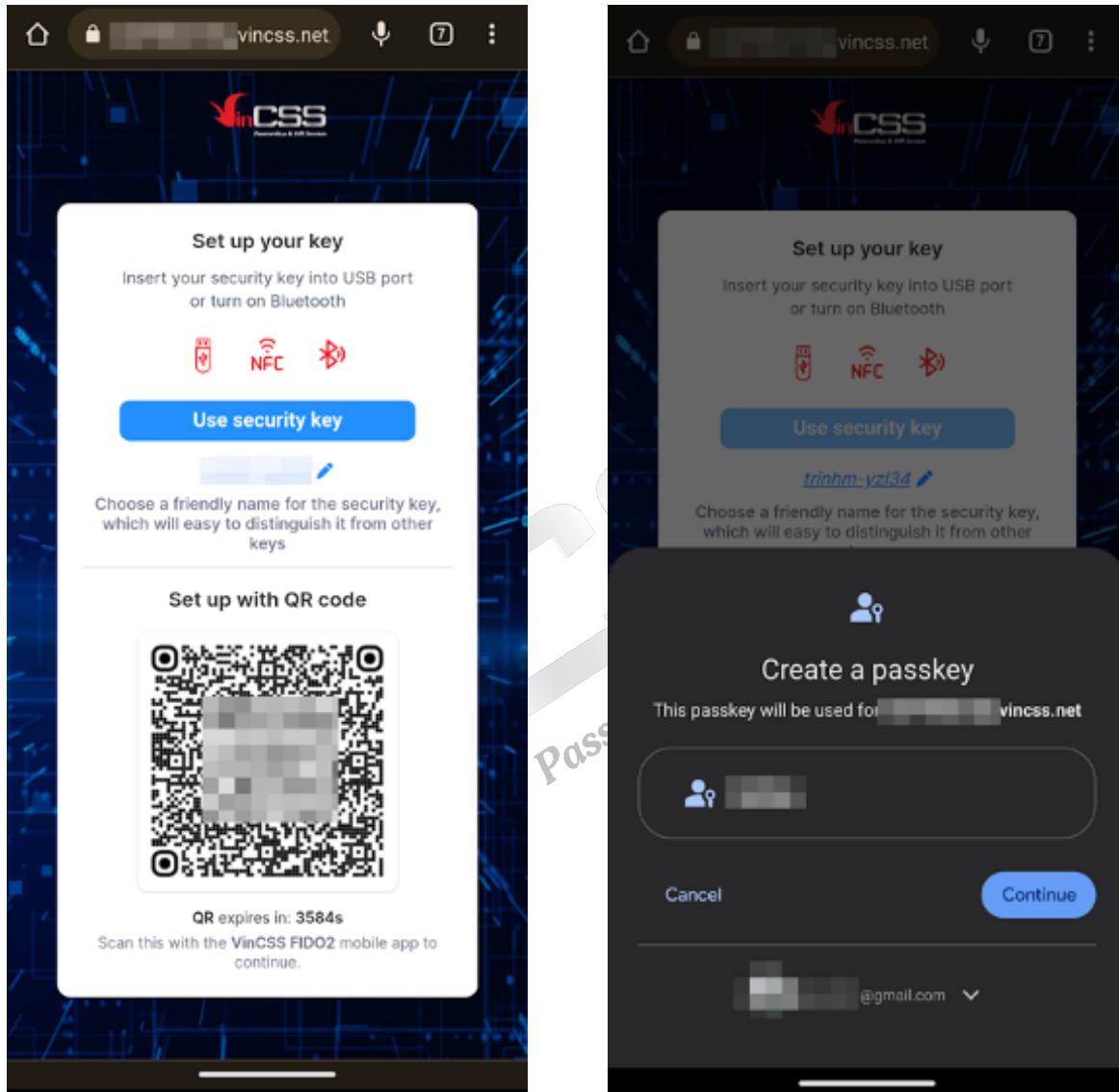
- Hoặc người dùng có thể đăng ký passkey theo hình thức khác bằng cách nhấn **Use security key** trên giao diện đăng ký, chọn **Use a phone or table**, tiến hành quét QR Code được hiện ra theo hướng dẫn phía dưới. (*Hình thức này yêu cầu cả máy tính và điện thoại phải có hỗ trợ Bluetooth*).



- **Đối với thiết bị iOS:** Mở phần mềm quét mã QR hoặc Camera trên điện thoại, sau đó tiến hành quét mã QR trên màn hình máy tính. Mở đường link quét được bằng trình duyệt, chọn **Continue**, sau đó xác thực bằng **FaceID/Touch ID** để hoàn tất đăng ký.



- **Đối với thiết bị Android:** Mở phần mềm quét mã QR hoặc Camera trên điện thoại, sau đó tiến hành quét mã QR trên màn hình máy tính. Mở đường link quét được bằng trình duyệt, chọn **Continue**, sau đó xác thực bằng **phương thức mở khoá màn hình** để hoàn tất.



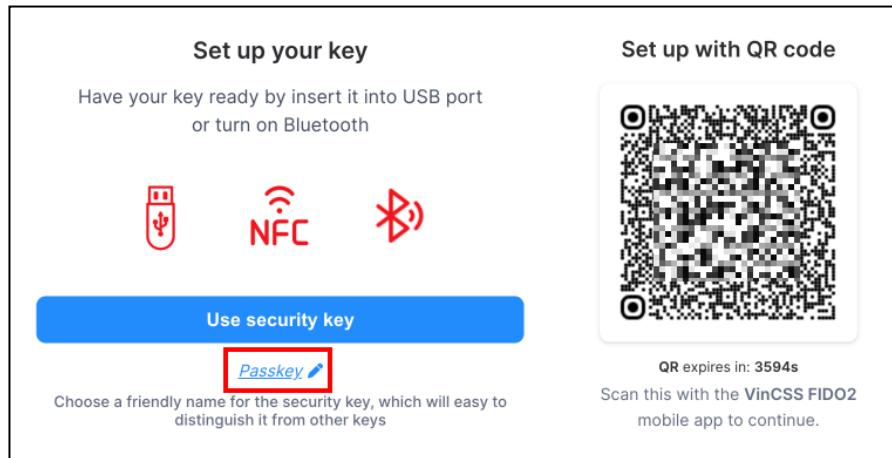
I.1.3.2. Passkey trên máy tính

I.1.3.2.1. Windows

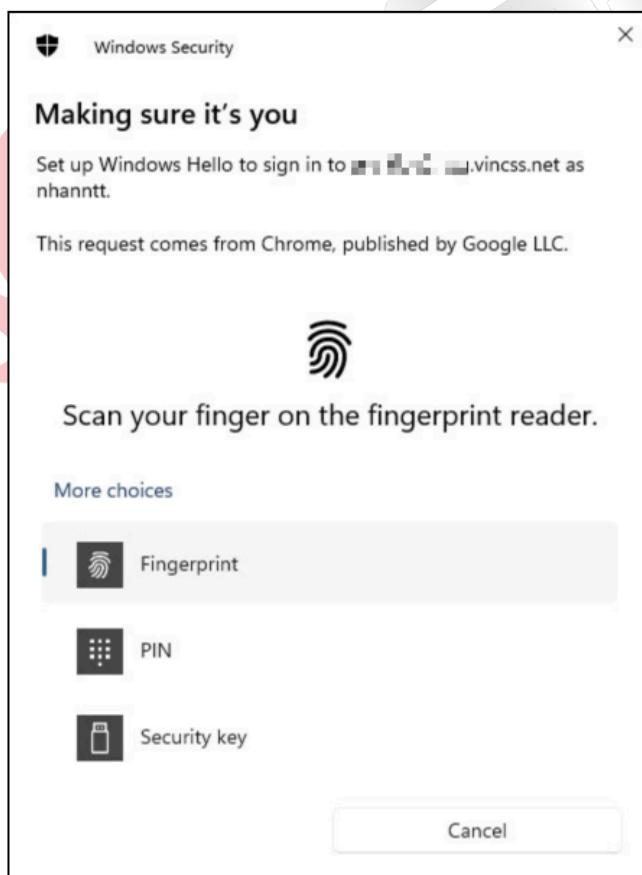
Lưu ý: Hỗ trợ Windows 11+.

Người dùng có thể đăng ký passkey trực tiếp tại máy tính bằng **Windows Hello** theo các bước như sau:

- Truy cập link đăng ký đã được gửi bởi quản trị viên, đổi tên khoá bảo mật và chọn **Use security key**.



- Sau đó chọn **Windows Hello or external security key**. Lựa chọn hình thức xác thực bằng **Fingerprint/PIN** để hoàn tất việc đăng ký.

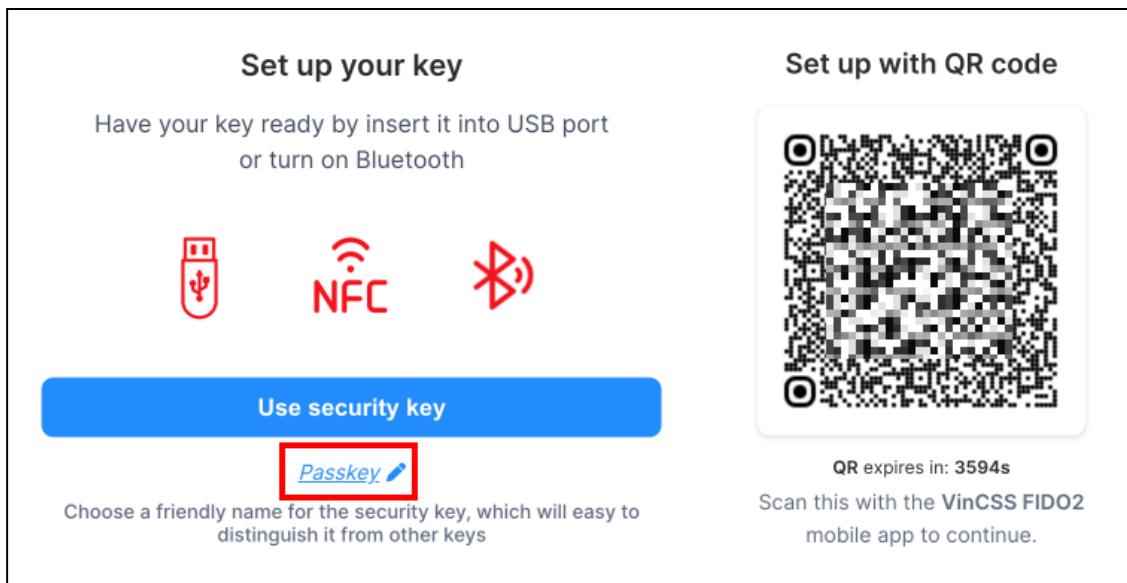


Lưu ý: Đối với phương thức xác thực **Security key**, người dùng vui lòng tham khảo mục [I.1.1.](#))

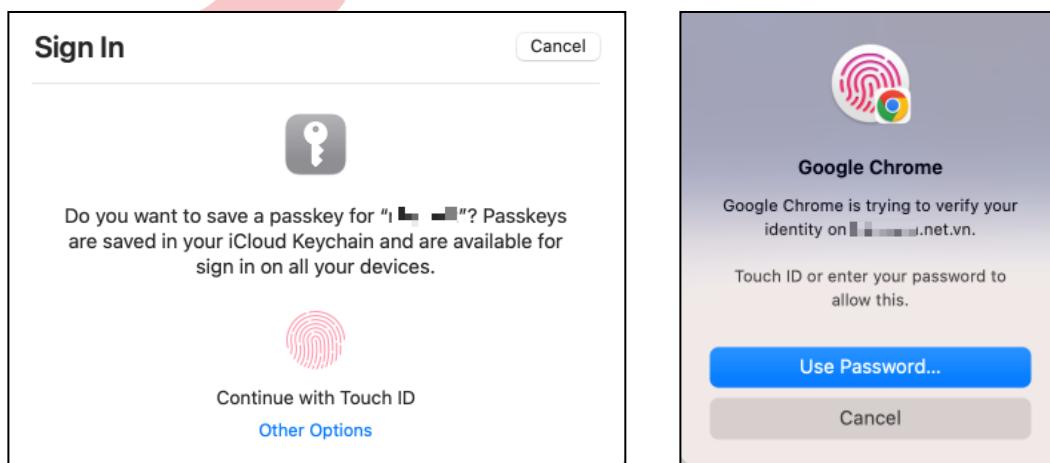
I.1.3.2.2. macOS

Ngoài ra, người dùng có thể đăng ký passkey trực tiếp tại máy tính thông qua trình duyệt **Safari** (*đối với hệ điều hành macOS*) hoặc **Chrome** (*đối với tất cả các hệ điều hành cho phép sử dụng passkey trên trình duyệt này*) theo các bước như sau.

- Truy cập link đăng ký đã được gửi bởi quản trị viên bằng trình duyệt **Safari/Chrome**, sau đó đổi tên khoá bảo mật.



- Chọn **Use security key**, sau đó xác thực bằng **TouchID/Password** (*tùy theo yêu cầu của thiết bị*) để hoàn thành quá trình đăng ký.



I.2. TRUY CẬP BẰNG ĐIỆN THOẠI

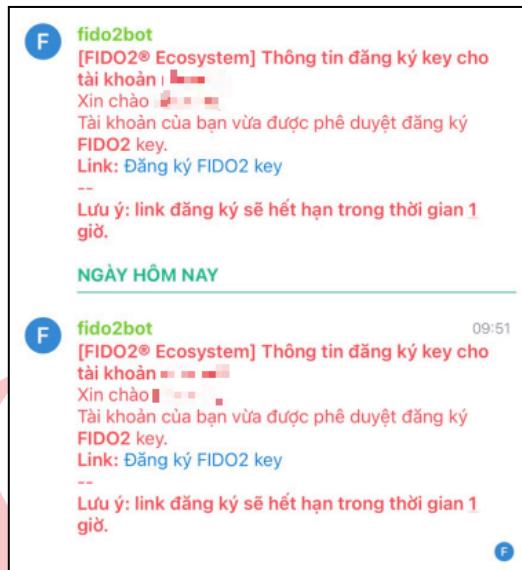
Lưu ý: Passkey hỗ trợ Android 9+, đã đăng nhập Google Account hoặc iOS 16+. Passkey sẽ được lưu trên điện thoại thông minh.

I.2.1. Đăng ký khoá bảo mật sử dụng Passkey trên điện thoại di động

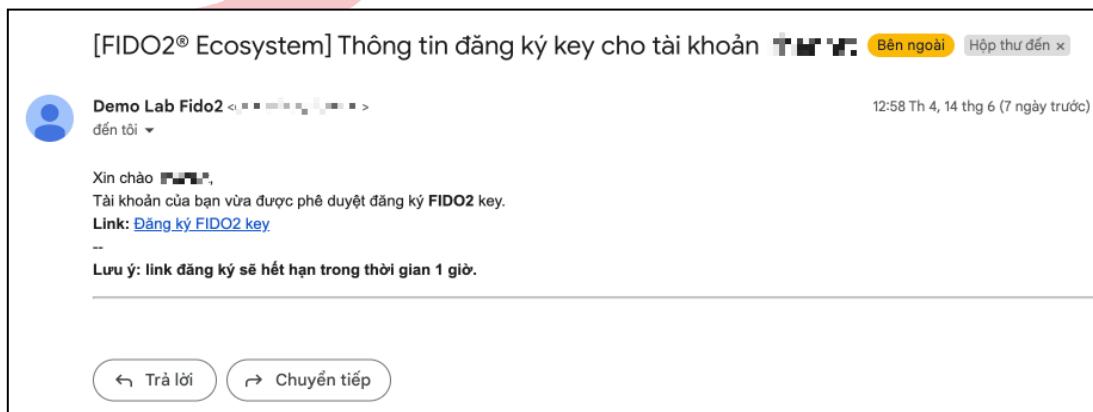
- Liên hệ quản trị viên để lấy link đăng ký Passkey khi xác thực không mật khẩu. Một đường dẫn được gửi tới người dùng qua email hoặc IM (*có hiệu lực trong 1 giờ, tùy cấu hình của từng hệ thống*) để tiến hành đăng ký khoá bảo mật cho lần đầu sử dụng.

Ví dụ:

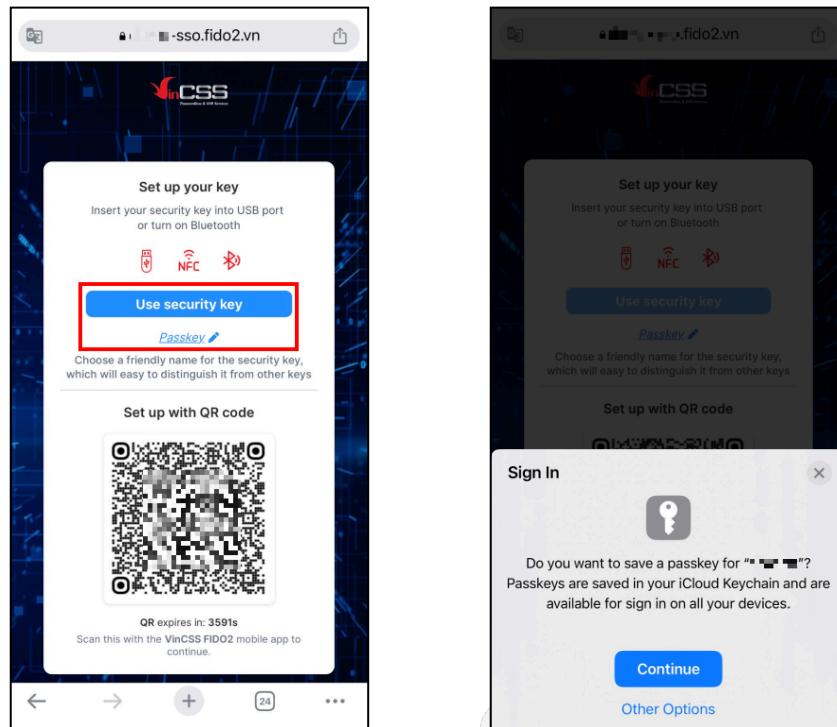
- *Hình dưới đây người dùng sẽ nhập thông báo qua Element (một ứng dụng IM):*



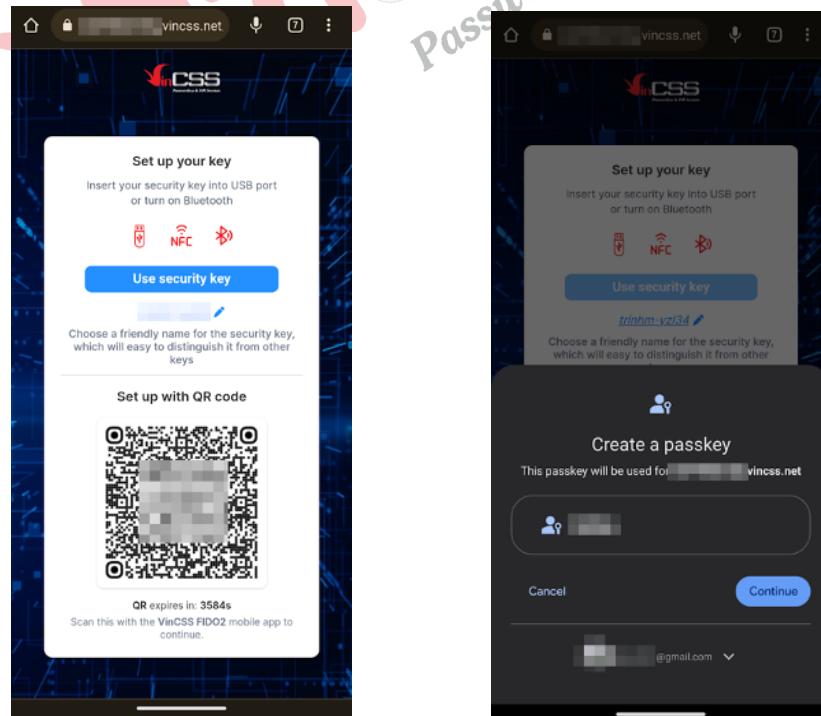
- *Hình dưới đây người dùng sẽ nhập thông báo qua Email.*



- **Đối với thiết bị iOS:** Nhấn vào link đăng ký khoá bảo mật rồi đổi tên khoá bảo mật, chọn **Use security key**. Sau đó chọn **Continue** và sử dụng **FaceID/TouchID/Passcode** (*theo yêu cầu của thiết bị*) để hoàn tất quá trình đăng ký.



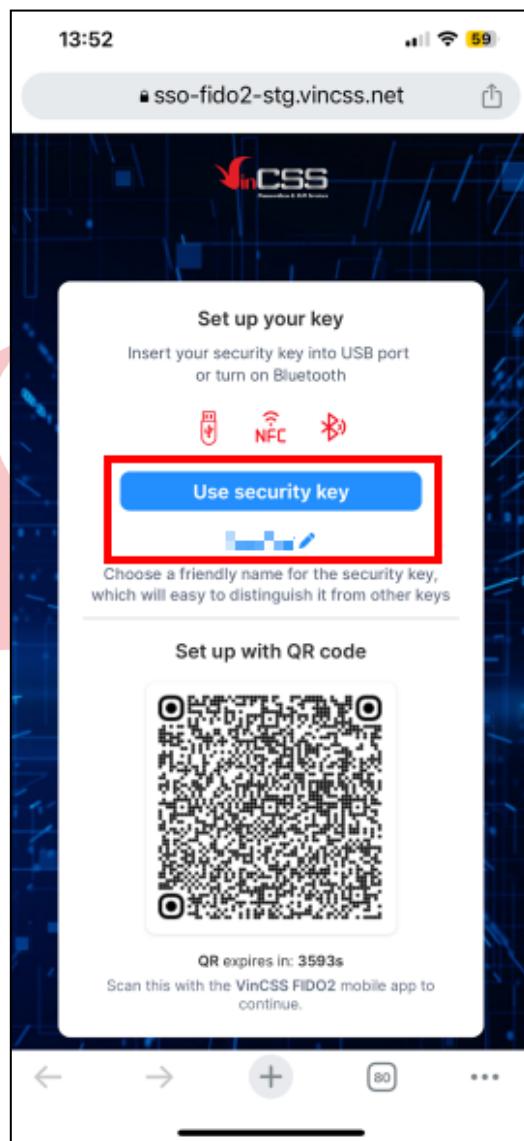
- **Đối với thiết bị Android:** Nhấn vào link đăng ký khoá bảo mật rồi đổi tên khoá bảo mật, chọn **Use security key**. Sau đó chọn **Continue** và sử dụng **phương thức mở khoá màn hình** (theo yêu cầu của thiết bị) để hoàn tất quá trình đăng ký.



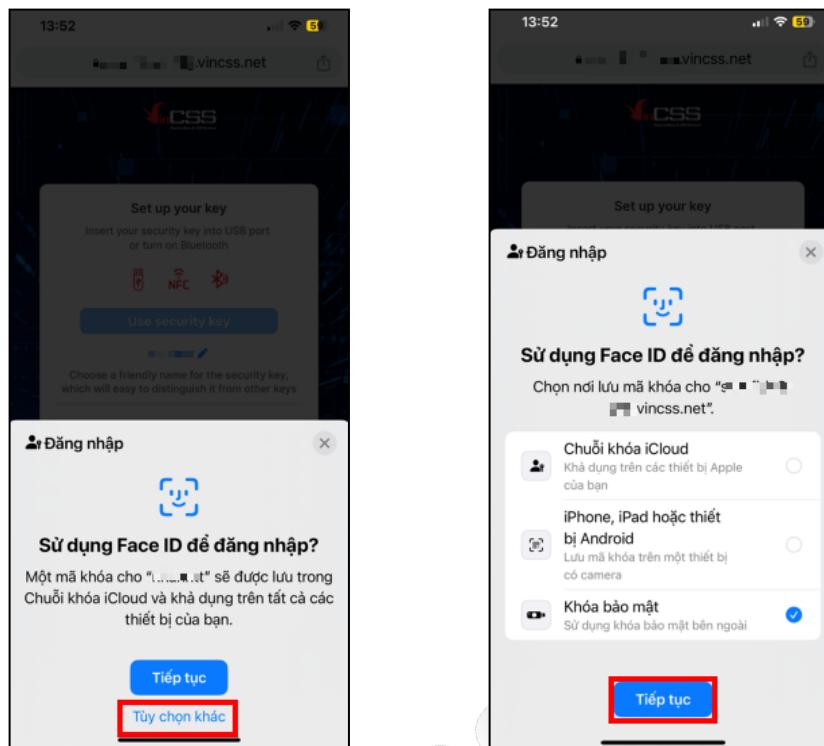
I.2.2. Đăng ký khoá bảo mật sử dụng VinCSS FIDO2® Touch 1/ VinCSS FIDO2® Fingerprint hoặc các khoá bảo mật có tính năng tương tự

Lưu ý: Hiện tại khoá bảo mật vật lý chỉ hỗ trợ đăng ký usernameless trên hệ điều hành iOS. Với hệ điều hành Android, sử dụng khoá bảo mật vật lý chỉ được hỗ trợ khi đăng ký passwordless.

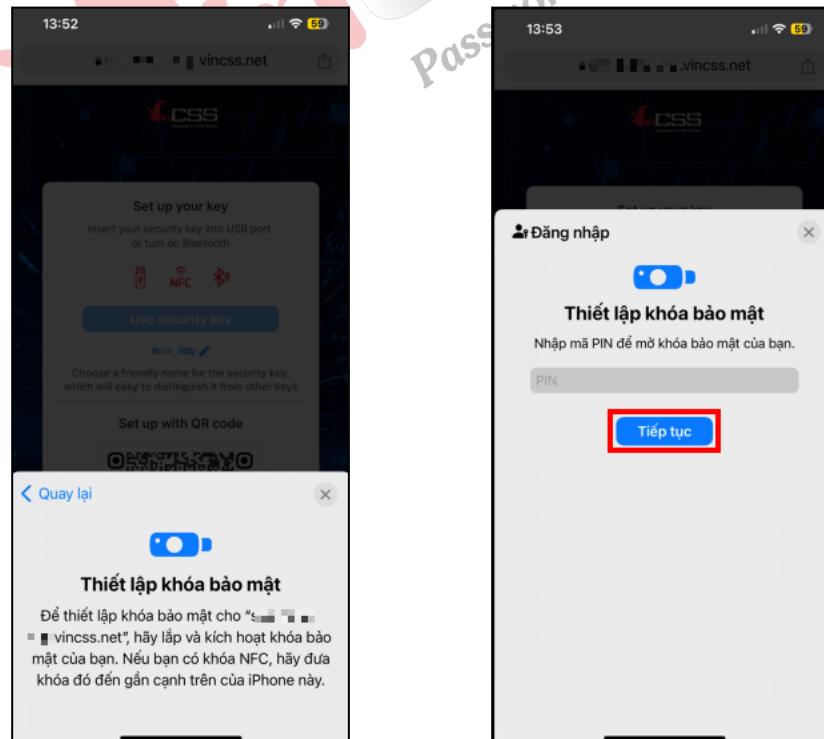
- Sau khi nhấn vào đường link, người dùng sẽ được chuyển hướng đến trang đăng ký khoá bảo mật. Trên giao diện đăng ký khoá bảo mật, điền tên khóa bảo mật sau đó chọn “**Use security key**”.



- Chọn **Tùy chọn khác > Khoá bảo mật > Tiếp tục** để lựa chọn hình thức đăng ký bằng khoá bảo mật vật lý.



- Kết nối trực tiếp khoá bảo mật với thiết bị thông qua **cổng USB/NFC (NFC chỉ hỗ trợ đối với khoá bảo mật VinCSS FIDO2® Fingerprint)**, sau đó xác nhận bằng mã PIN của khoá bảo mật. Sau đó nhấn **Tiếp tục**.



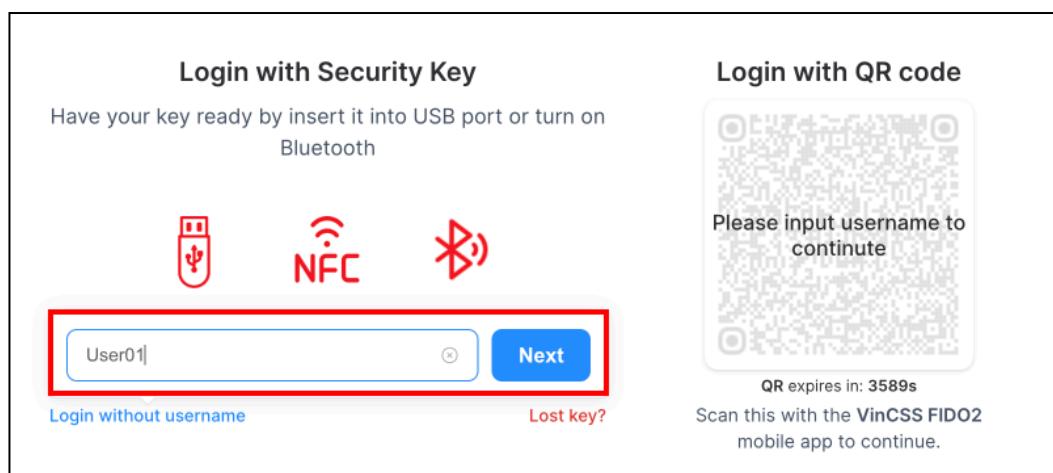
II. ĐĂNG NHẬP VÀO HỆ THỐNG

Người dùng truy cập **Account Portal**. Tại mục này, người dùng có hai hình thức đăng nhập: **Login with username** và **Login without username**.

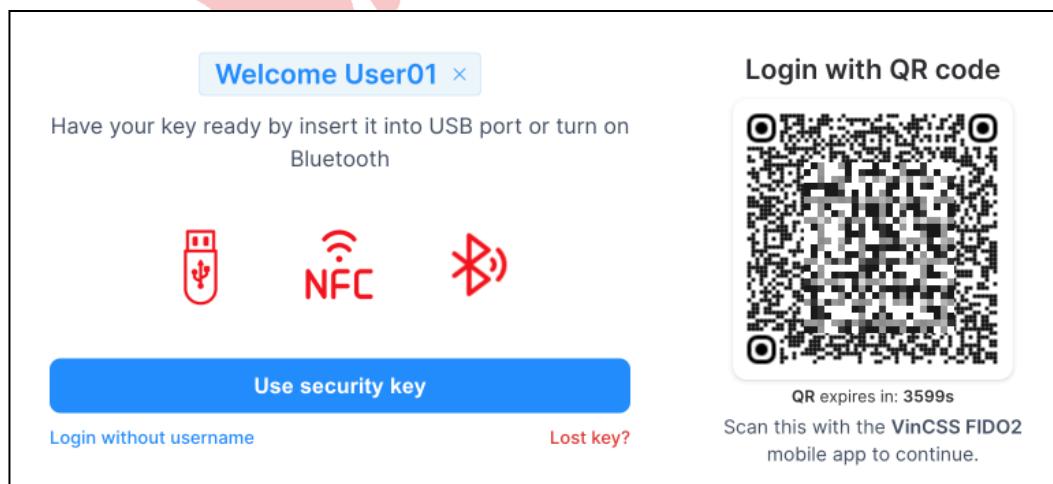
Lưu ý: Việc đăng nhập bằng hình thức nào phụ thuộc vào cách thức đăng ký khoá bảo mật được hướng dẫn tại mục **III. ĐĂNG KÝ THÊM KHOÁ BẢO MẬT MỚI**.

- Login with username

- Chọn “**Login with username**”. Nhập thông tin **username** (*không phân biệt chữ hoa, chữ thường*), sau đó chọn **Next**.

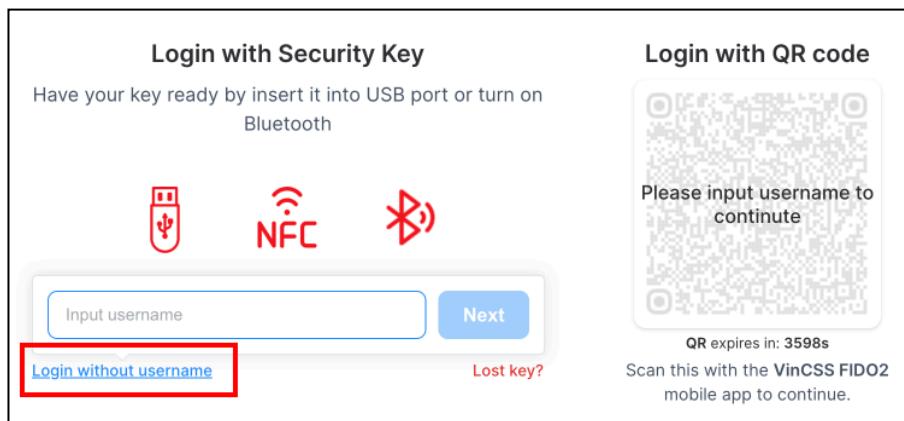


- Giao diện đăng nhập sẽ được hiển thị như hình bên dưới.

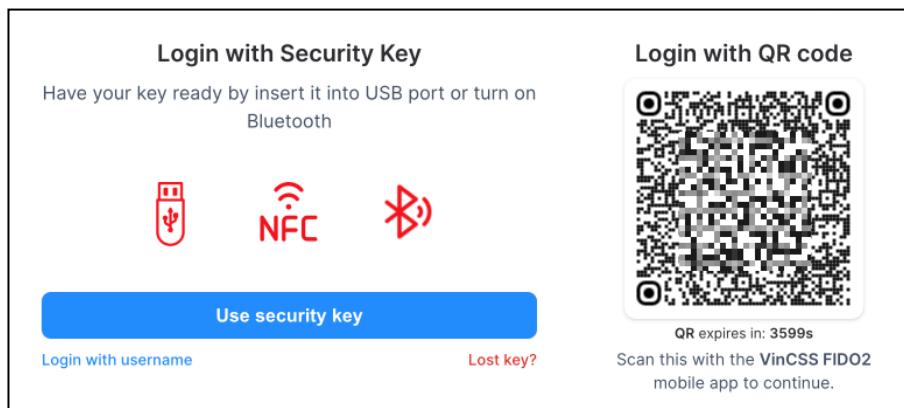


- Login without username

- Hoặc người dùng có thể chọn hình thức đăng nhập khác bằng cách chọn “**Login without username**” để thay cho bước nhập **username**.



- Giao diện sẽ được hiện ra theo hình bên dưới.



Lưu ý: Từ bước này trở đi, các bước thực hiện ở hình thức “Login with username” tương tự như “Login without username”.

II.1. Truy cập trên máy tính

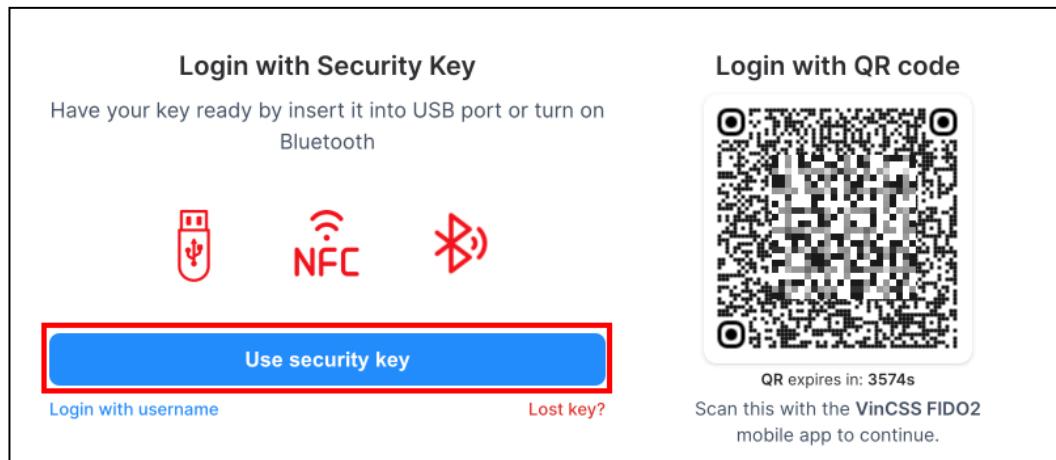
Lưu ý: Các bước thực hiện để đăng ký khoá bảo mật sử dụng khoá vật lý/khoá mềm/passkey trên máy tính sử dụng hệ điều hành Windows, Linux và macOS tương tự nhau. Dưới đây là hướng dẫn minh họa các bước thực hiện trên hệ điều hành Windows.

II.1.1. Đăng nhập bằng khoá bảo mật sử dụng khoá vật lý

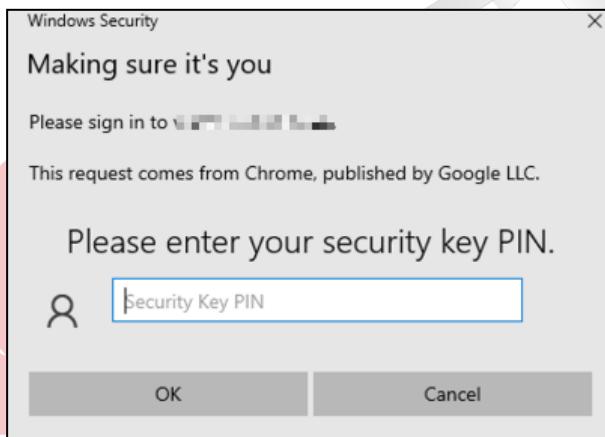
II.1.1.1. Đăng nhập bằng cách sử dụng VinCSS FIDO2® Touch 1 hoặc các khoá bảo mật có tính năng tương tự

Khoá bảo mật đã được đăng ký trước đó (Tham khảo mục [I.1.1.1. Đăng ký khoá bảo mật sử dụng VinCSS FIDO2® Touch 1 hoặc các khoá bảo mật có tính năng tương tự](#)).

- Kết nối khóa bảo mật với máy tính, trên giao diện đăng nhập chọn “**Use security key**”.



- Nhập mã PIN của khoá bảo mật và nhấn **OK**.



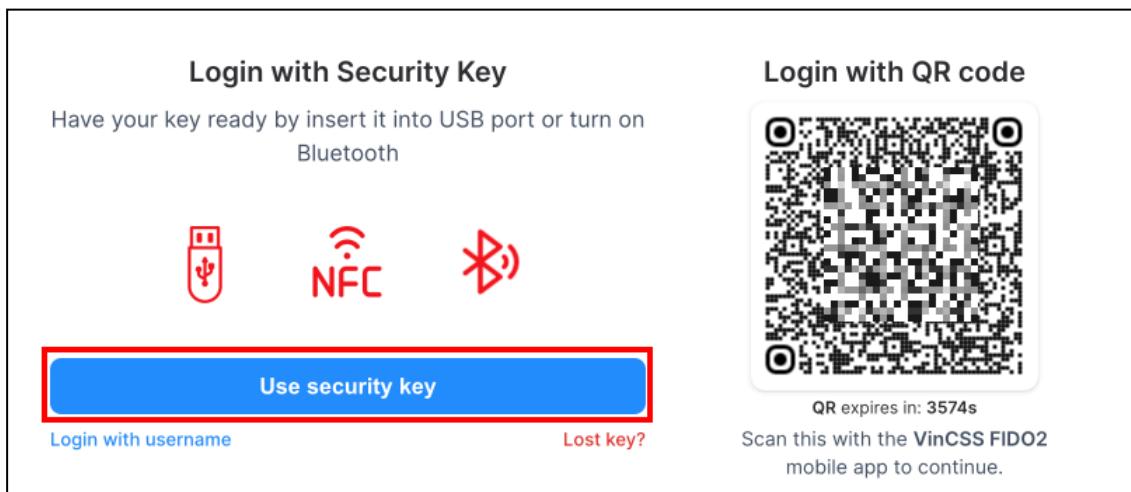
- Chạm vào logo màu vàng trên khóa bảo mật để tiếp tục. Hệ thống sẽ hiển thị thông báo khi người dùng đăng nhập thành công.



II.1.1.2. Đăng nhập bằng cách sử dụng VinCSS FIDO2® Fingerprint hoặc các khoá bảo mật có tính năng tương tự

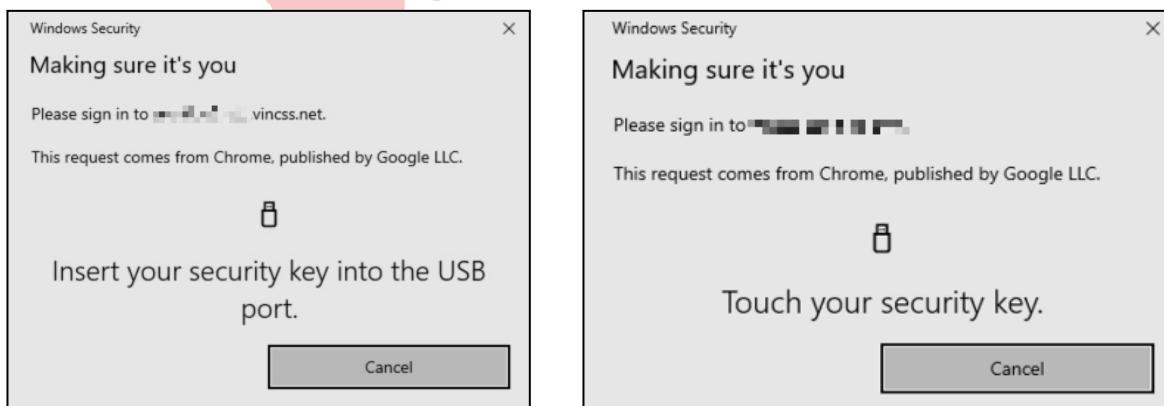
Khoá bảo mật VinCSS FIDO2® Fingerprint đã được đăng ký trước đó (Tham khảo mục [I.1.1.2. Đăng ký khoá bảo mật sử dụng VinCSS FIDO2® Fingerprint hoặc các khoá bảo mật có hỗ trợ sinh trắc học](#)).

- Trên giao diện đăng nhập, chọn “Use security key”.



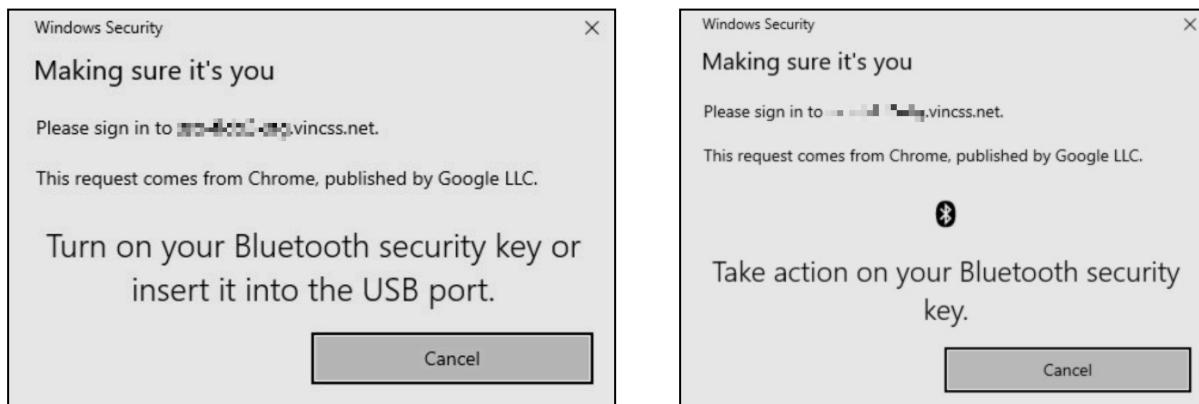
II.1.1.2.1. Sử dụng kết nối USB

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



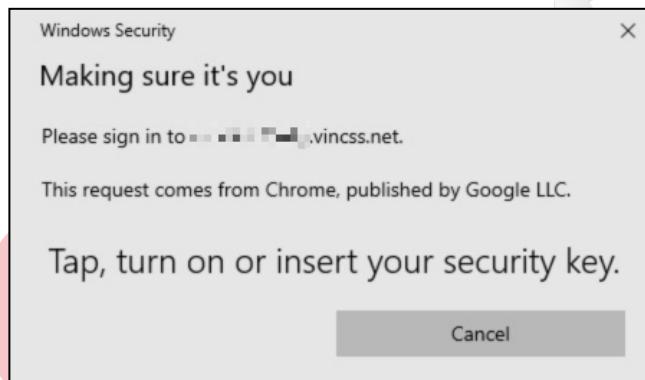
II.1.1.2.2. Sử dụng kết nối Bluetooth

- Kết nối khoá bảo mật với máy tính thông qua kết nối Bluetooth. Quét vân tay trên khoá bảo mật khi nhận được thông báo.

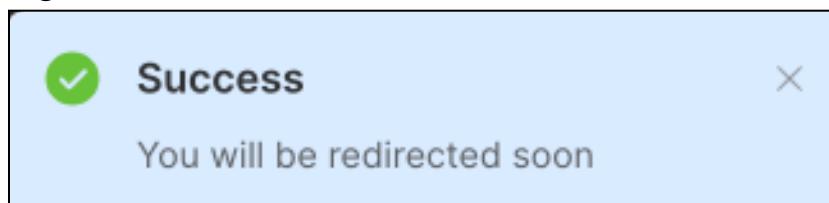


II.1.1.2.3. Sử dụng kết nối NFC

- 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.



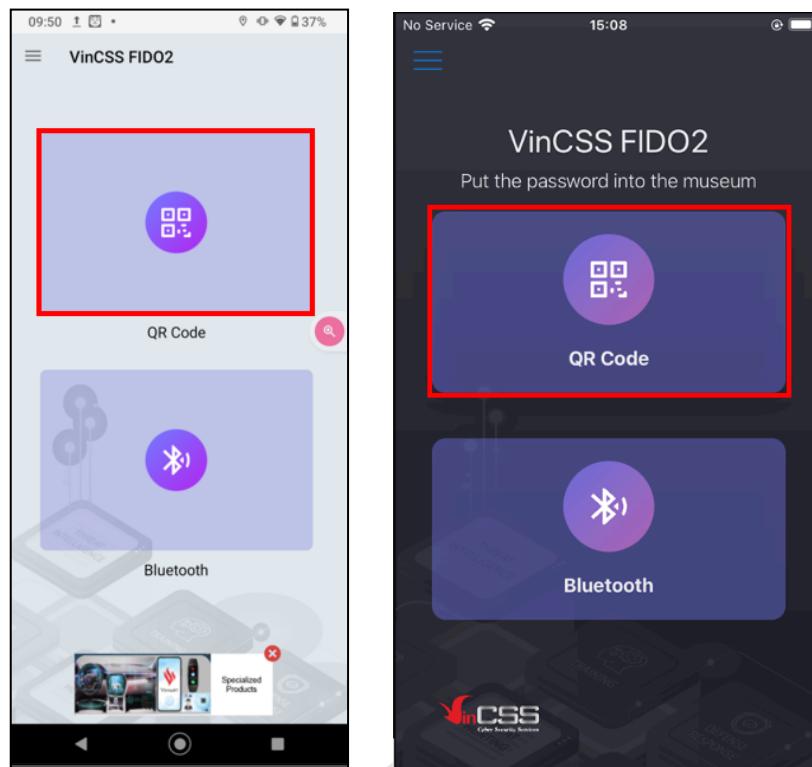
- Xác thực trên khoá bảo mật thành công, hệ thống hiển thị thông báo đăng nhập thành công như hình dưới.



II.1.2. Đăng nhập bằng ứng dụng VinCSS FIDO2

Ứng dụng VinCSS FIDO2 đã được đăng ký khoá bảo mật trước đó (Tham khảo mục [I.1.2. Đăng ký khoá bảo mật sử dụng khoá mềm với ứng dụng VinCSS FIDO2](#)).

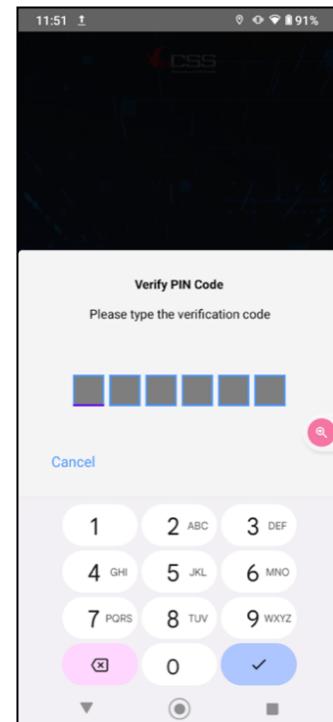
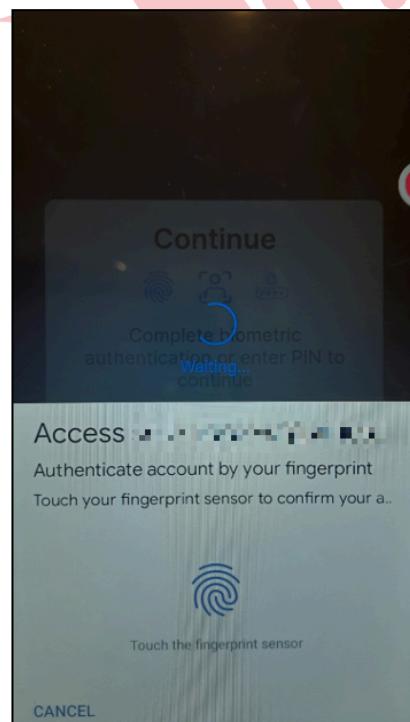
- Trên giao diện ứng dụng VinCSS FIDO2, chọn **QR code**. Sau đó tiến hành quét mã QR trên giao diện đăng nhập.



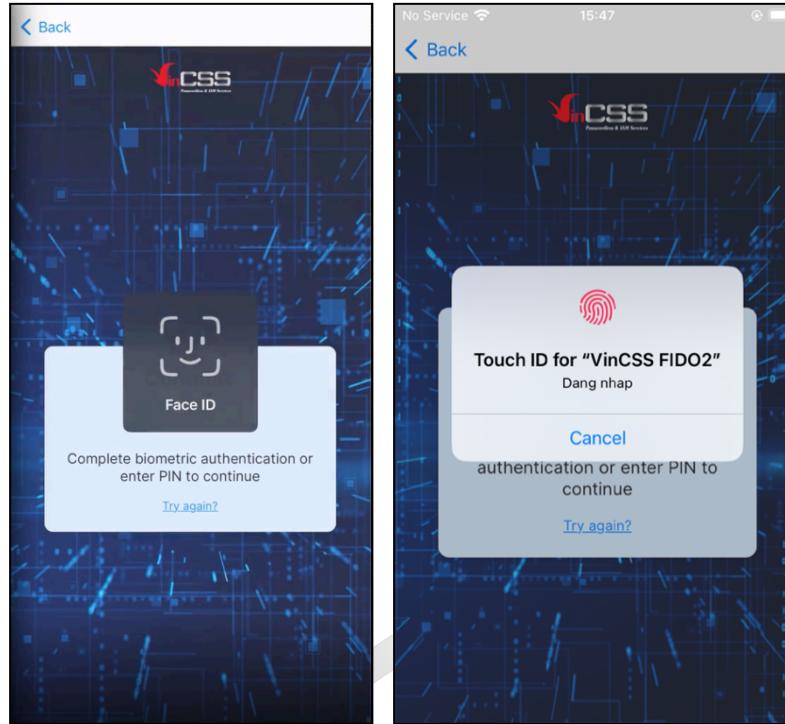
Android

iOS

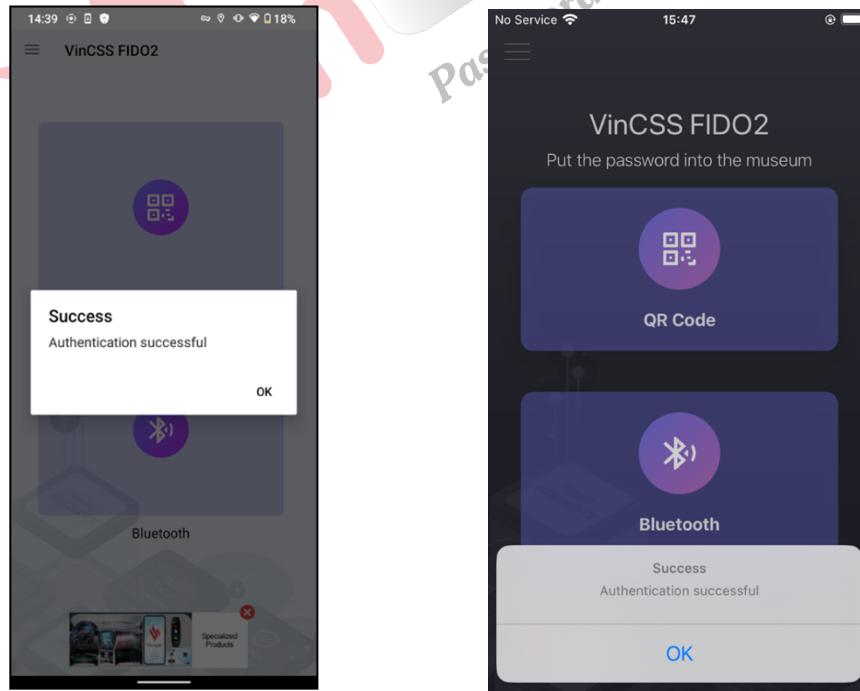
- Đối với hệ điều hành Android: Xác nhận bằng sinh trắc học hoặc nhập mã PIN (*theo yêu cầu của thiết bị*).



- Đối với hệ điều hành iOS: chọn **Login** sau đó xác nhận **FaceID/TouchID** trên điện thoại (*theo yêu cầu của thiết bị*).



- Trên màn hình điện thoại hiển thị thông tin xác thực thành công.

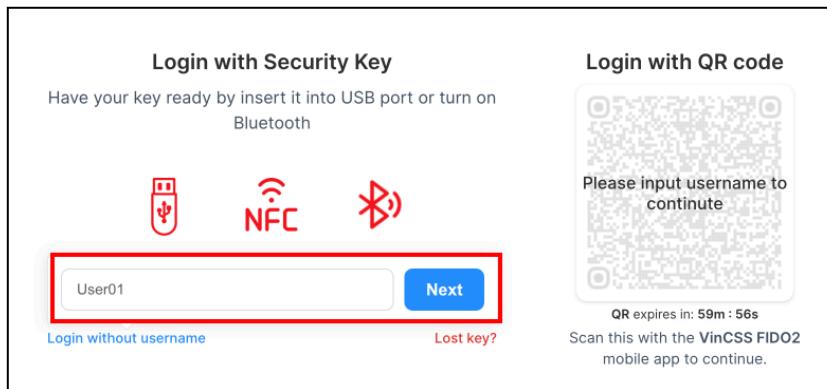


Android

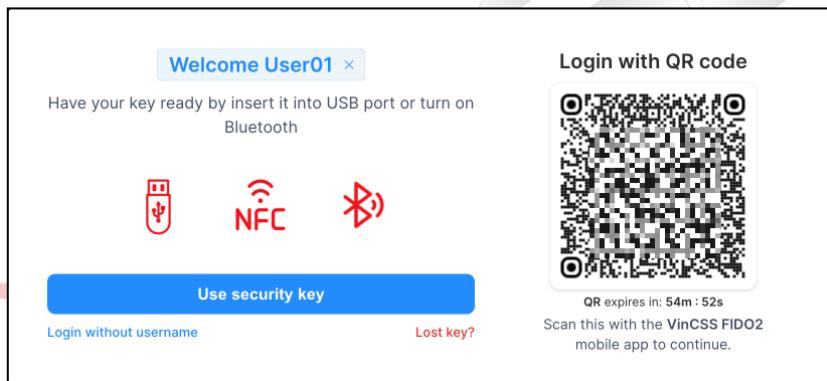
iOS

II.1.3. Đăng nhập hệ thống bằng passkey

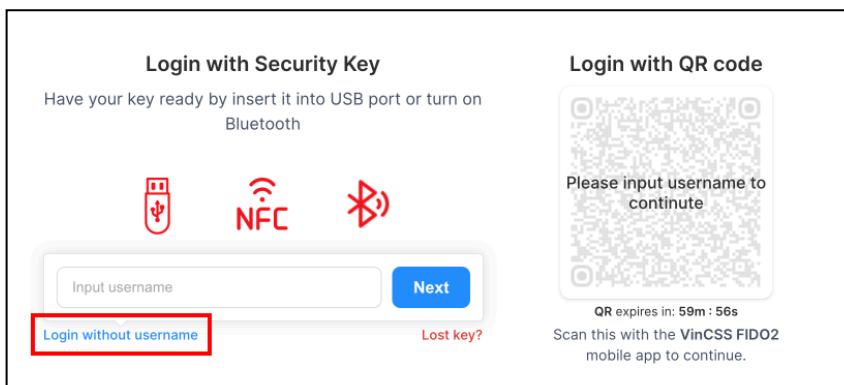
- **Xác thực không mật khẩu**
 - o Điền thông tin **username** (*không phân biệt chữ hoa, chữ thường*), sau đó chọn **Next**.



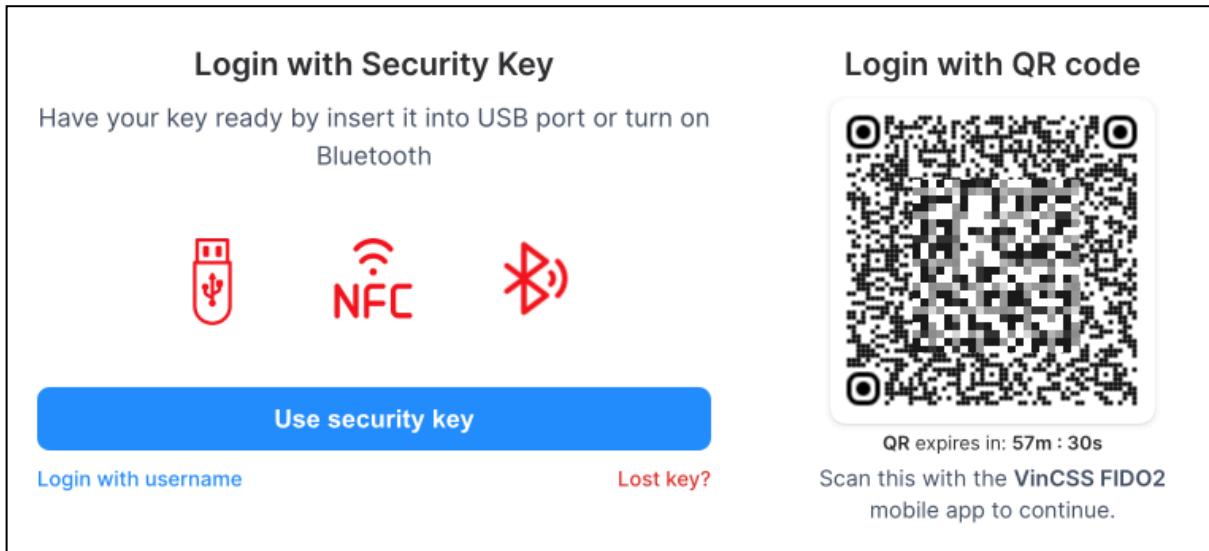
- o Giao diện đăng nhập sẽ hiển thị như hình dưới.



- **Xác thực không tên người dùng**
 - o Hoặc trong trường hợp khoá được khởi tạo với tùy chọn sử dụng xác thực không tên người dùng, người dùng có thể chọn **Login without username** để thay cho bước nhập **username**.



- Giao diện đăng nhập sẽ hiển thị như hình dưới.

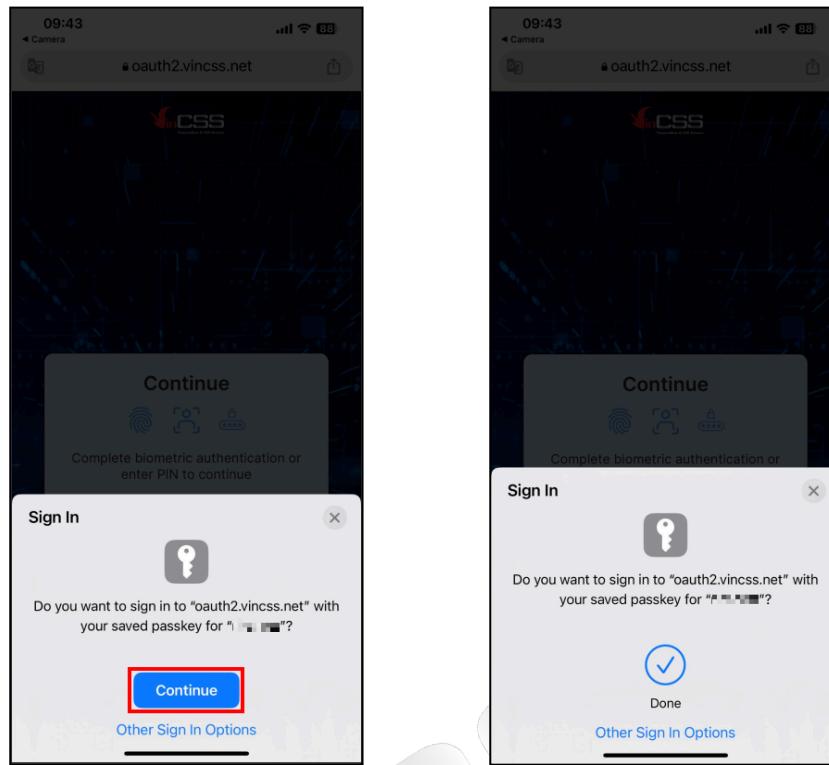


- Hoặc người dùng có thể đăng nhập bằng passkey theo hình thức khác bằng cách nhấn **Use security key** trên giao diện đăng nhập. Sau đó chọn **Use a phone or table**. Một mã QR sẽ hiện ra.

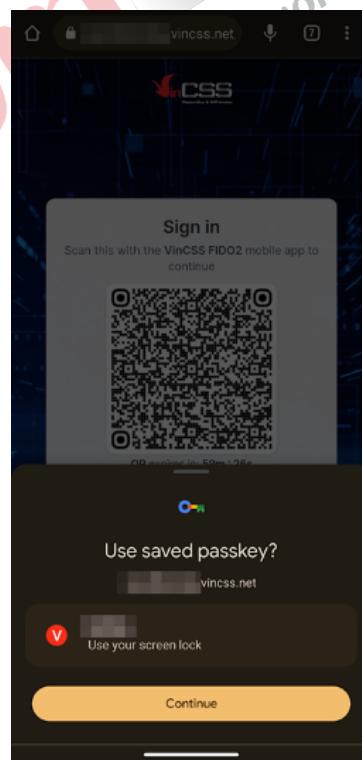


II.1.3.1. Passkey trên điện thoại thông minh

- Đối với **thiết bị iOS**: Mở phần quét mã QR/Camera trên điện thoại, sau đó tiến hành quét mã QR trên màn hình máy tính. Chọn **Continue**, sau đó xác thực bằng FaceID/TouchID (*theo yêu cầu của thiết bị*).



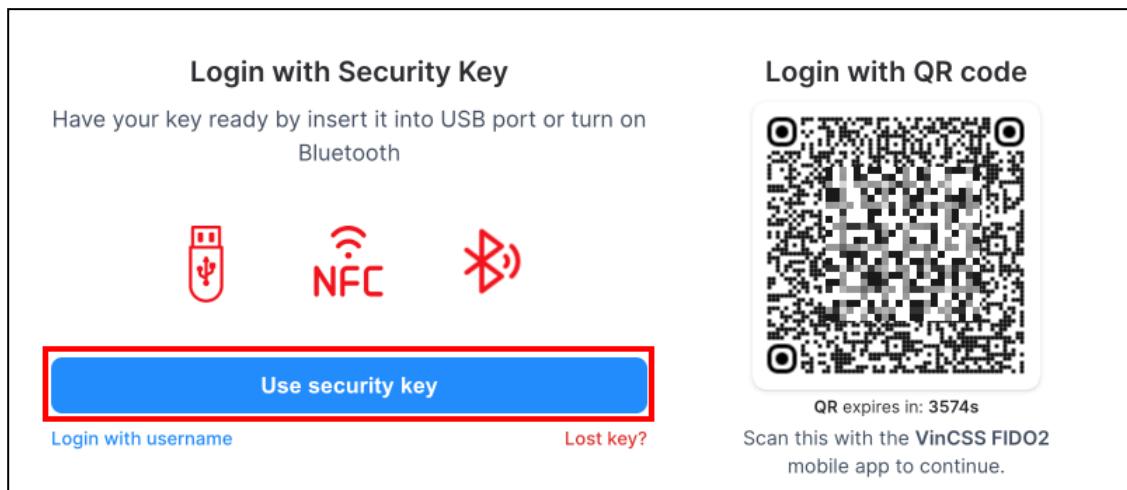
- Đối với **thiết bị Android**: Mở phần quét mã QR/Camera trên điện thoại, sau đó tiến hành quét mã QR trên màn hình máy tính. Chọn **Continue**, sau đó xác thực bằng phương thức mở khoá màn hình (*theo yêu cầu của thiết bị*).



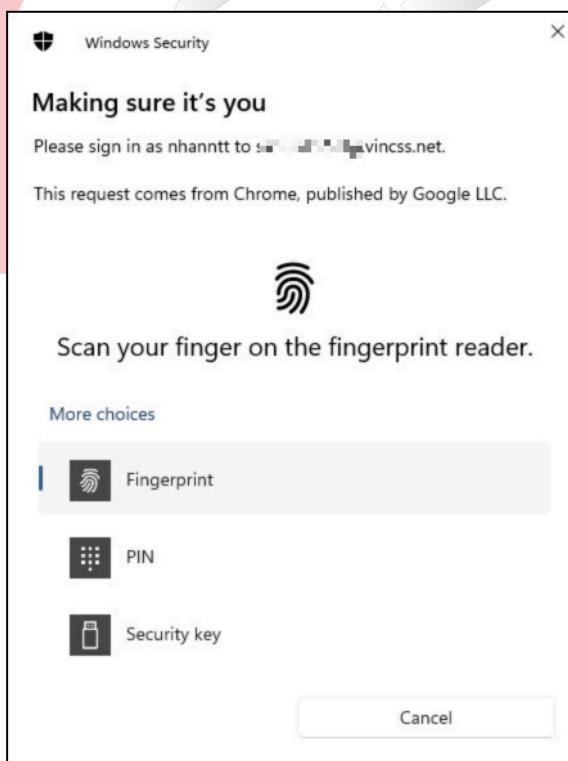
II.1.3.2. Passkey trên máy tính

II.1.3.2.1. Windows

- Trên giao diện đăng nhập, chọn **Use security key**.



- Sau đó chọn **Windows Hello or external security key** để tiếp tục. Lựa chọn hình thức xác thực bằng **Fingerprint/PIN** để hoàn tất việc đăng ký.

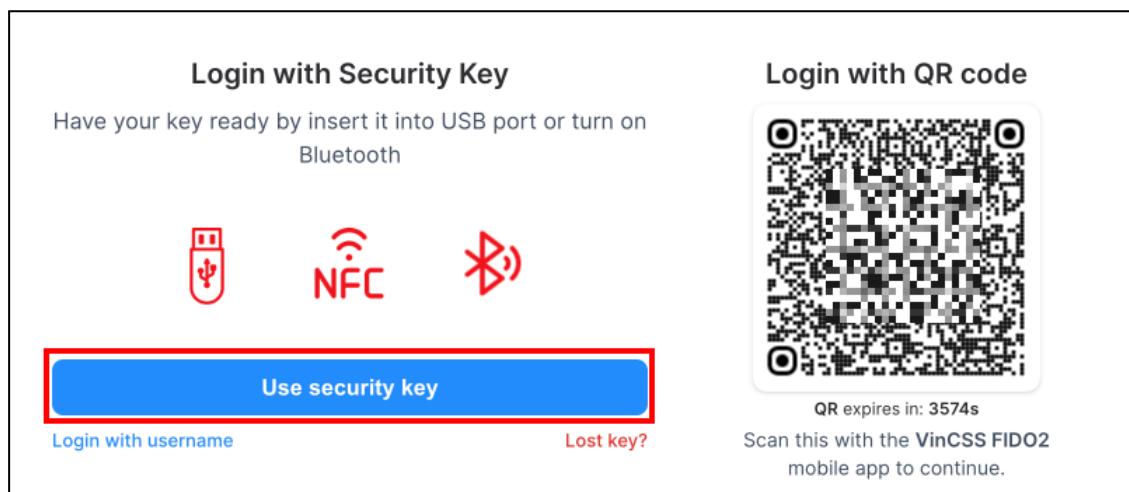


Lưu ý: Đối với phương thức xác thực **Security key**, người dùng vui lòng tham khảo mục [I.I.1.](#))

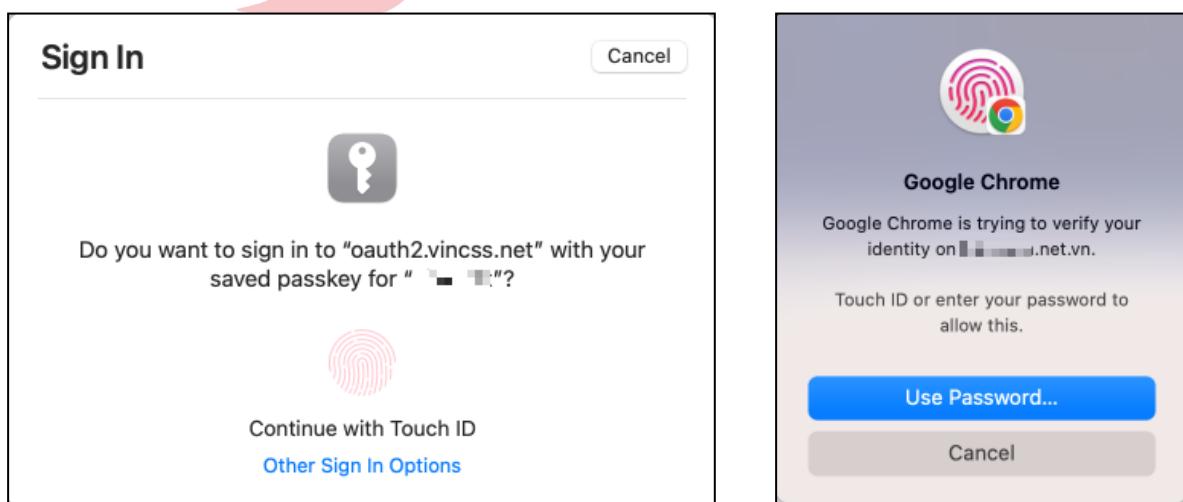
II.1.3.2.2. macOS

Lưu ý: Ngoài ra, người dùng có thể sử dụng passkey để xác thực trực tiếp tại máy tính thông qua trình duyệt **Safari** (macOS Ventura trở lên - đã được đăng ký đồng bộ keychain trước đó) hoặc **Chrome** (đối với tất cả các hệ điều hành cho phép sử dụng passkey trên trình duyệt này và đã được đăng ký trước đó) theo các bước sau.

- Truy cập link đăng ký đã được gửi bởi quản trị viên bằng trình duyệt **Safari/Chrome**, sau đó đổi tên khoá bảo mật.



- Chọn **Use security key**, sau đó xác thực bằng **TouchID/Password** (tùy theo yêu cầu của thiết bị) để hoàn tất quá trình đăng nhập.

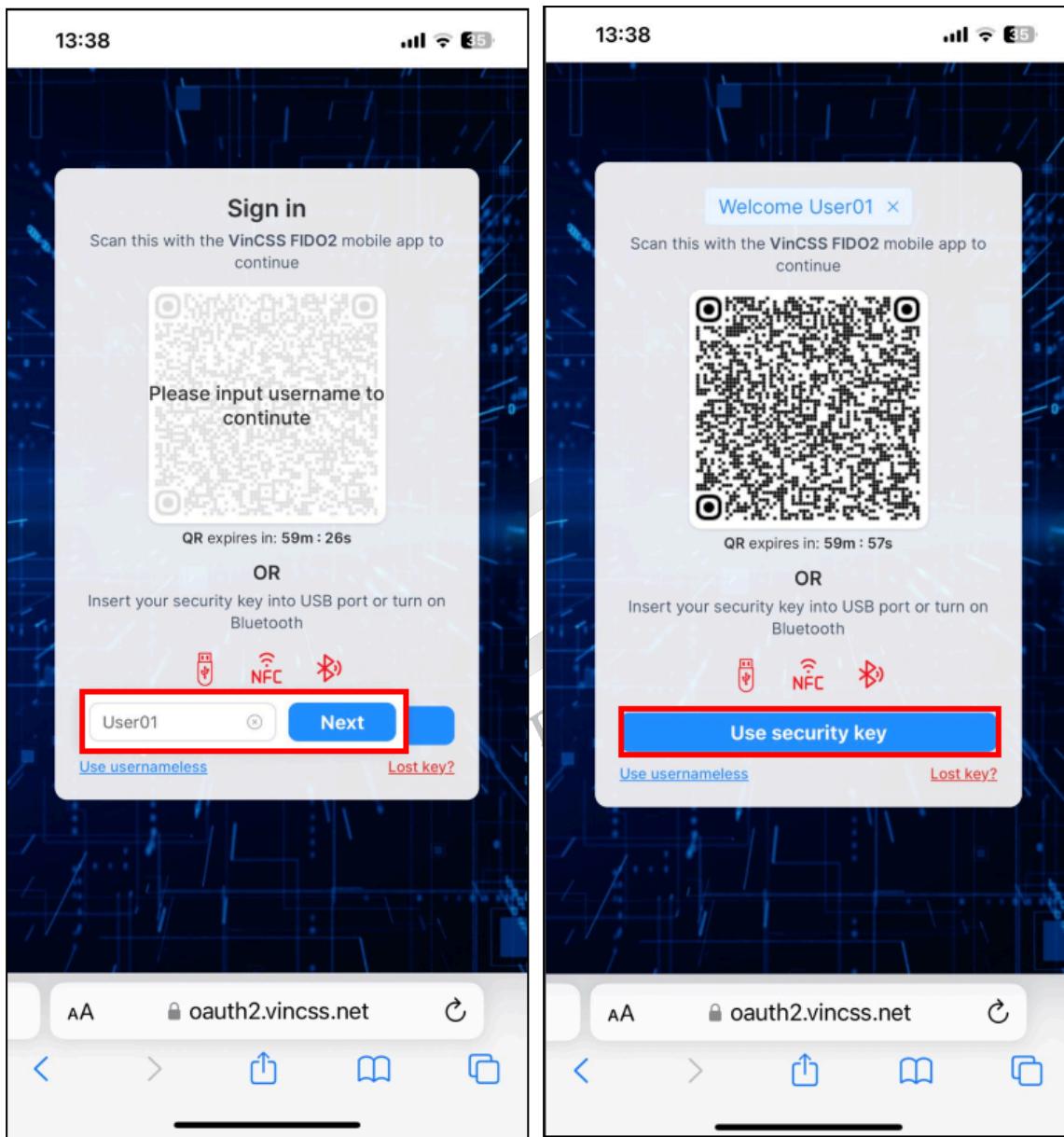


Safari

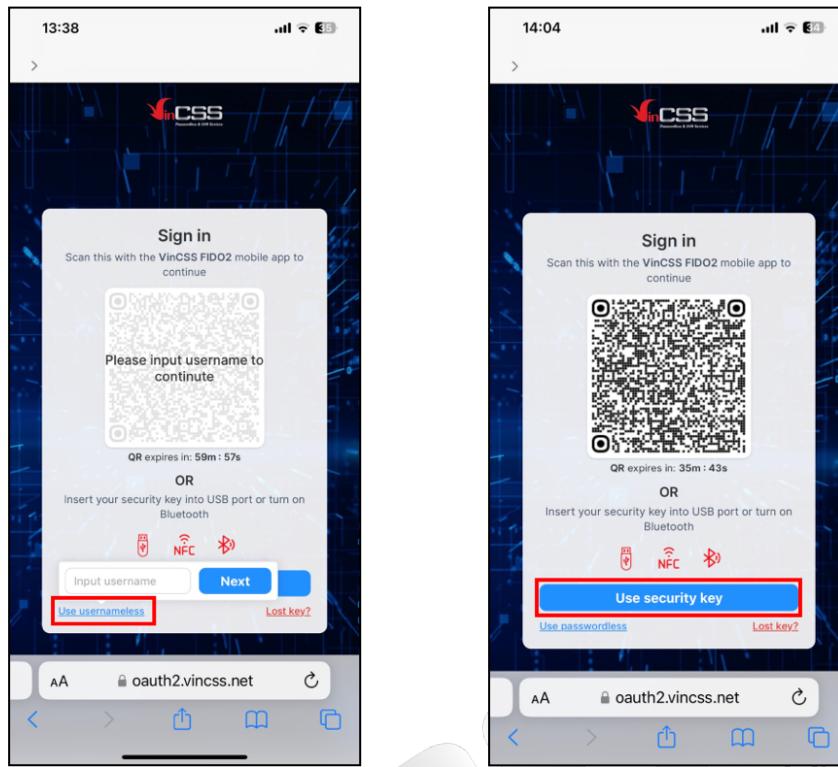
Chrome

II.2. Truy cập bằng điện thoại thông minh

- Xác thực không mật khẩu
 - o Điền thông tin **username** (*không phân biệt chữ hoa, chữ thường*), sau đó chọn **Next**. Chọn **Use Security Key** để tiếp tục.

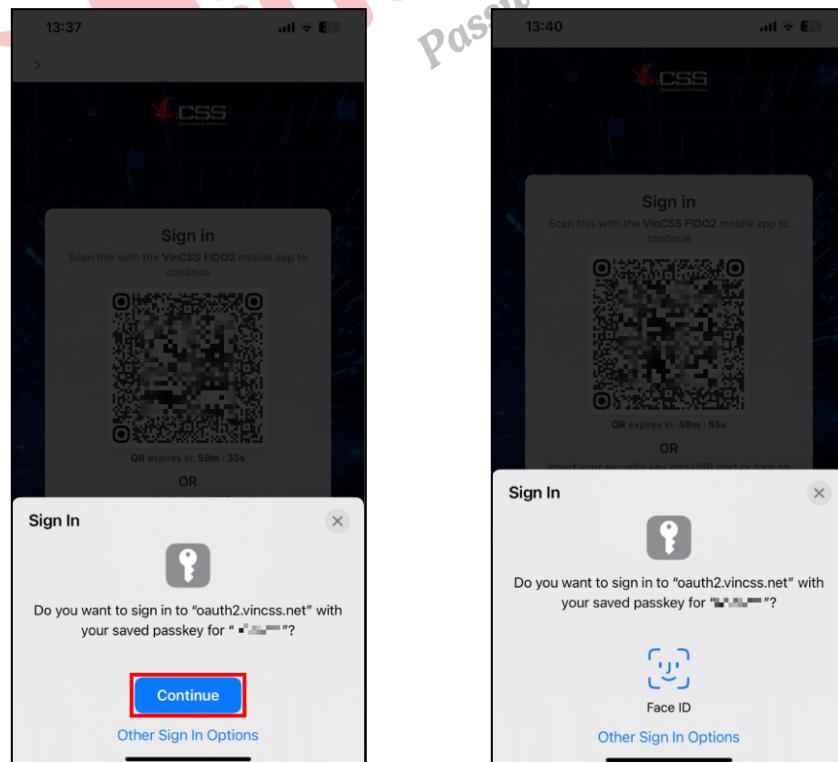


- Xác thực không tên người dùng
 - o Hoặc trong trường hợp khoá được khởi tạo với tùy chọn sử dụng xác thực không tên người dùng, người dùng có thể chọn **Use Usernameless** để thay cho bước nhập **username**. Sau đó chọn **Use Security Key** để tiếp tục.

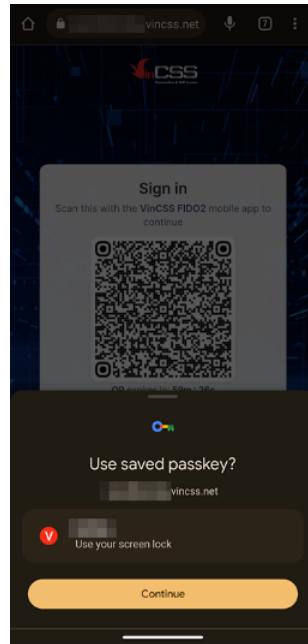


II.2.1. Đăng nhập bằng passkey trên thiết bị

- Đối với thiết bị iOS: Chọn Continue, sau đó xác thực bằng FaceID/TouchID (theo yêu cầu của thiết bị).

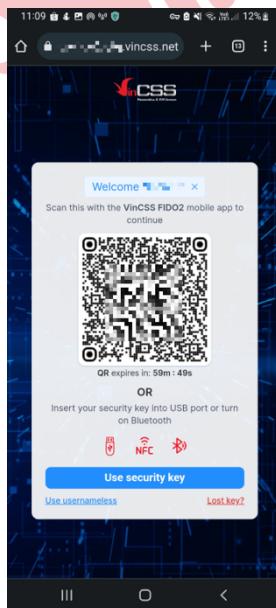


- Đối với **thiết bị Android**: Chọn **Continue**, sau đó xác thực bằng **phương thức mở khoá màn hình** (*theo yêu cầu của thiết bị*).

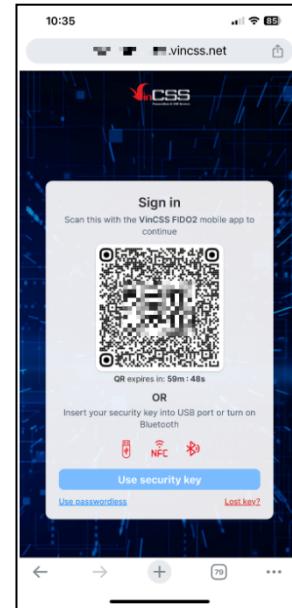


II.2.2. Đăng nhập bằng khoá bảo mật vật lý VinCSS FIDO2® Touch 1/ VinCSS FIDO2® Fingerprint hoặc các khoá bảo mật có tính năng tương tự

- Trên giao diện đăng nhập, chọn “**Use security key**”.



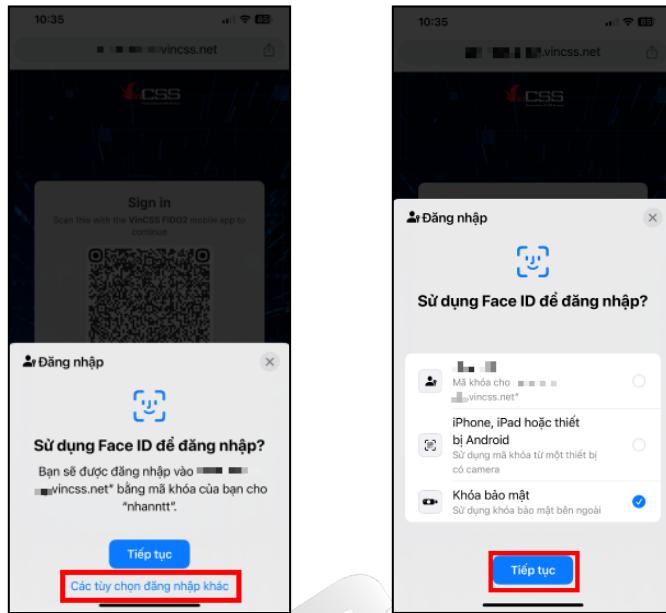
Android



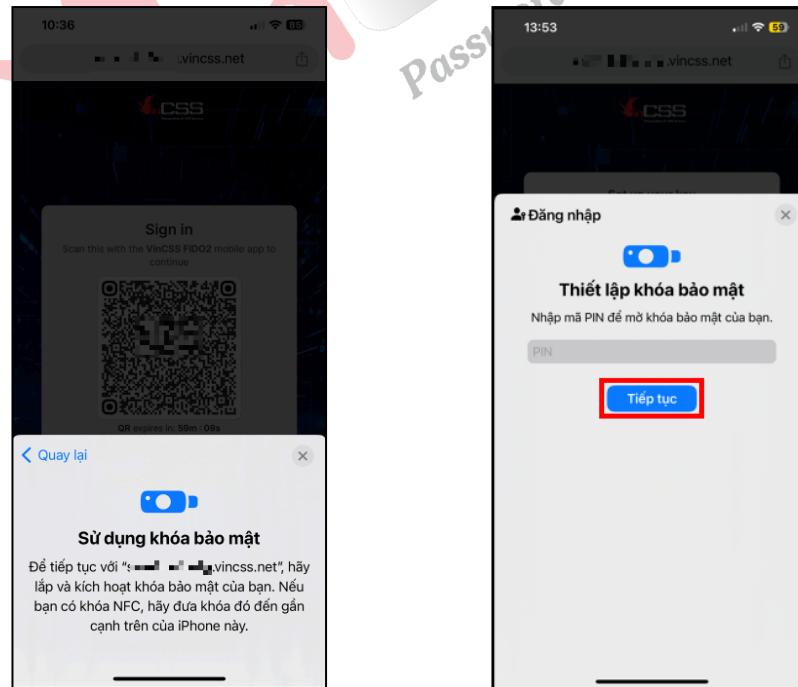
iOS

- Đối với iOS:

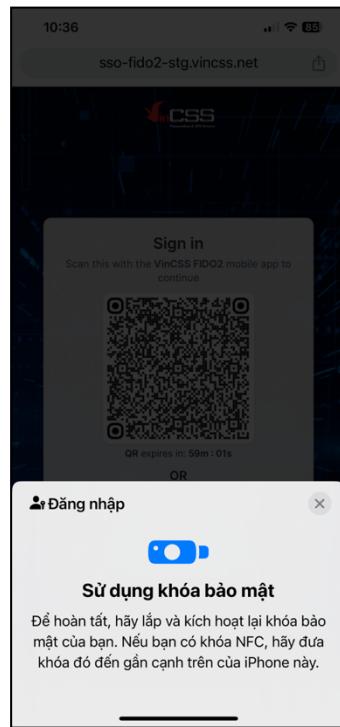
- o Chọn **Các tùy chọn đăng nhập khác > Khoá bảo mật > Tiếp tục** để lựa chọn hình thức đăng nhập bằng khoá bảo mật vật lý.



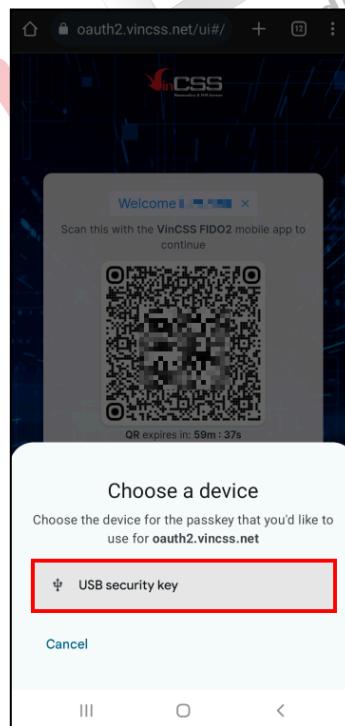
- o Kết nối trực tiếp khoá bảo mật với thiết bị thông qua **cổng USB/NFC**, xác nhận bằng **mã PIN/vân tay** của khoá bảo mật. Sau đó nhấn **Tiếp tục**.



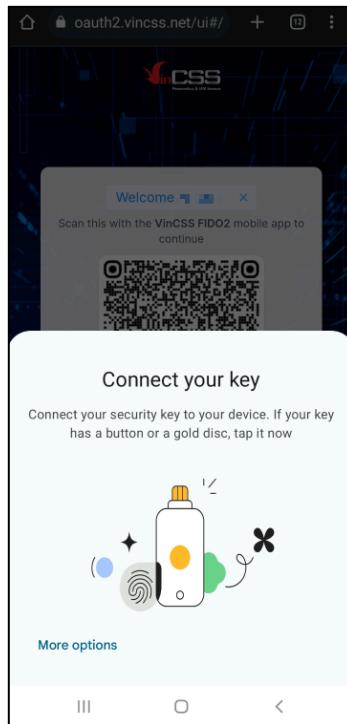
- o Xác thực lại bằng **mã PIN/vân tay** để hoàn tất.



- Đối với Android:
 - o Chọn **USB Security key** để lựa chọn hình thức đăng nhập bằng khoá bảo mật vật lý.

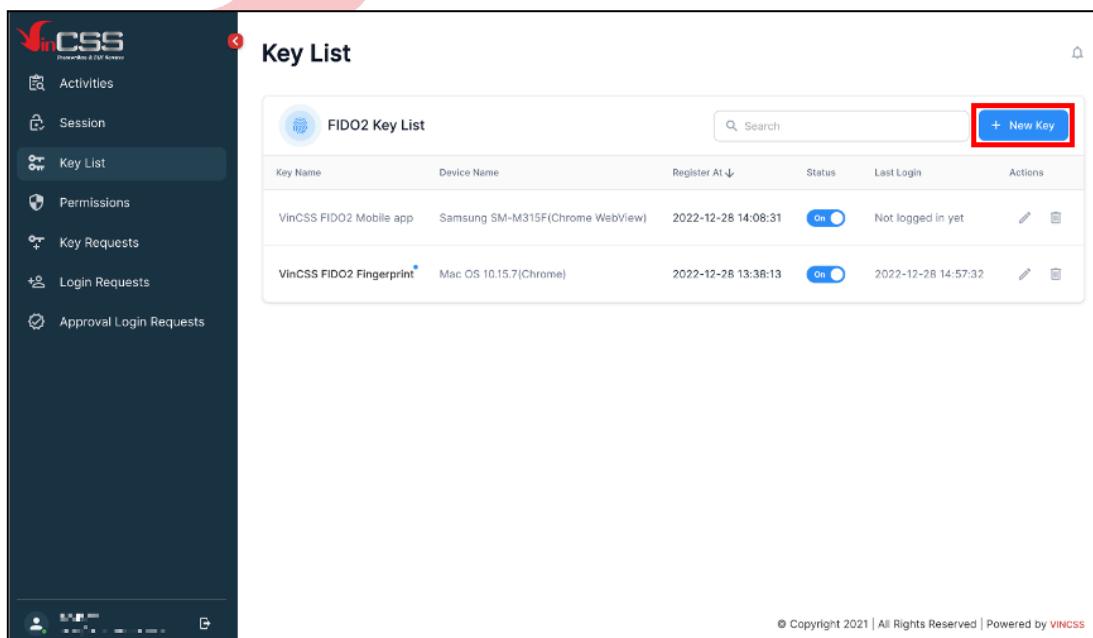


- Kết nối trực tiếp khoá bảo mật với thiết bị thông qua **cổng USB/NFC/Bluetooth**, xác nhận người dùng. Sau đó nhấn **Tiếp tục**.

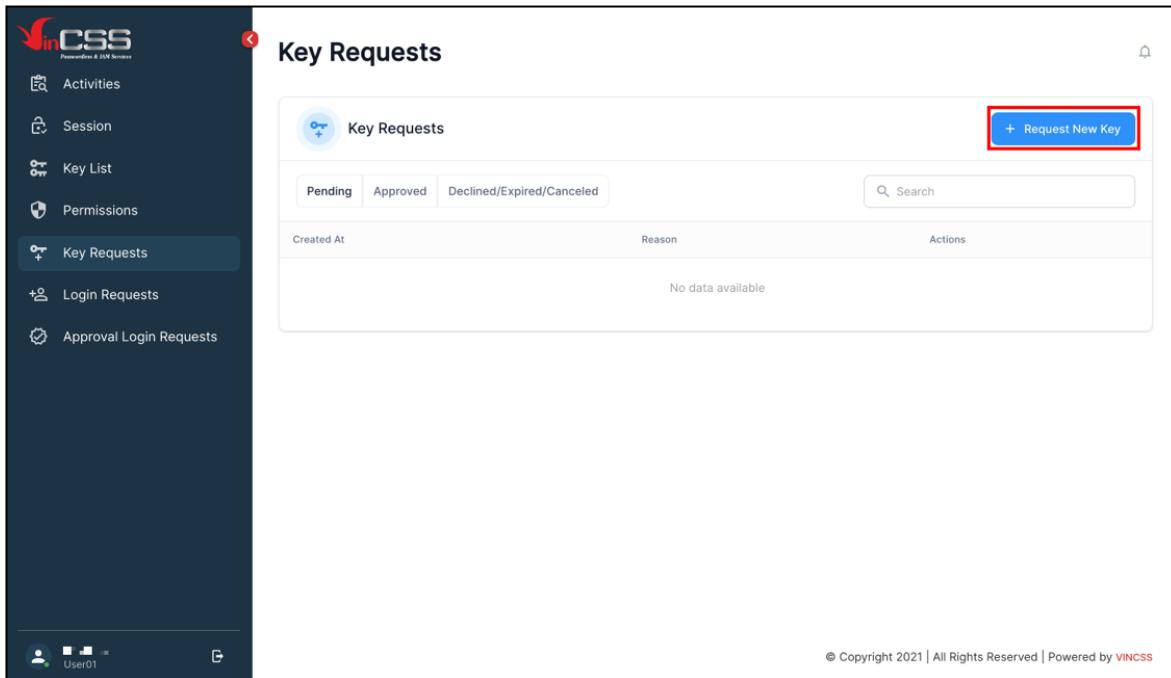


III. ĐĂNG KÝ THÊM KHOÁ BẢO MẬT MỚI

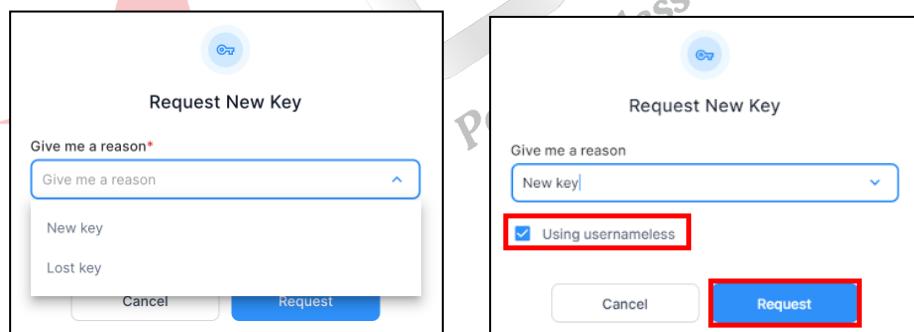
- Trên giao diện Account Portal, chọn **Key List > New Key** để đăng ký thêm khoá bảo mật mới.

A screenshot of the VinCSS Account Portal. On the left, a sidebar menu includes "Activities", "Session", "Key List" (which is selected and highlighted in blue), "Permissions", "Key Requests", "Login Requests", and "Approval Login Requests". The main content area is titled "Key List" and contains a table titled "FIDO2 Key List". The table has columns for "Key Name", "Device Name", "Register At", "Status", "Last Login", and "Actions". Two entries are listed: "VinCSS FIDO2 Mobile app" (Device Name: Samsung SM-M315F(Chrome WebView)) and "VinCSS FIDO2 Fingerprint" (Device Name: Mac OS 10.15.7(Chrome)). A red box highlights the "New Key" button located at the top right of the table header. At the bottom of the page, a copyright notice reads "© Copyright 2021 | All Rights Reserved | Powered by VINCSS".

- Hoặc có thể đăng ký khoá bảo mật mới bằng cách chọn **Key Request** trên giao diện **Account Portal**. Sau đó chọn **Request New Key**



- Nhập lý do thêm khoá bảo mật mới sau đó chọn **Request**.



The image displays two side-by-side screenshots of a 'Request New Key' dialog box. Both screenshots show a dropdown menu under the 'Give me a reason*' input field, with 'New key' selected. The right screenshot has a red box around the 'Using usernameless' checkbox, which is checked. Both screenshots have a red box around the 'Request' button at the bottom right.

- o Nếu chọn “**Using usernameless**”, người dùng có thể đăng nhập hệ thống bằng cả 2 hình thức “**Login with username**” và “**Login without username**”.
- o Nếu không chọn “**Using usernameless**”, người dùng chỉ có thể đăng nhập hệ thống bằng hình thức “**Login with username**”
- Các bước thao tác đăng ký khoá bảo mật mới, người dùng thực hiện như hướng dẫn tại mục “**I. KHỞI TẠO TÀI KHOẢN VÀ ĐĂNG KÝ KHOÁ BẢO MẬT**”.