Hướng dẫn sử dụng khóa bảo mật VinCSS FIDO2® Fingerprint

Giới thiệu

Khóa bảo mật VinCSS FIDO2® Fingerprint là khóa xác thực đã được chứng nhận FIDO2. FIDO2 cung cấp phương thức xác thực không cần mật khẩu để xác thực người dùng và giải quyết các vấn đề liên quan đến sự bảo mật, sự thuận tiện, quyền riêng tư và khả năng mở rộng mà mật khẩu không làm được. Số lượng tài khoản có thể đăng ký với khóa bảo mật VinCSS FIDO2® Fingerprint là không giới hạn trong trường hợp dùng khoá để xác thực hai lớp, và giới hạn 50 tài khoản trong trường hợp dùng khoá để xác thực không mật khẩu.

Khoá bảo mật VinCSS FIDO2® Fingerprint không phải là USB lưu trữ nên không có nguy cơ lây nhiễm mã độc. Khóa bảo mật chỉ có chức năng xác thực cho người dùng, không lưu trữ thêm bất kỳ thông tin nào khác, đảm bảo tính riêng tư.

Khoá bảo mật VinCSS FIDO2® Fingerprint yêu cầu người dùng tương tác trực tiếp vào khoá nên không thể bị tấn công từ xa, khoá áp dụng chuẩn FIDO2 nên bảo vệ người dùng khỏi các cuộc tấn công lừa đảo (phishing) trên internet, tấn công xen giữa (man-in-the-middle attack), tấn công sao chép thông tin bí mật (skimming)... Phần cứng khóa được thiết kế để bảo vệ các dữ liệu trong khóa xác thực, ngăn chặn việc các dữ liệu này bị đọc trộm.

USB, BLE và NFC là ba phương thức kết nối đã được tích hợp tại khóa bảo mật VinCSS FIDO2® Fingerprint. Người dùng có thể thực hiện kết nối khoá bảo mật trên bất kỳ thiết bị được hỗ trợ kết nối không dây nào, chẳng hạn như máy tính để bàn, máy tính xách tay, máy tính bảng hoặc điện thoại thông minh và hoàn thành xác thực FIDO2® an toàn.

Sơ đồ

Khóa bảo mật VinCSS FIDO2® Fingerprint

Ý nghĩa các đèn tín hiệu

Tín hiệu	Ý nghĩa	Trạng thái
Nháy đỏ 3 lần liên tiếp ●●● ●●●	Pin tích của khoác gần cạn, cần kết nối sạc	Sử dụng Bluetooth hoặc NFC
Sáng màu hổ phách	Khóa bảo mật đang được sạc	Kết nối USB
Sáng màu xanh lá	Khóa bảo mật đã sạc đầy	Kết nối USB
Sáng màu xanh dương	Chế độ Bluetooth được bật, khoá đã được kết nối với một thiết bị Bluetooth	Sử dụng Bluetooth
Nháy xanh dương liên tục ●●●	Khoá bảo mật vào chế độ ghép nối	Sử dụng Bluetooth
Sáng màu tím	NFC được kích hoạt	Sử dụng NFC
Nháy trắng nhanh, liên tục ○○○	Khoá bảo mật đang trong quá trình xử lý và yêu cầu người dùng tương tác	Yêu cầu người dùng xác thực bằng vân tay
Sáng màu trắng/ Nháy trắng chậm ▭ / ○ ○	Khoá bảo mật đang trong quá trình xử lý và yêu cầu người dùng tương tác	Yêu cầu người dùng xác nhận bằng việc chạm vào khoá bảo mật

Trạng thái kết nối

Thao tác	Trạng thái ban đầu	Cách thực hiện	Trạng thái sau	Lưu ý
Bật kết nối Bluetooth	Khóa bảo mật ở trạng thái nghỉ (không kết nối USB, LED tắt)	Chạm giữ cảm biến vân tay trong 5 giây	LED sáng màu xanh dương	Cần đảm bảo dung lượng pin của khóa bảo mật còn đủ để sử dụng. Nếu LED nháy đỏ, vui lòng cắm sạc trước khi sử dụng.
Chuyển chế độ ghép đôi	Khóa bảo mật đang ở trạng thái bật Bluetooth	Chạm giữ cảm biến vân tay trong 5 giây	LED nháy xanh dương	
Tắt kết nối không dây	Khóa bảo mật đang bật Bluetooth/ NFC	Chạm đúp cảm biến vân tay	LED tắt	

Lưu ý: *Khóa bảo mật sẽ tự động kết nối với thiết bị nếu khóa bảo mật đã được kết nối trước đó.*

Kết nối với máy tính

Lưu ý:

- *Pin sẽ được để ở chế độ nghỉ để duy trì thời gian chờ của pin được lâu hơn. Đối với lần đầu tiên sử dụng, người dùng cần phải kết nối trực tiếp khoá bảo mật vào máy tính thông qua dây USB type C.*

- *Hiện tại hệ điều hành macOS mới chỉ hỗ trợ sử dụng khoá bảo mật VinCSS FIDO2® Fingerprint thông qua hình thức kết nối USB, chưa hỗ trợ người dùng sử dụng thông qua hình thức kết nối BLE và NFC. (Tuy nhiên vẫn có thể sử dụng kết nối Bluetooth/NFC trên khóa bảo mật nếu ứng dụng có hỗ trợ xác thực FIDO2 thông qua kết nối Bluetooth/NFC).*

- *Hệ điều hành Windows hỗ trợ sử dụng cả 3 hình thức kết nối khoá bảo mật qua USB, Bluetooth và NFC (cần có phần cứng hỗ trợ).*

Sử dụng qua kết nối USB

- Tiến hành kết nối khoá bảo mật VinCSS FIDO2® Fingerprint vào máy tính thông qua dây USB type C, đảm bảo rằng khoá bảo mật đang không trong chế độ Bluetooth/NFC.

Sử dụng qua kết nối NFC

- Đặt khóa bảo mật VinCSS FIDO2® Fingerprint lên đầu đọc NFC của thiết bị. Khi đèn LED màu tím, có thể sử dụng tính năng NFC.
- Để ngắt kết nối NFC, nhấc khoá bảo mật ra khỏi đầu đọc NFC. Ngắt kết nối thành công, đèn LED màu tím sẽ bị tắt.

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.*

Sử dụng qua kết nối BLE

- Kích hoạt chế độ Bluetooth của khóa bảo mật.
- Bật kết nối Bluetooth của thiết bị cần sử dụng khóa, sau đó kết nối với khoá bảo mật có tên **V-FIDO2**.
- Nhập mã ghép đôi để kết nối.

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 gồm 6 chữ số cuối được lấy tại 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 Bluetooth thành công, đèn LED hiển thị màu xanh dương.

Lưu ý: *Do thay đổi trong chính sách hiển thị thiết bị Bluetooth trên Windows 11, máy tính có thể không tìm thấy khóa bảo mật. Khi đó, vui lòng thực hiện thay đổi cài đặt như hướng dẫn dưới đây:*
-Mở Cài đặt -> Bluetooth & devices -> Devices -> Device settings.
-Ở mục Bluetooth devices discovery, chọn Advanced.

Kết nối khoá bảo mật

o Bước đầu tiên sau khi kết nối khóa bảo mật là thiết lập mã PIN và Vân tay của khóa bảo mật, có các công cụ hỗ trợ có sẵn có thể được sử dụng để thiết lập khóa bảo mật được liệt kê dưới đây:

	Trình quản lý khóa bảo mật tích hợp trong Windows	Trình quản lý khóa bảo mật tích hợp trong Chrome
Chức năng	- Thiết lập/thay đổi mã PIN của khóa bảo mật - Thêm/Xoá vân tay - Đặt lại khóa bảo mật	- Thiết lập/thay đổi mã PIN của khóa bảo mật - Thêm/Xoá vân tay - Đặt lại khóa bảo mật - Quản lý dữ liệu đăng nhập
Thực hiện	“Cài đặt” => “Tài khoản” => “Tuỳ chọn đăng nhập” => “Khoá bảo mật”	“Cài đặt” => “Quyền riêng tư và bảo mật” => “Bảo mật” => “Quản lý khoá bảo mật”

Lưu ý: *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.*

Bảng chuyển đổi hình thức kết nối

Lưu ý: *Vui lòng cập nhật liên tục hệ điều hành/ phần mềm mới nhất để đạt được khả năng tương thích tối đa.*

BẢNG CHUYỂN ĐỔI HÌNH THỨC KẾT NỐI

	Google Chrome / Microsoft Edge / Firefox					
	U2F			FIDO2		
	USB	BLT	NFC	USB	BLT	NFC
macOS Hỗ trợ phiên bản macOS 10.15 trở lên	✓	✗	✗	✓	✗	✗
iOS Hỗ trợ phiên bản iOS 13.3 trở lên (NFC được hỗ trợ từ iphone 7 trở lên)	✓	✗	✓	✓	✗	✓
Hỗ trợ phiên bản Windows 8.1trở lên	✓	✓	✓	✓	✓	✓
Hỗ trợ phiên bản Android 9.0 trở lên	✓	✗	✓	✓	✗	✓

CHROME	Hỗ trợ phiên bản 100.0.4896 trở lên
EDGE	Hỗ trợ phiên bản 93 trở lên
FIREFOX	Hỗ trợ phiên bản 92 trở lên
SAFARI	Hỗ trợ phiên bản 13 trở lên

✓	Hỗ trợ
✗	Không hỗ trợ
U2F	Xác thực đa yếu tố
FIDO2	Xác thực không mật khẩu

BẢNG CHUYỂN ĐỔI HÌNH THỨC KẾT NỐI

	Safari					
	U2F			FIDO2		
	USB	BLT	NFC	USB	BLT	NFC
macOS Hỗ trợ phiên bản macOS 10.15 trở lên	✓	✗	✗	✓	✗	✗
iOS Hỗ trợ phiên bản iOS 13.3 trở lên (NFC được hỗ trợ từ iphone 7 trở lên)	✓	✗	✓	✓	✗	✓

CHROME	Hỗ trợ phiên bản 100.0.4896 trở lên
EDGE	Hỗ trợ phiên bản 93 trở lên
FIREFOX	Hỗ trợ phiên bản 92 trở lên
SAFARI	Hỗ trợ phiên bản 13 trở lên

✓	Hỗ trợ
✗	Không hỗ trợ
U2F	Xác thực đa yếu tố
FIDO2	Xác thực không mật khẩu

CHUẨN BỊ KHÓA BẢO MẬT VỚI CÁC DỊCH VỤ WEB

Bước đầu tiên của việc sử dụng xác thực FIDO là đăng ký khóa bảo mật cho tài khoản của bạn. Để đăng ký khoá bảo mật cho tài khoản của bạn, vui lòng làm theo các bước dưới đây:

Bước 1: Đăng nhập tài khoản như bình thường với máy tính và trình duyệt được hỗ trợ WebAuthn.

Bước 2: Truy cập phần cài đặt tài khoản - phương thức đăng nhập – Thêm khóa bảo mật.

Bước 3: Kết nối khóa bảo mật với thiết bị bằng 1 trong 3 phương thức: USB, BLE hoặc NFC và thực hiện theo các thông báo hướng dẫn được hiển thị trên màn hình.

Lưu ý: *Tham khảo bảng chuyển đổi hình thức kết nối bên trên để lựa chọn phù hợp nhất với thiết bị của bạn.*

Bước 4: Xác thực vân tay/Chạm vào phần cảm biến để chứng minh sự hiện diện của người dùng khi đèn báo xác thực nhấp nháy. Quá trình đăng ký sẽ được hoàn tất trong giây lát.

XÁC THỰC KHOÁ BẢO MẬT VỚI CÁC DỊCH VỤ WEB

Sau khi đăng ký, người dùng có thể đăng nhập tài khoản của mình bằng hình thức xác thực không mật khẩu hoặc các bước xác thực tài khoản khác.

- Đối với hình thức **xác thực không mật khẩu**, người dùng có thể nhấp vào "**Đăng nhập với khóa bảo mật**" trong cửa sổ đăng nhập, sau đó làm theo hướng dẫn xác thực được hiển thị trên màn hình.

- Đối với hình thức **xác thực hai bước**, người dùng phải nhập xác thực bằng tên người dùng và mật khẩu như bình thường, sau đó cửa sổ xác minh hai bước sẽ bật lên, người dùng làm theo hướng dẫn được hiển thị trên màn hình để hoàn tất xác thực.

Câu hỏi thường gặp

Q: **Phải làm gì khi bị mất khóa bảo mật VinCSS FIDO2® Fingerprint?**

A: Trong trường hợp bị mất khoá bảo mật VinCSS FIDO2® Fingerprint, bạn có thể dùng các phương thức dự phòng đã đăng ký trong quá trình cài đặt đăng ký dùng khoá lần đầu để đăng nhập vào tài khoản, và huỷ liên kết với khoá đã bị mất. Các phương thức dự phòng có thể là mã khôi phục dùng một lần, SMS OTP hoặc các ứng dụng Authenticator trên thiết bị di động.

Q: **Trường hợp bị mất khóa xác thực VinCSS FIDO2® Fingerprint, người dùng có bị mất tài khoản không?**

A: Khi bị mất khóa bảo mật VinCSS FIDO2® Fingerprint thì người dùng sẽ không bị mất tài khoản, vì trên khóa bảo mật VinCSS FIDO2® Fingerprint không chứa toàn bộ thông tin cần thiết cho việc đăng nhập.

Q: **Hiện nay có các dịch vụ nào hỗ trợ xác thực bằng khóa VinCSS FIDO2® Fingerprint?**

A: Hầu hết các dịch vụ trực tuyến hiện nay đều hỗ trợ xác thực bằng khoá xác thực VinCSS FIDO2® Fingerprint, ví dụ:

- Tài khoản Microsoft (Outlook, Office, Skype, OneDrive, Xbox Live, Bing...)
- Tài khoản Google (Drive, Google Cloud, Hangout, Gmail, Play, YouTube...)
- AWS Web Service
- Facebook
- GitHub
- Dropbox
- Salesforce
- Gitlab
- Jira

Câu hỏi thường gặp

Q: **Khi tôi dùng khóa xác thực VinCSS FIDO2® Fingerprint có tăng nguy cơ lây nhiễm mã độc (malware) giữa các máy tính không, vì tôi thường xuyên cắm khóa VinCSS FIDO2® Authenticator từ nhiều máy tính khác nhau?**

A: Không, vì VinCSS FIDO2® Fingerprint không phải là USB lưu trữ nên không có nguy cơ lây nhiễm mã độc.

Q: **Làm thế nào để tôi có thể biết pin đã được sạc đầy?**

A: Khi cắm cáp USB, quá trình sạc sẽ bắt đầu ngay lập tức. 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.

Q: **Khách hàng mua sản phẩm VinCSS FIDO2® Fingerprint sẽ được bảo hành ở đâu?**

A: Khách hàng mua khoá bảo mật VinCSS FIDO2® Fingerprint có thể gửi bảo hành sản phẩm thông qua đại lý phân phối, hoặc gửi bảo hành trực tiếp tại trung tâm VinCSS tại Hà Nội và Thành phố Hồ Chí Minh.

Q: **Dùng khóa VinCSS FIDO2® Fingerprint có ảnh hưởng đến chính sách phải đổi mật khẩu trong vòng 90 ngày đang áp dụng hầu hết tại các công ty hiện nay không?**

A: Khóa xác thực VinCSS FIDO2® Fingerprint được thiết kế không kết nối với dịch vụ lưu trữ mật khẩu tập trung, nên chính sách đổi mật khẩu không ảnh hưởng đến khóa VinCSS FIDO2® Fingerprint.

THÔNG SỐ KỸ THUẬT

Khóa bảo mật VinCSS FIDO2® Fingerprint

THÔNG TIN	CHI TIẾT
Tên sản phẩm	VinCSS FIDO2® Fingerprint
Chuẩn 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	Xác thực không mật khẩu, xác thực 2 yếu tố, xác thực mạnh đa yếu tố
Chứng chỉ	FIDO2® Certified, FCC, JQA
Giao thức hỗ trợ	WebAuthn, FIDO2 CTAP1, FIDO2 CTAP2, Xác thực 2 yếu tố (U2F)
Trình duyệt hỗ trợ	Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge, Microsoft Edge Chromium
Số lượng tài khoản có thể lưu trữ	50
Số lượng vân tay có thể lưu trữ	5
Đèn báo hiệu	RGB Led
Độ phân giải cảm biến vân tay	508 dpi
Trọng lượng	20gr

THÔNG SỐ KỸ THUẬT

Khóa bảo mật VinCSS FIDO2® Fingerprint

THÔNG TIN	CHI TIẾT
CPU	32-bit ARM® Cortex™-M4
Tỉ lệ chấp nhận sai FAR	<0.0002%
Thời gian xác thực vân tay	<1s
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
Kích thước sản phẩm	45,7 x 38 x 8,3 mm
Nhiệt độ hoạt động	-10°C đến 60°C
Màu sắc	Đen, trắng, xanh
Phụ kiện đi kèm	Cáp USB type-C, móc khoá, giá đỡ
Xuất xứ	Việt Nam

Để biết thêm thông tin, vui lòng liên hệ *sales@vincss.net*,
Hoặc nhà cung cấp dịch vụ của bạn.

VinCSS

Trusted Cybersecurity Pioneer

fido ALLIANCE

VinCSS - A member of FIDO ALLIANCE

The FIDO Alliance is an open industry association with a focused mission: Authentication standards to help reduce the world's over-reliance on passwords

CÔNG TY CỔ PHẦN DỊCH VỤ AN NINH MẠNG VINCSS

- Tầng 20A, Vincom Center
45A Lý Tự Trọng, phường Bến Nghé, quận 1, TPHCM
- Email: sales@vincss.net
- Website: https://passwordless.vincss.net