



Fido2 NFC card

with MIFARE[®]DESFire[®] Functionality

Manual and Specifications



Member of the



Version 1.3 - August 2024

Table of content

Table of content	1
Introduction - What is FIDO2	4
How FIDO2 Works.....	4
Examples of FIDO2 Applications.....	4
FIDO2 startup guide	6
Compatibility.....	6
Android and IOS Mobile Phones.....	6
Communication.....	6
Mobile browsers website login.....	6
Mobile OS login.....	6
Windows and MacOS desktops.....	7
Communication.....	7
Desktop browsers website login.....	7
Desktop OS login.....	7
Different Server Implementations.....	8
With PIN or Without PIN.....	9
Server PIN Policy.....	9
Pop Up Notifications.....	10
PIN management and Reset.....	12
Max PIN Try.....	13
A note on the terms "Security Key" and "Passkey".....	14
NFC phone location.....	15
How to Properly Select the Cryptnox Card for Login.....	17
Testing.....	22
Sites accepting FIDO2 and U2F.....	22
AAGUID.....	22
Google Account	23
Use case:.....	23
Server implementation:.....	23
PIN policy:.....	23
Steps:.....	24
AppleID account	29
Use case:.....	29
Server implementation:.....	29
PIN policy:.....	29
Steps:.....	29
Windows Sign In	34
Use case:.....	34
Server implementation:.....	34

PIN policy:.....	34
Steps:.....	35
Cryptnox FIDO2 App on the Apple Store.....	42
How to check the genuinity of a Cryptnox Card.....	42
Other features of the Cryptnox FIDO2 application.....	46
Chip Specification.....	47
Provider.....	47
Model.....	47
JCOP Platform.....	47
Capacitances available.....	47
Available functionalities from Cryptnox.....	47
Chip Certifications.....	47
Communication.....	47
Form Factors Available.....	47
Unique Identifier.....	47
FIDO2 v2.1 Specifications.....	48
Execution Environment.....	48
Applet Certification.....	48
Applet characteristics.....	48
Applet Options.....	48
Client Management Application.....	48
AAGUID.....	48
MIFARE DESFire	50
Overview.....	50
Application Areas.....	50
Mifare Technical Specifications available on Cryptnox Card.....	50
About FIDO Alliance.....	52
About Mifare.....	52
About Cryptnox.....	52
References.....	53

Introduction - What is FIDO2

FIDO stands for **F**ast **I**dentify **O**nline. FIDO2 is the latest evolution of a cutting-edge authentication standard designed to enhance security and simplify the login process across both mobile and desktop environments. It allows users to utilize devices such as the Fido2 Certified Cryptnox card to authenticate to online services without relying on traditional passwords. In addition to online services, it can also authenticate in environments such as AppleID on an iPhone or MacOS, or a work/school account on a Microsoft Windows desktop.

The FIDO2 specifications include two primary components: the World Wide Web Consortium's (W3C) Web Authentication (WebAuthn) specification and the FIDO Alliance corresponding Client-to-Authenticator Protocol (CTAP). Together, these specifications enable secure and easy-to-use authentication experiences.

How FIDO2 Works

In the case of Cryptnox Card, it operates as a hardware Security Key using public key cryptography. During the registration process with an online service, the Cryptnox Card creates a new public-private key pair. The private key is stored securely, while the public key is shared with the online service. For authentication, the user proves possession of the private key by signing a challenge within the Cryptnox Card, which is verified by the service using the stored public key.

FIDO2 authentication is versatile and can be used in various authentication scenarios. By order of popularity, we can mention two-Factor Authentication (2FA), Passwordless Authentication, and Credential Less Authentication (Resident Login). These will be described later in this guide.

Examples of FIDO2 Applications

- **Corporate Security:** Many organizations implement FIDO2 to secure access to corporate applications and networks, ensuring that only authenticated users can access sensitive information.
- **Online Banking:** Banks and financial institutions are increasingly adopting FIDO2 to secure online banking transactions, providing customers with a secure and convenient way to access their accounts without passwords.
- **Government Services:** Various government agencies worldwide are implementing FIDO2 to secure access to services, ensuring that citizens can safely interact with government platforms.

- Various Personal Online Accounts: FIDO2 is already implemented on well known websites such as Google, Facebook, X (Twitter), Gitlab and many more, expanding every day. It is mostly used as a second factor authentication, but passwordless implementation is becoming more and more popular.
- Use cases are also expanding into more specific environments, such as Secure Shell (SSH) connections and blockchain smart contracts.

For more information on FIDO2, visit the FIDO Alliance website at <https://fidoalliance.org/fido2>.

FIDO2 startup guide

Note before you start:

There is no specific FIDO2 software installation required.

Compatible browsers and operating systems include built-in support for FIDO2 devices (no need to install any Cryptnox software).

Compatibility

FIDO2 authentication is a technology that is entering its maturity phase, and is still evolving. The compatibility characteristics listed in this guide are valid only as of its publication date, and will expand in the future.

Android and IOS Mobile Phones

Communication

The Cryptnox Card supports NFC communication with NFC enabled iPhone and Android devices. The FIDO2 NFC communication functionality is already built in, there is no software installation required.

Mobile browsers website login

- **Android:**
For websites login on mobile phones (via NFC), major mobile browsers are compatible on Android.
- **iOS:**
Only Safari is compatible

Mobile OS login

Only iOS is supported. It can be used as a highly secure 2FA for logging an iPhone into an AppleID.

Windows and MacOS desktops

Communication

The Cryptnox Card requires a smartcard reader to communicate with the operating system and the browser. It can either be an integrated reader, or an external reader connected via USB.

The card can be used with:

- A contactless reader (must be ISO 14443 Compliant (13.56 Mhz)
- Contact reader (must be ISO 7816 compliant) if the card is designed with a contact module.

Desktop browsers website login

- **Windows:**
The Cryptnox Card is currently supported on Microsoft Windows with most browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge.
- **Apple MacOS**
Safari and Firefox are supported.

Desktop OS login

- **Windows:**
A Cryptnox Card can be used as Security key sign-in into a Windows computer with a work or school account. A work account can be implemented with a Microsoft Windows 365 Business subscription. Note: with a Microsoft Personal account, a Cryptnox Card can still be used to log in to a Microsoft online account with a browser, but not to log into the computer itself.
- **MacOS:**
A Cryptnox Card can be used as a highly secure 2FA for logging a MacOS into an AppleID.

Different Server Implementations

FIDO2 authentication can be implemented server side in various configurations depending on the security requirements. The user has no influence on the implementation, it is fully dependent on the server. Here's a breakdown of the various options:

Method	Explanation
Two-Factor Authentication (2FA)	In this mode, FIDO2 authentication serves as a 2FA. The user first logs in using its username and password, and then uses a Cryptnox Card for 2FA. This greatly enhances security by adding an additional layer that requires physical possession of a physical device.
Passwordless Authentication	This mode allows users to log in without the need for passwords. Authentication is achieved using a username and the Cryptnox Card. This approach simplifies the login process while increasing security, as it eliminates the vulnerabilities associated with passwords.
2FA or Passwordless	Some servers allow Cryptnox Card registration for either Passwordless or 2FA authentication. If it is used for Passwordless authentication, the user will be prompted to use an alternate method for 2FA.
Resident Key	This mode involves storing the username on the internal memory of the Cryptnox Card, which is then provided automatically to the server during the authentication process. In this case, all the necessary authentication data is provided by the card. The number of maximum usernames stored by a Cryptnox Card is 32 for the certified FIDO2 version 2.0, and 64 for certified FIDO2 Version 2.1.

With PIN or Without PIN

A Cryptnox Card can operate with or without a PIN. Once a PIN is set, it is not possible to disable it without a full reset (and corresponding loss of credentials). If a card is to be registered on site with a "PIN Required" policy, setting a PIN during the process will be necessary.

Method	Explanation
With PIN	In this mode, it may or may not be required to enter a PIN to perform authentication with a registered Cryptnox Card (see Server PIN Policy below). The PIN is local to the device, enhancing security by combining something the user knows (the PIN) with something the user has (the Cryptnox Card).
Without PIN	This mode doesn't require the user to enter a PIN, simplifying the process. The authentication relies solely on the possession of the Cryptnox Card. If the server PIN policy is set to "Required", card registration is only possible if a PIN is irreversibly set.

Server PIN Policy

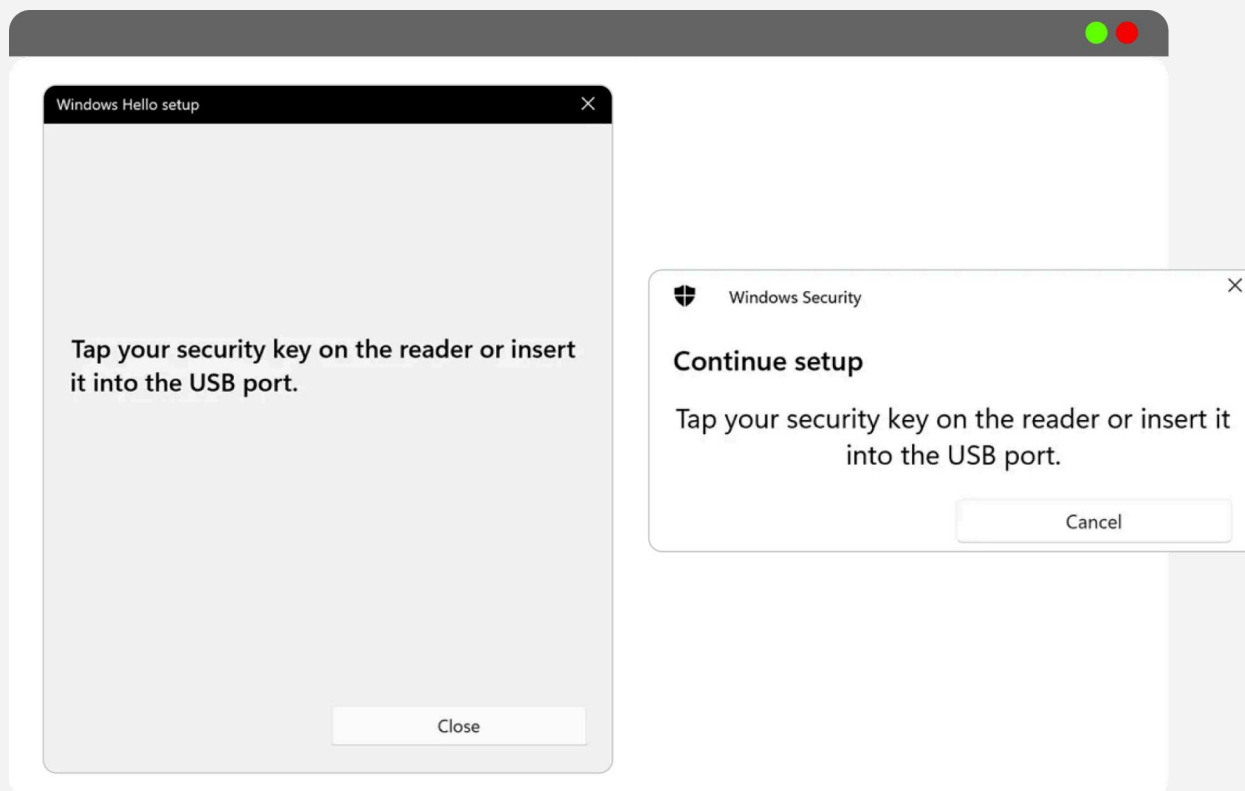
The following three different server implementations for PIN policy are possible. Each of these modes enhances security in different ways and can be adopted based on the security needs and user management practices of the organization.

Server PIN policy	Explanation
PIN Required	This means that the environment or site always requires PIN input whenever the card is used. PIN input is mandatory for authentication, and it will not be possible to proceed without a PIN set.
PIN Optional	This means that the environment or site will only ask for a PIN if one has been set on the card. If no PIN is set, there will be no request to enter one. However, if a PIN is set, it will be required for authentication.
PIN not required	This means that the environment or site does not require a PIN, whether one is set or not. Only the card itself is necessary for authentication, with no PIN requirement.

Pop Up Notifications

The request to connect with the Cryptnox Card is displayed as a pop-up notification with the "tap your Security Key on the reader" mention.

See examples below:



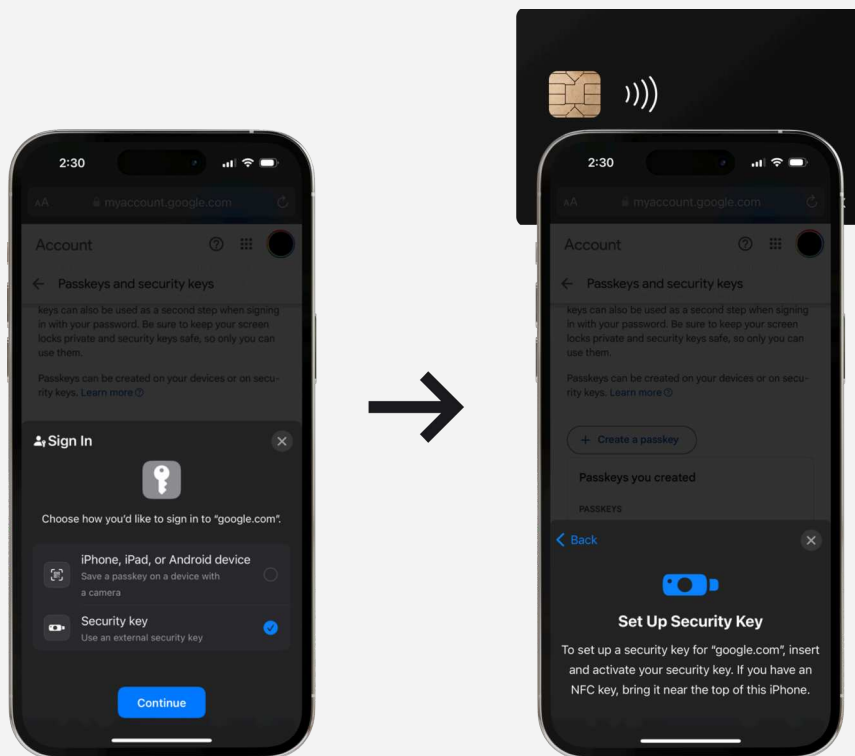
With an NFC or contact reader

Simply remove and replace the Cryptnox Card from the reader.



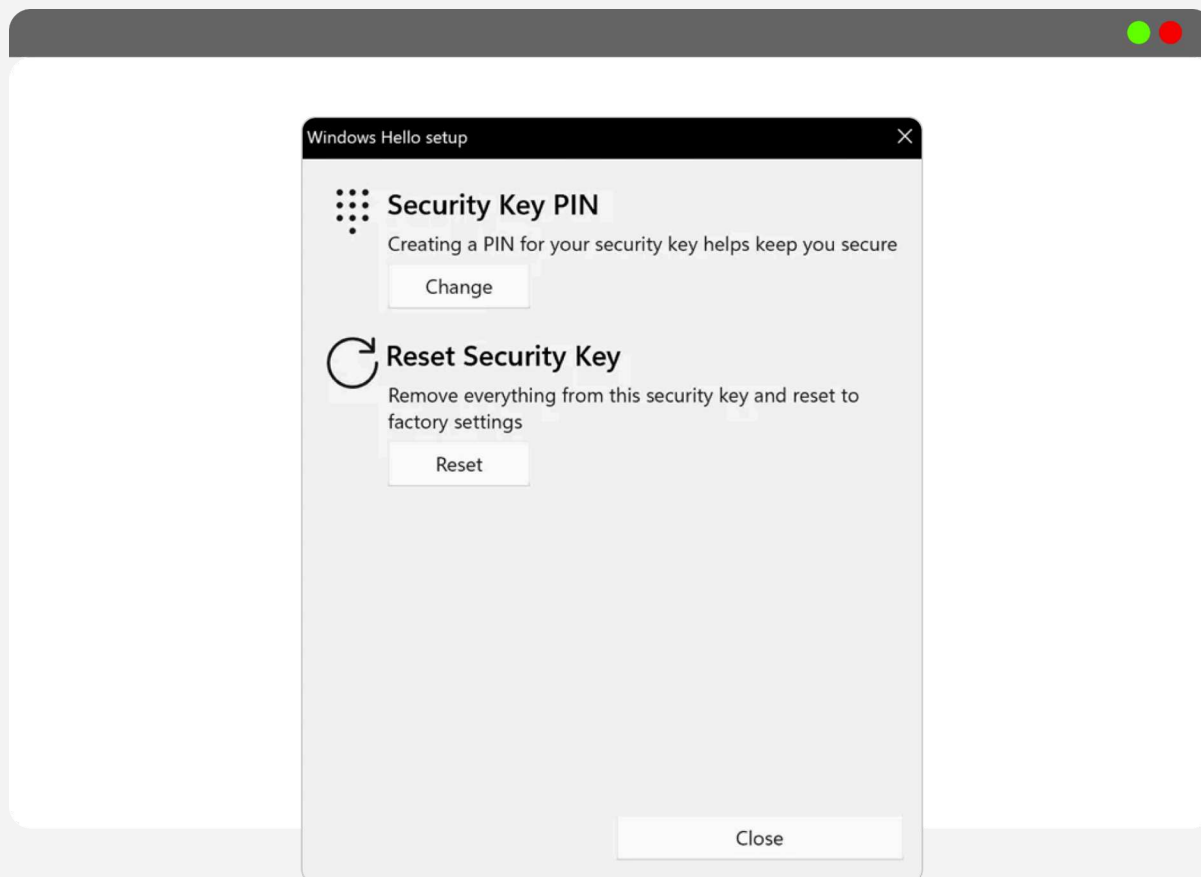
With a Phone

Simply select the "Security key" option and then tap the Cryptnox Card at the back of the phone.



PIN management and Reset

PIN can be managed (set or modify) and a Cryptnox Card can be fully reset with a Windows Desktop/laptop connected to a card reader. Go to Settings → Accounts → Sign In Options → Security Key → Manage.



Follow instructions and choose to manage the PIN or reset card.
Resetting the card will return it to the factory setting and delete all credentials.

It is also possible to use the Cryptnox FIDO2 Application to manage the PIN and fully reset the card (available only on IOS).

Max PIN Try

Important:

After three failed attempts, the card will need to be disconnected and reconnected before further attempts.

In any case, **the maximum number of attempts to enter the PIN is eight**. If the correct PIN is not entered within these attempts, the Cryptnox Card will be locked, requiring a full reset.

These rules are a requirement of the FIDO2 technical specifications.

A note on the terms “Security Key” and “Passkey”

The term “Passkey” is a general catch-all term used for any FIDO2 authentication solution. They include both hardware devices (cross platform) such as Cryptnox Cards as well as virtual keys (platform), which are generated and stored on an operating system itself. Windows, MacOS/iOS and Android operating systems can all generate virtual “Passkeys” that are linked to the device itself or the user account in the case of AppleID. Their FIDO2 authentication functionality is identical, the main difference is that the external hardware key is portable, and can be used on any device. Generally, the term “Passkey” will be used to describe both virtual “platform” keys, as well as external hardware “cross platform” keys. The term “Security Key” will generally refer more specifically to external hardware security keys such as the Cryptnox Card.

One advantage of hardware security keys is that they are compatible everywhere. As they are considered more secure, some high security implementations (such as government or financial institutions) will only allow the registration of hardware security keys, and block virtual keys. In addition, for environment logins into AppleID or Windows Desktop, only hardware security keys such as the Cryptnox Card can be used.

NFC phone location

Important:

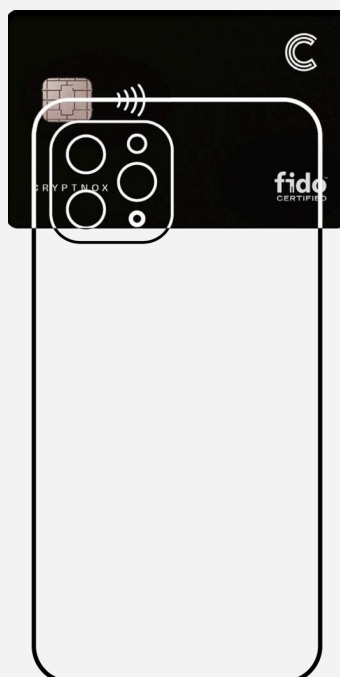
CARD POSITIONING ON PHONES FOR NEAR FIELD COMMUNICATION(NFC) VARIES ACCORDING TO BRANDS AND MODELS.

It is important to place it in the corresponding NFC antenna location for optimal operation. When prompted by the application, the card must be held firmly without movement until the end of the scanning process. Check the list below to identify the correct location for your phone, or look into the corresponding instructions manual.

NFC area 1

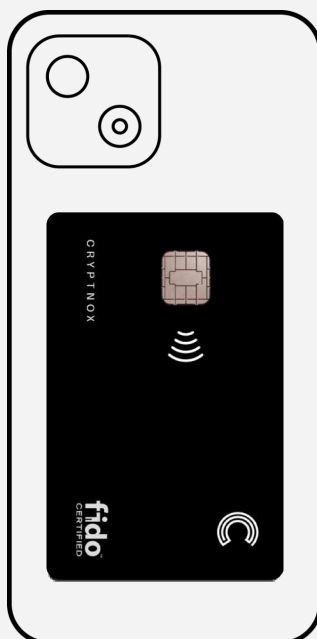
Antennae can be found on the back-side of the phone, on the top area.

Applicable to the following phones: iPhone 14, iPhone 13, Samsung Galaxy Fold, etc.



NFC area 2

Antennae can be found on the back-side of the phone, in the middle section.
Applicable to the following phones: Samsung galaxy S23, GooglePixel 6a, GooglePixel 7 pro.



NFC area 3

Antennae can be found on the back-side of the phone, on the top area.
Applicable to the following phones: Other pixels phones

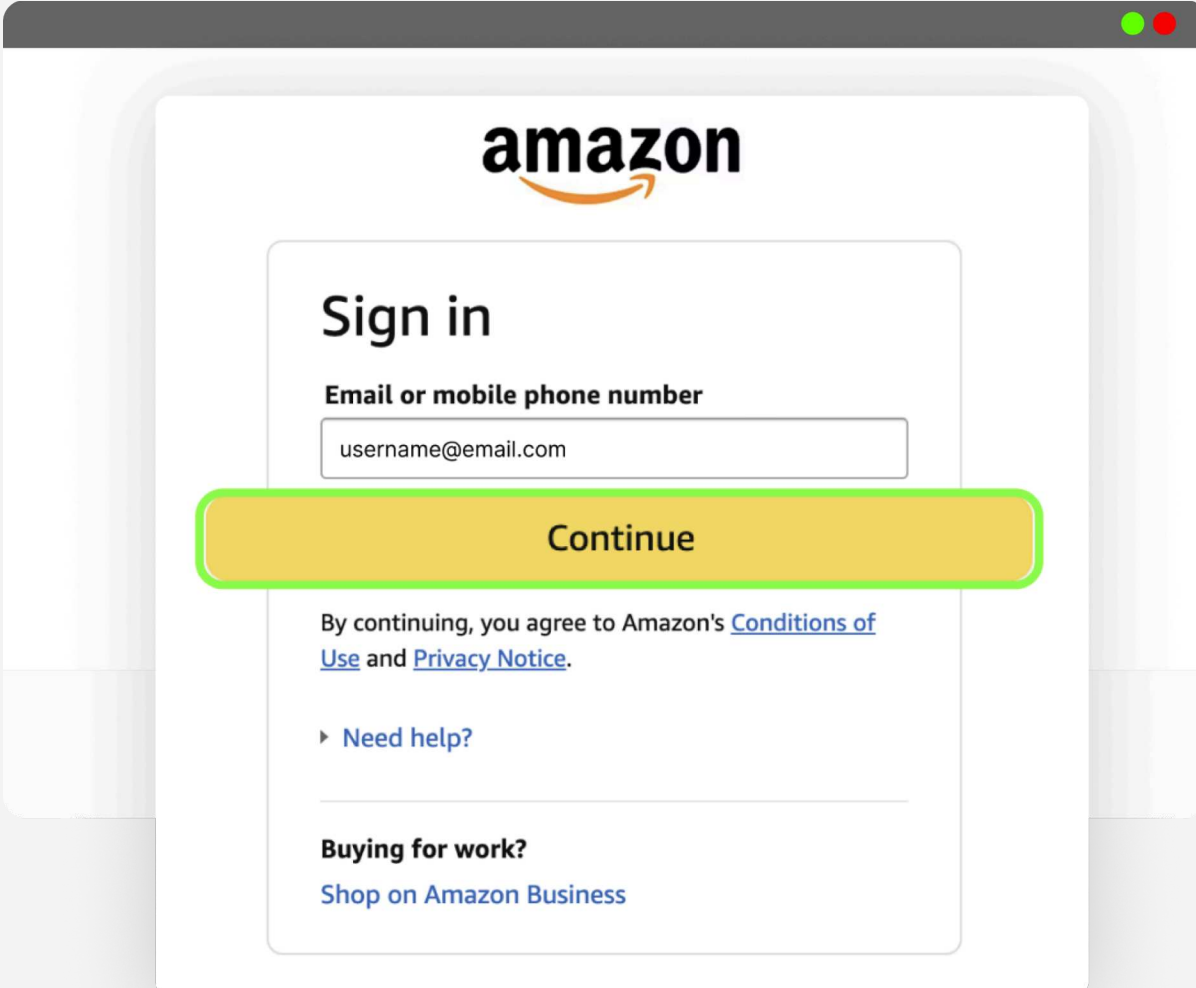


How to Properly Select the Cryptnox Card for Login

When the passkey option shows up during the log-in process, the choice of a Cryptnox Card as an external hardware Security Key might not be presented as a first option, especially from an environment with virtual Passkey availability such as Windows OS. Here below is presented the process of logging into an Amazon account as an example. The Amazon server implementation is Passwordless, and the PIN policy is Required

Step 1

Enter your email address and select "Continue".



amazon

Sign in

Email or mobile phone number

Continue

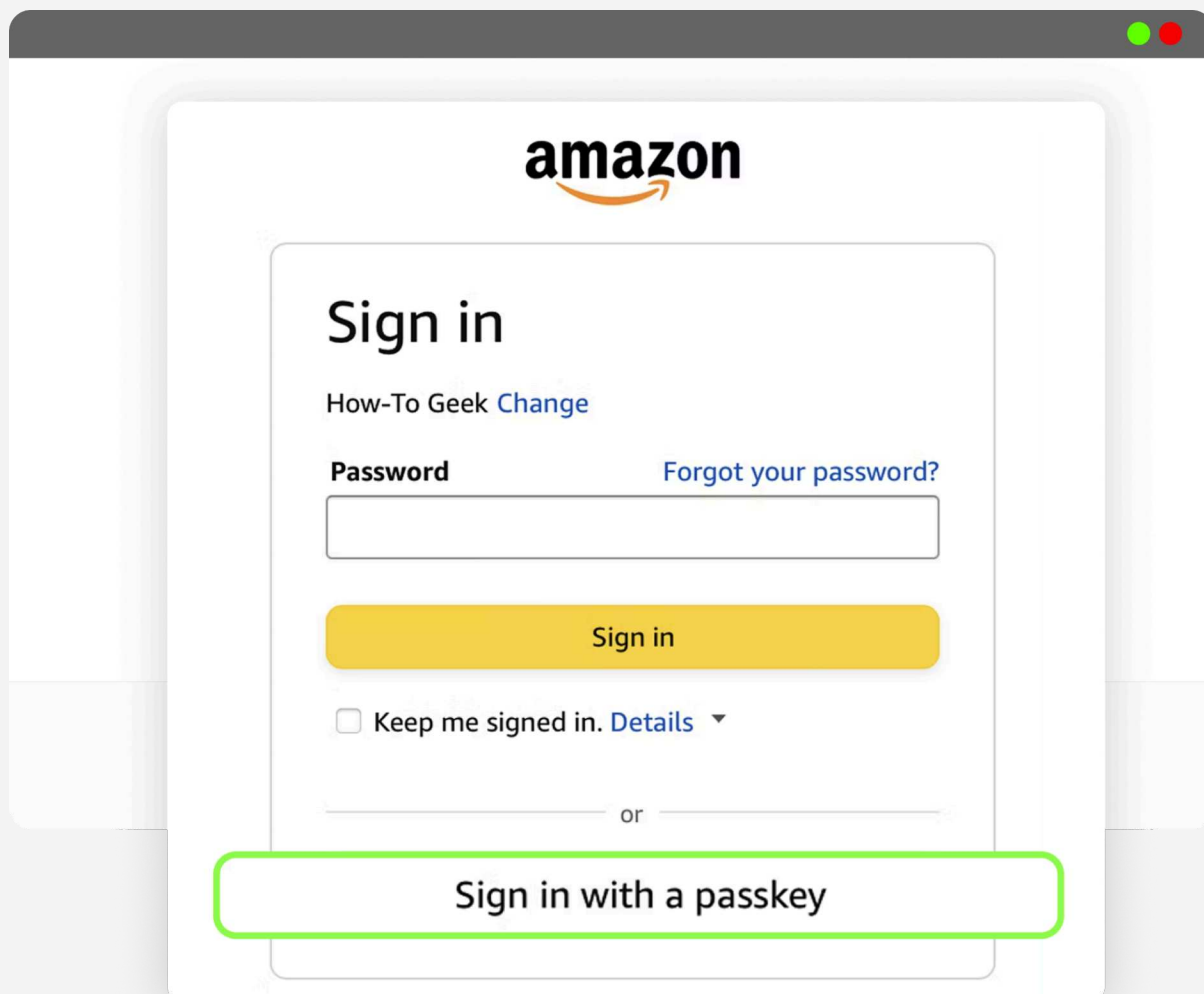
By continuing, you agree to Amazon's [Conditions of Use](#) and [Privacy Notice](#).

► [Need help?](#)

Buying for work?
[Shop on Amazon Business](#)

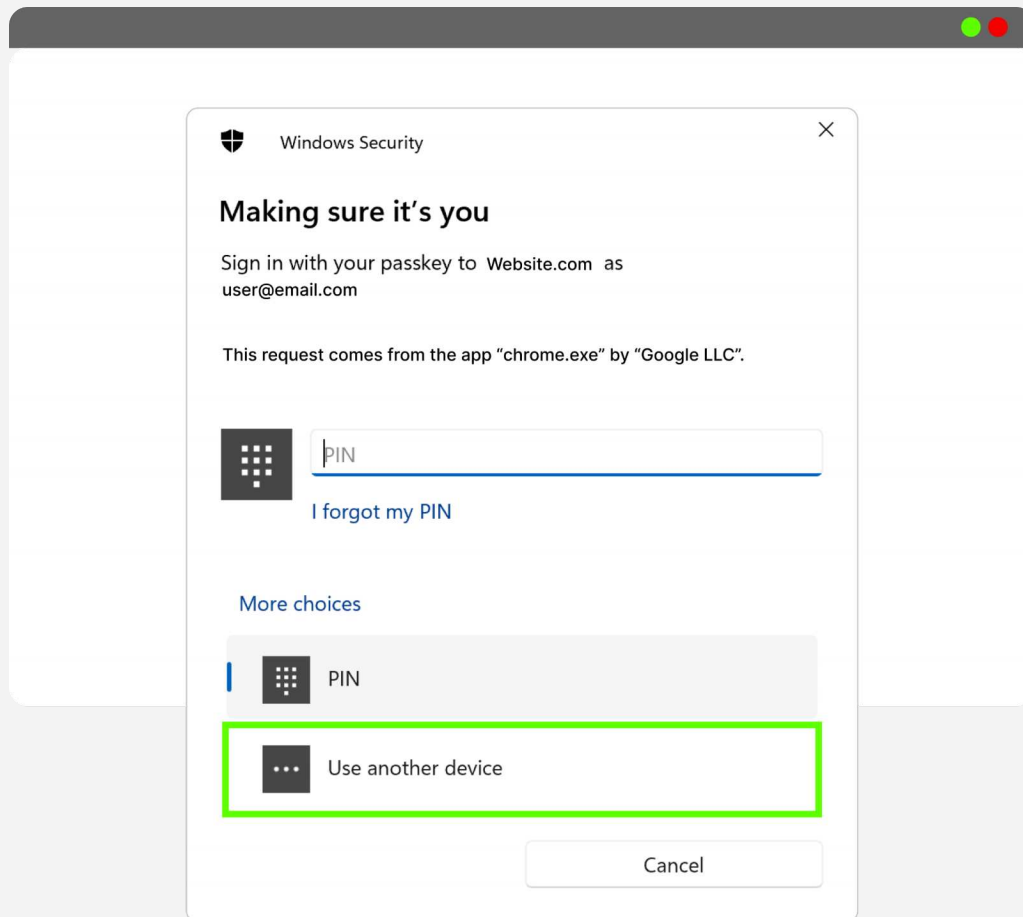
Step 2

If a Passkey/Security Key is registered, a Passwordless sign-in option will be displayed as "Sign in with a passkey", which must be selected.



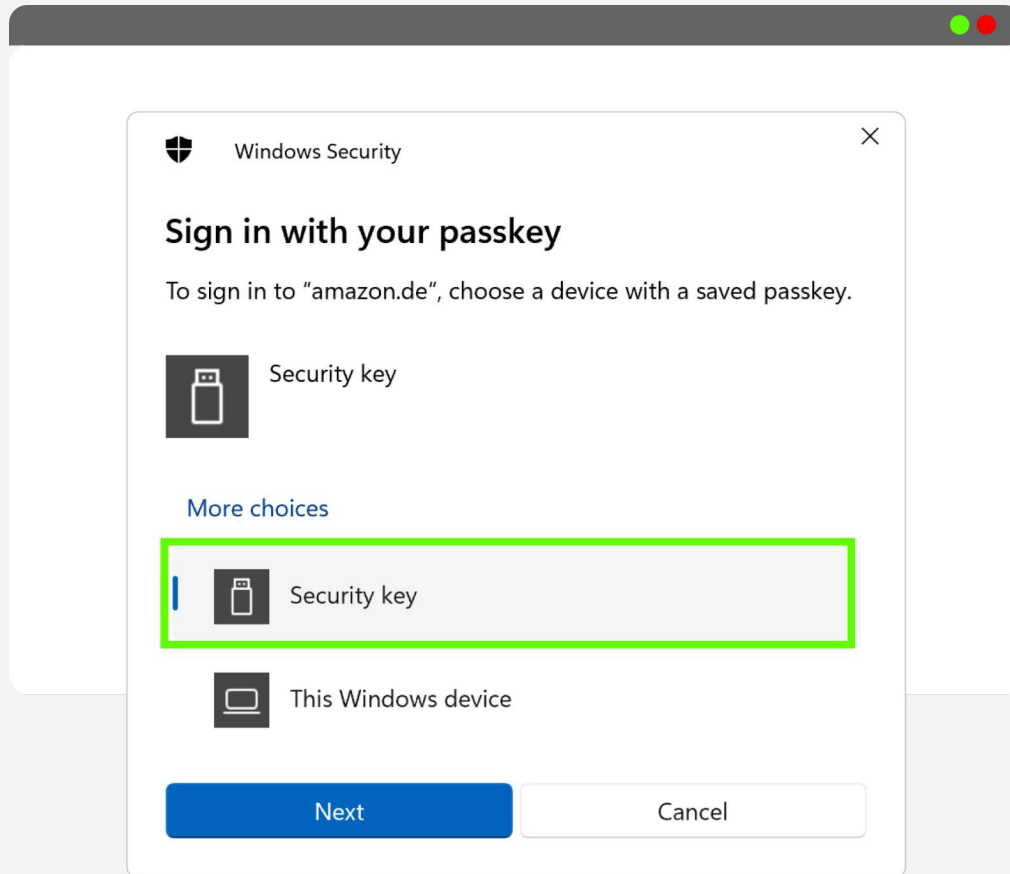
Step 3

If the website offers multiple sign-in options, 'User another device' option must be selected from the pop-up menu.



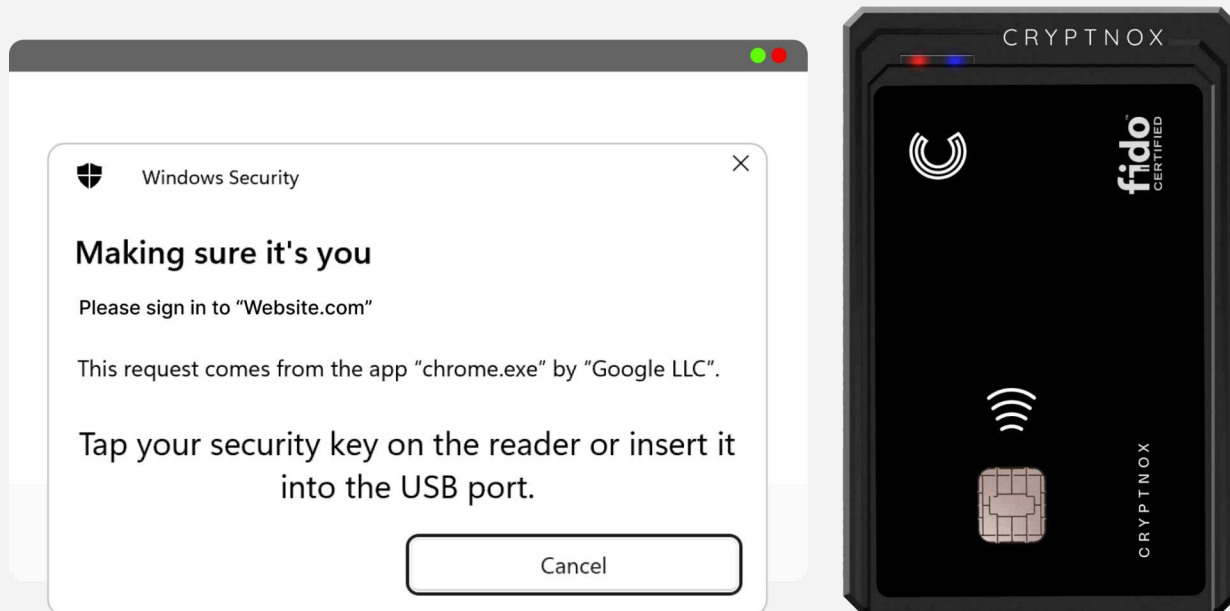
Step 4

Then select "Security key" from the pop-up menu.



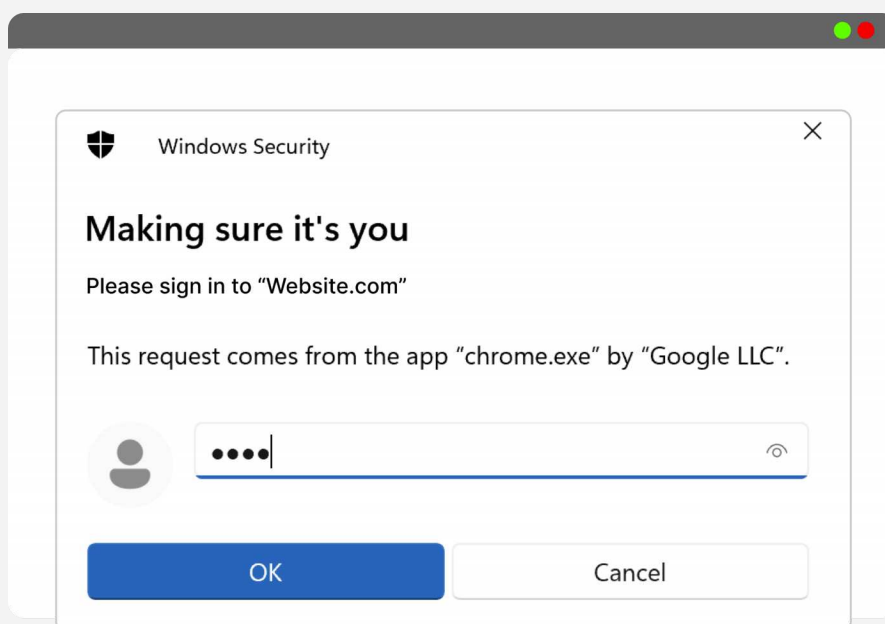
Step 5

The system will prompt the message to set up the Security Key. While the prompt is opening, place the card on the contactless reader.



Step 6

Enter the PIN for the card to log in to the website successfully.



Testing

Cryptnox Card registration and logging can be tested on the following “test” websites:
<https://fido2.cryptnox.tech> Or <https://webauthn.io>

If the box “Authenticator Type” appears, choose “Cross Platform”, which will direct the browser to the external Cryptnox Card. When choosing “Platform”, it will direct to system virtual key if enabled.

Sites accepting FIDO2 and U2F

The information about accepting FIDO2 authentication is generally displayed in the user account settings of websites. If they do, they generally have specific instructions.

AAGUID

In some rare cases, whitelisting of the AAGUID is required to register a Cryptnox Card.

For FIDO2 V2.0, it is:

9c835346-796b-4c27-8898-d6032f515cc5

For FIDO2 V2.1, it is:

1d1b4e33-76a1-47fb-97a0-14b10d0933f1

Google Account

Here we will present how to register a Cryptnox Card as a Security Key for a Google account.

Use case:

Website login (Google Account). Note: can also be used to connect a Google account to an Android phone.

Server implementation:

The configuration here is, interestingly, either Passwordless or Two Factor Authentication (2FA). This means that a username must be provided in any case, but if a Cryptnox Card is registered, it can be used either as an alternative to providing a password, or as a 2FA option if 2FA is activated. In case it is used for Passwordless authentication, another option will have to be selected for 2FA authentication. The server implementation will not allow the use of a Cryptnox card for both.

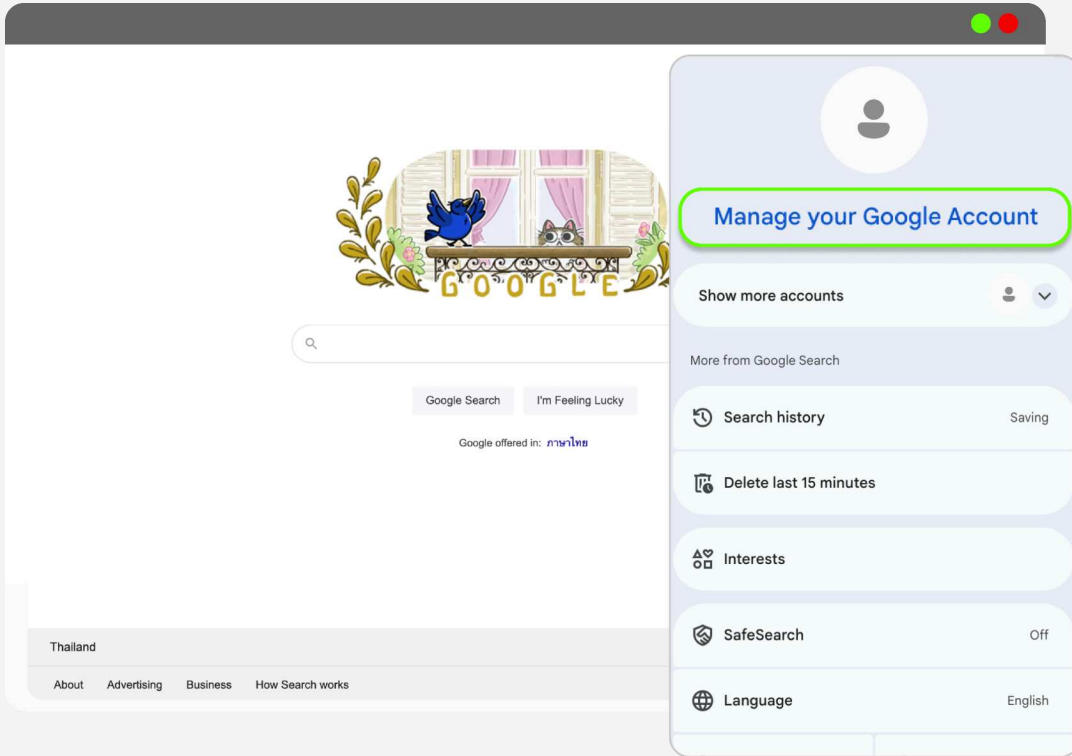
PIN policy:

The PIN policy on this site is Required, which means that a PIN will be required in all cases. If the Card does not have a PIN already set, the user will be prompted to set one, which will be asked every time at every login.

Steps:

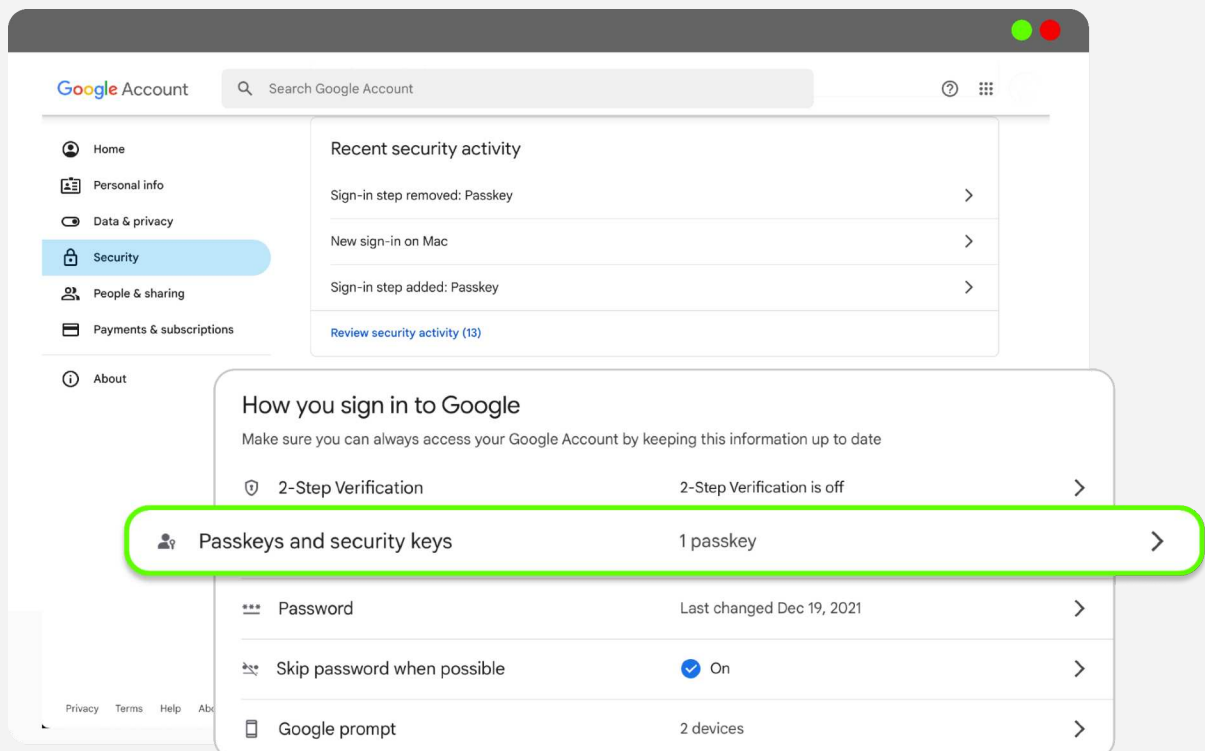
Step 1

Log in to your Google account first in the browser and Select "Manage your Google Account".



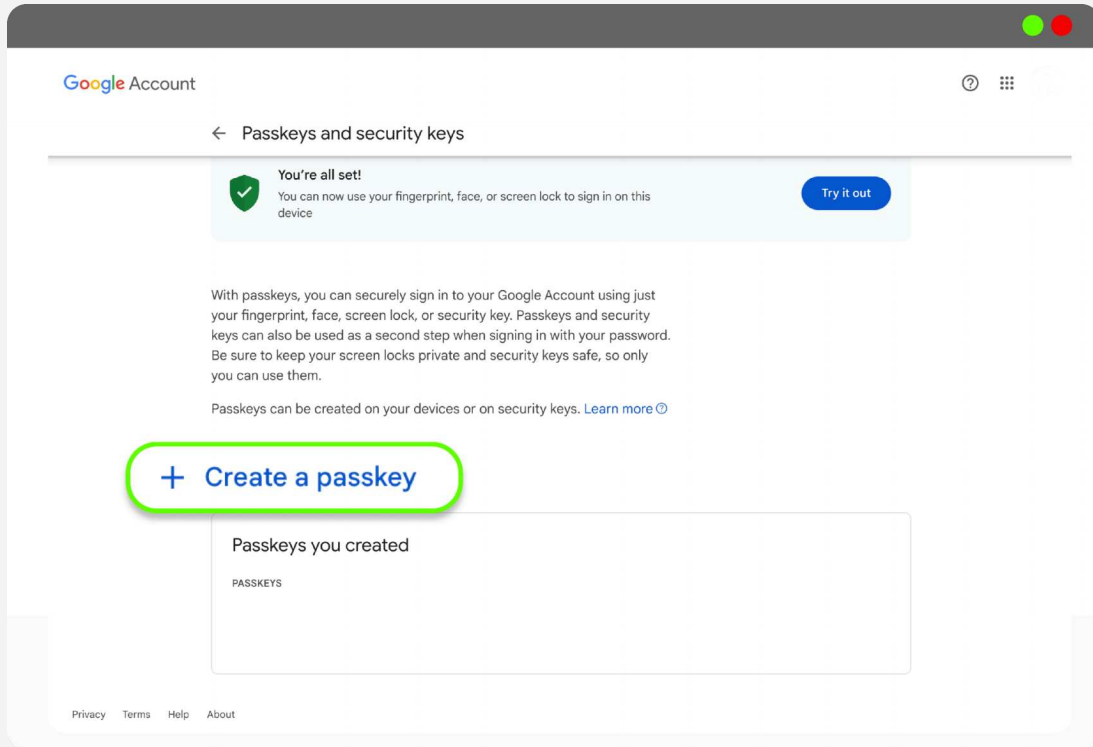
Step 2

Then "Security" and select "Passkeys and Security Keys".



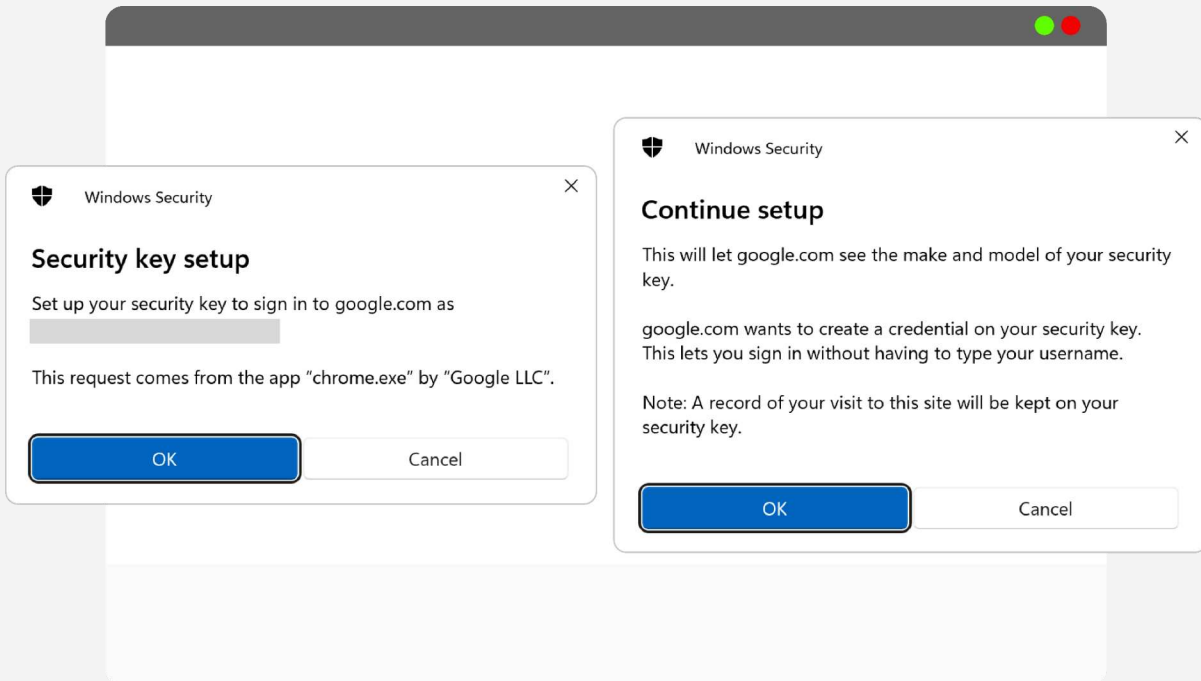
Step 3

Select "Create a passkey".



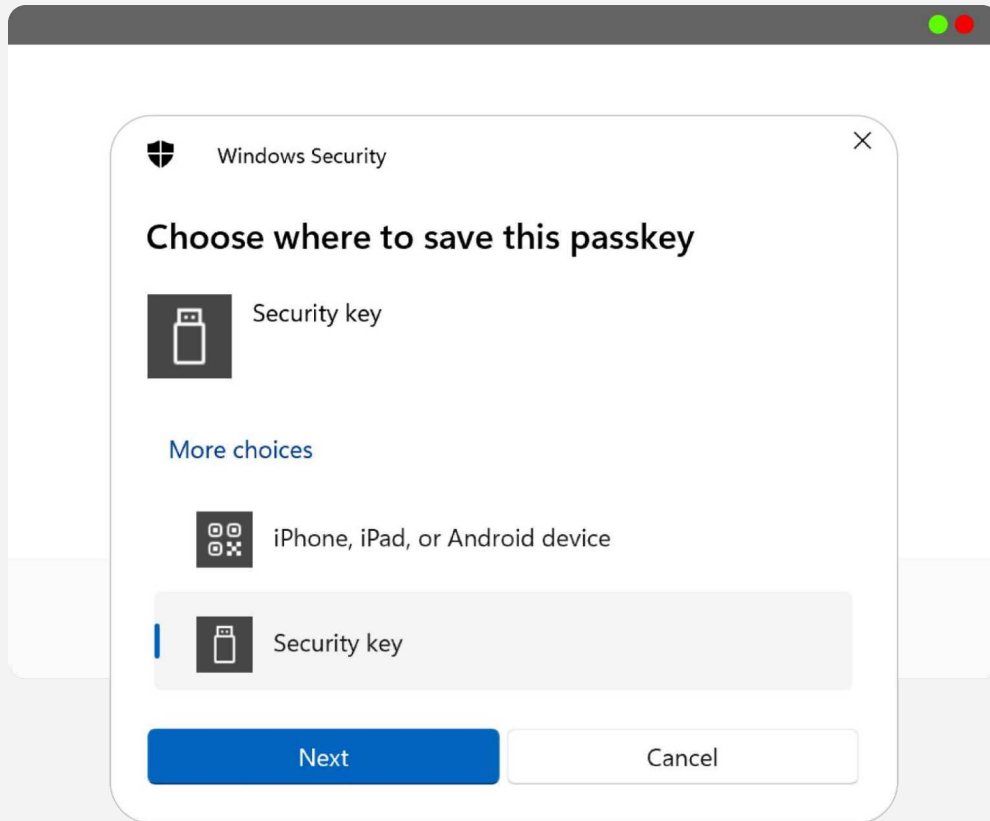
Step 4

Two Windows Security pop-ups will appear. Click 'OK' on both to continue.



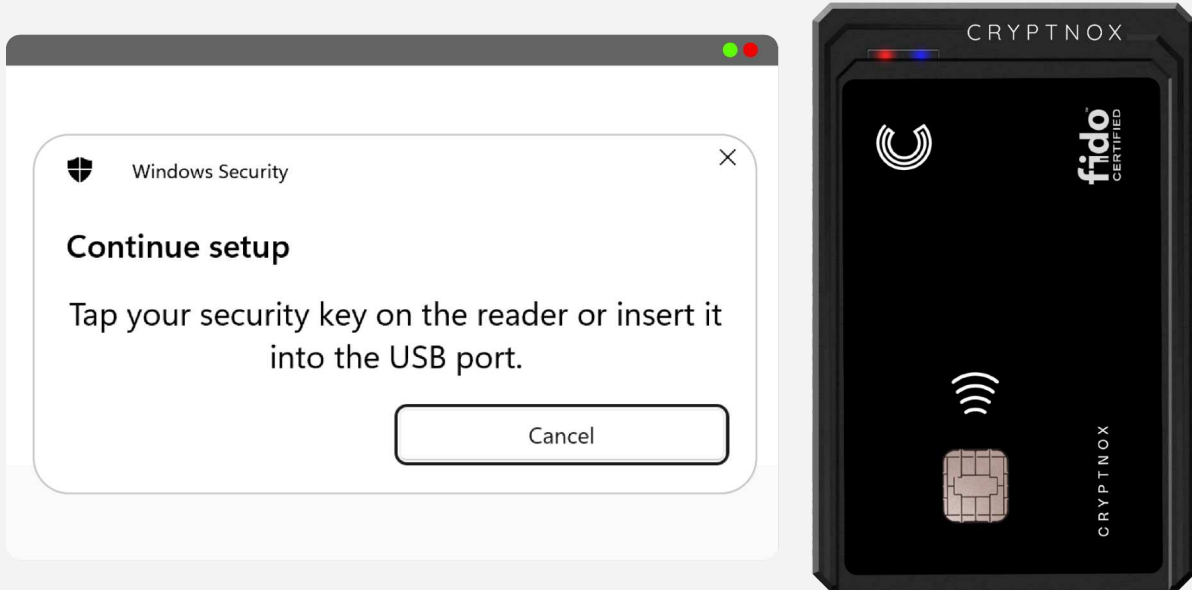
Step 5

Select "Security key" from the Passkey options.



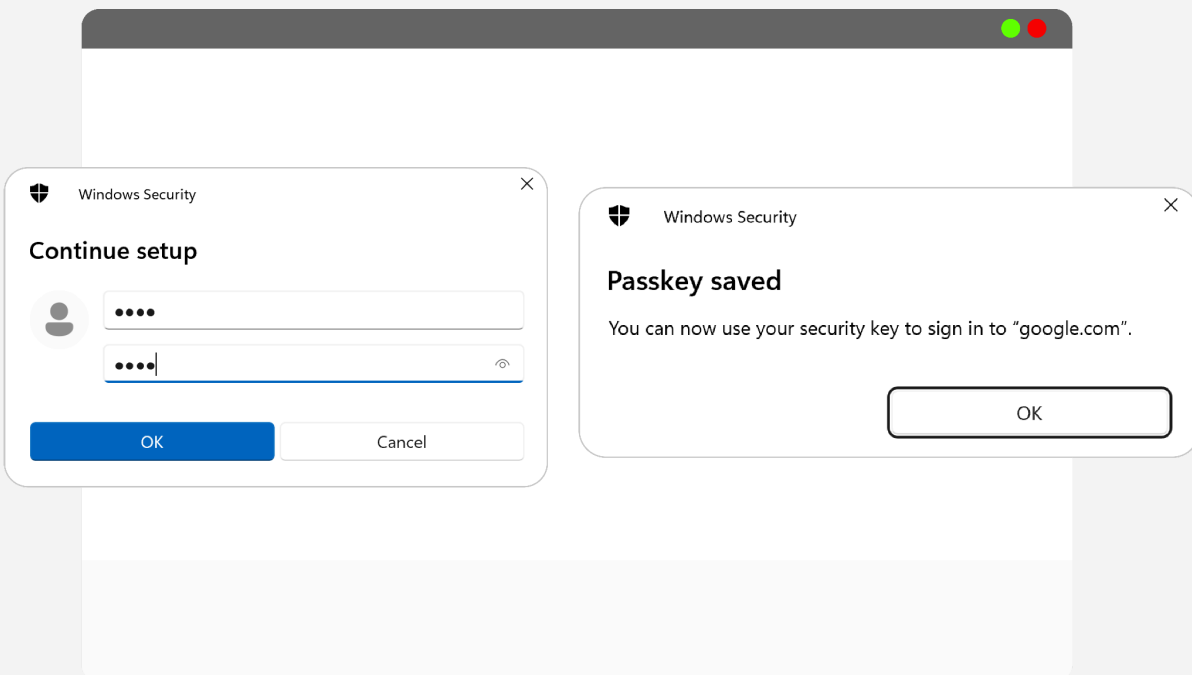
Step 6

The system will prompt the message to setup the Security Key. While the prompt is opening, place the Cryptnox Card on the contactless reader.



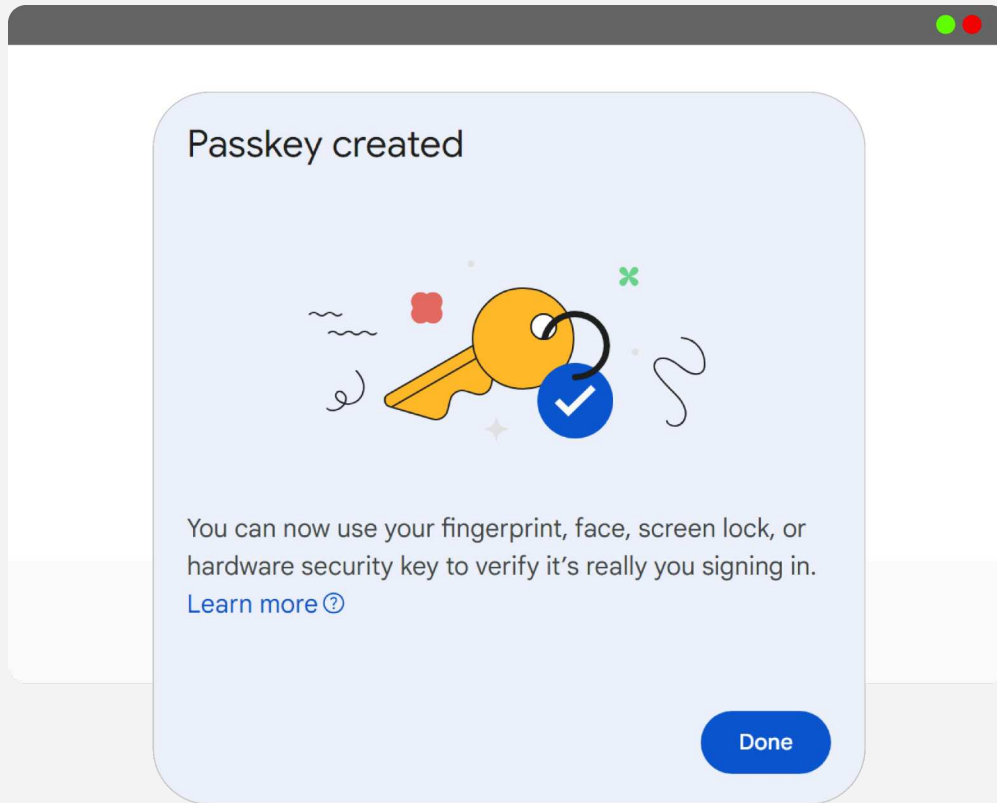
Step 7

Once the card is registered properly, the system will ask to enter the PIN. Then select "Continue".



Step 8

A Cryptnox Card has been successfully set up as a Security Key on the Google account.



AppleID account

Here we present how to register a Cryptnox Card as a Security Key for 2FA on AppleID on an Iphone. A minimum of two cards is required.

Use case:

Environment and Website login (IOS + MacOS AppleID & Website AppleID login)

Server implementation:

The configuration here is Two Factor Authentication (2FA). This means that if cards are registered as "Security Key" and 2FA is activated on an AppleID account, tapping one of them at the back of the phone will be required to log into an AppleID account.

PIN policy:

The PIN policy is Optional. This means that if a pin is set, entering a pin will be required. If no pin is set, no pin is required.

Steps:

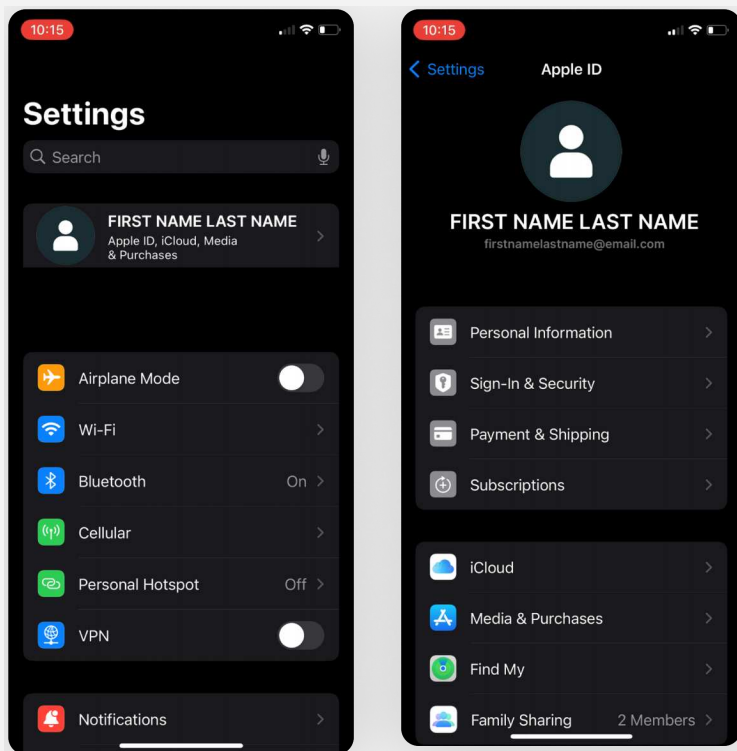
Ready your phone and cards

A minimum of two Cryptnox Cards is required for set up.



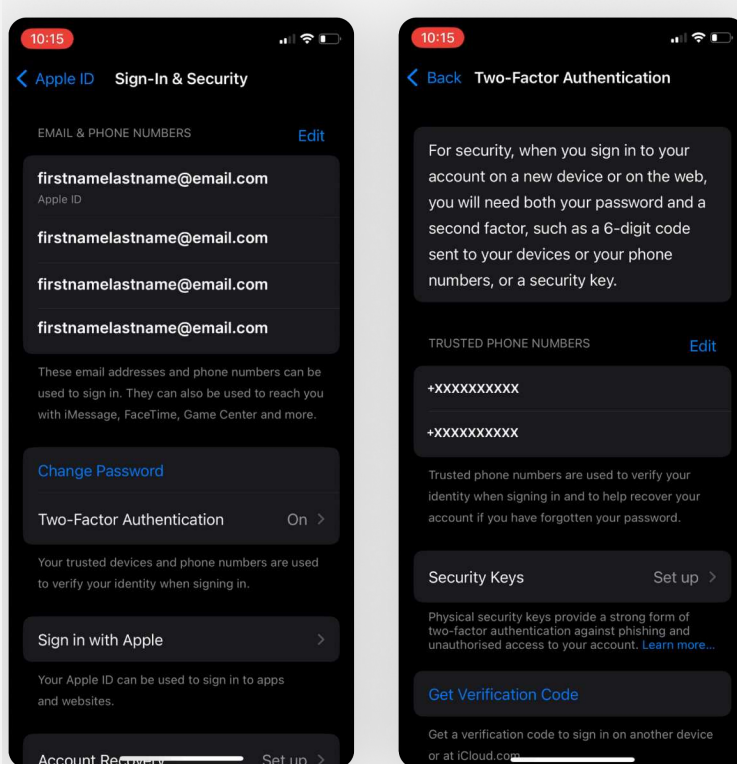
Step 1

Open setting, tap on username and tap on "Sign-in & Security".



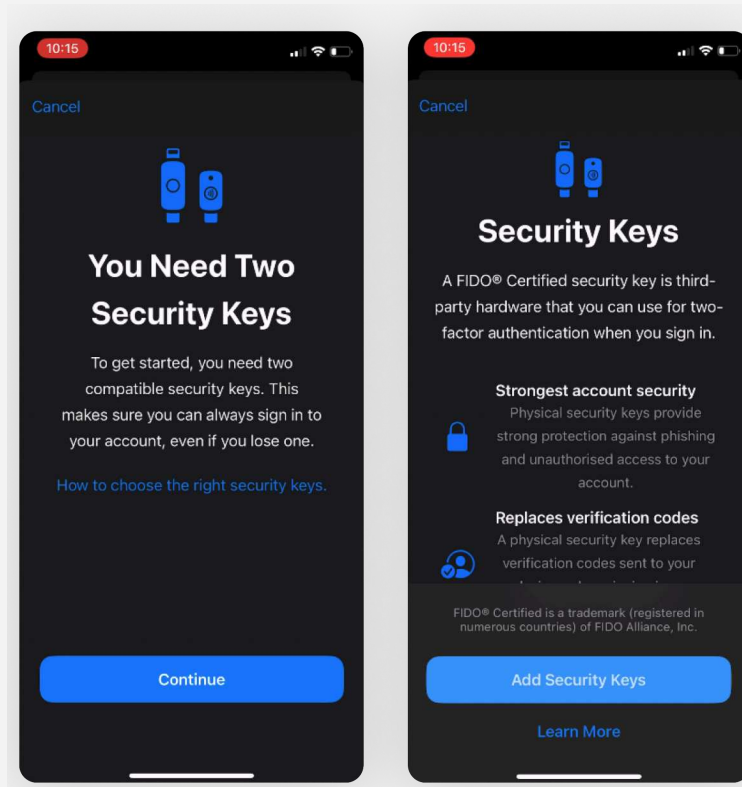
Step 2

Tap on Two-Factor Authentication and tap Security Keys.

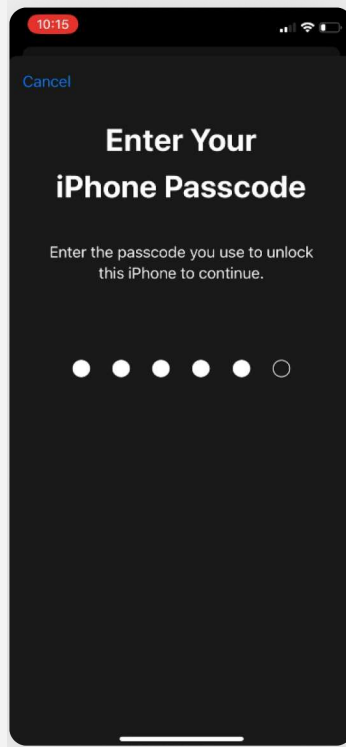


Step 3

Tap "Add Security Keys" and tap "Continue"

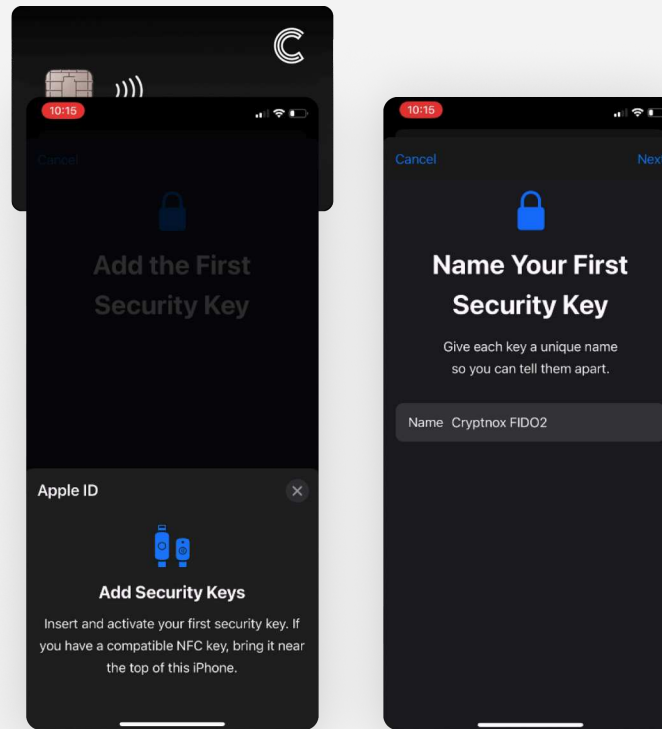
**Step 4**

Enter your phone passcode.

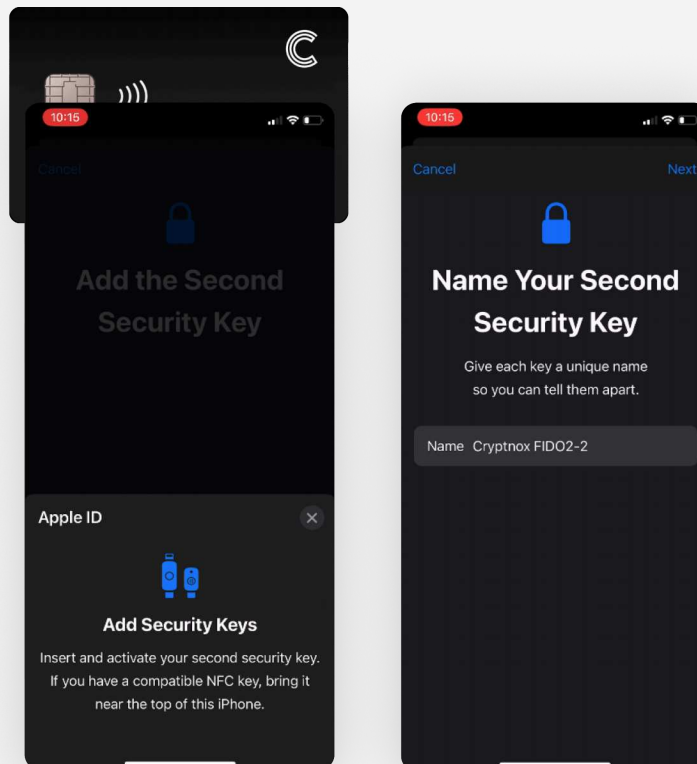


Step 5

Tap the 1st Cryptnox Card from the back of the phone, give a name for the card and tap "Next".

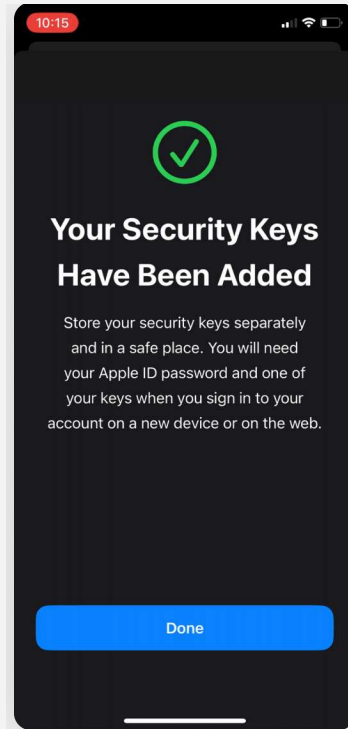
**Step 6**

Tap the 2nd Cryptnox Card from the back of the phone, give a name for the card and tap "Next".



Step 7

Cryptnox Card have successfully been set up with the AppleID.



Windows Sign In

Here we present how to register a Cryptnox Card as a Security Key for Passwordless Authentication on a Microsoft account. After registration, it can be used for website login on a personal, work or school accounts. For use with environment login (login into Windows Desktop), a work or school account is required.

Use case:

Environment and Website login (Windows Desktop Sign in & Website Microsoft account login)

Server implementation:

The configuration here is Passwordless. This means that a username must be provided, and the Cryptnox Card can be used as an alternative to provide a password.

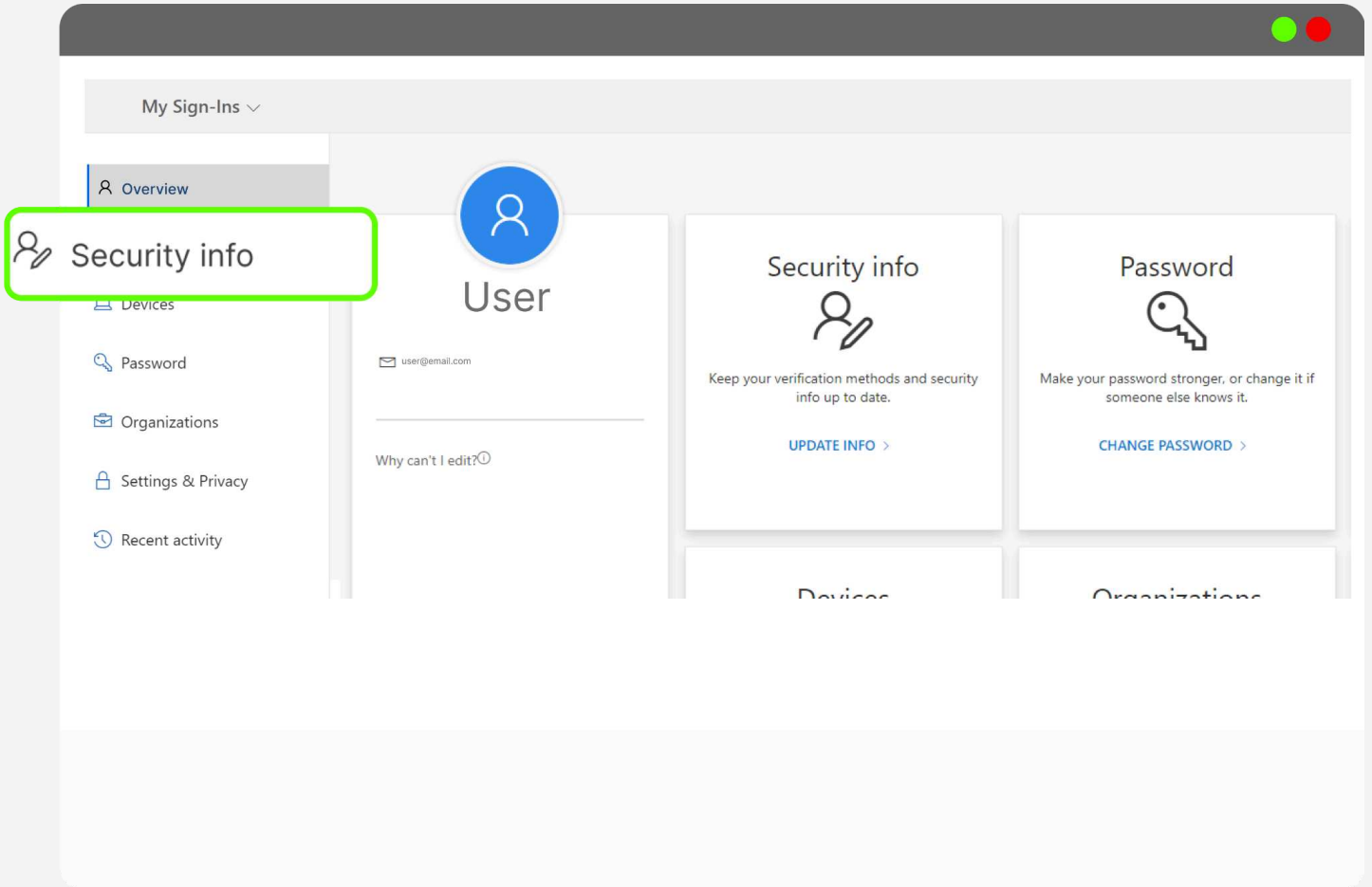
PIN policy:

The PIN policy on this site is Required, which means that a PIN will be required in all cases. If the Card does not have a PIN already set, the user will be prompted to set one, which will be asked every time at every login.

Steps:

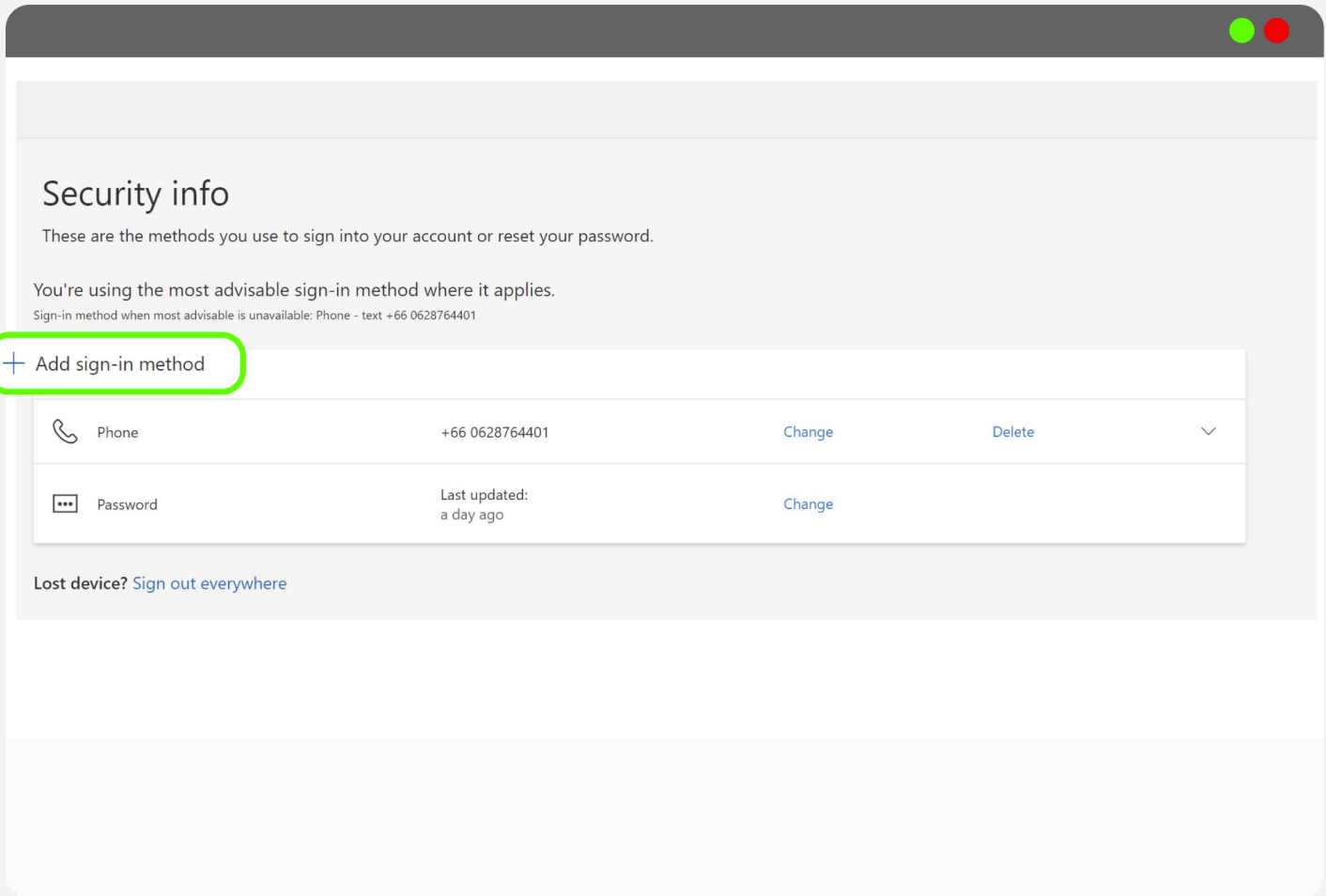
Step 1

Log in to your Microsoft account first and go to "Security info".



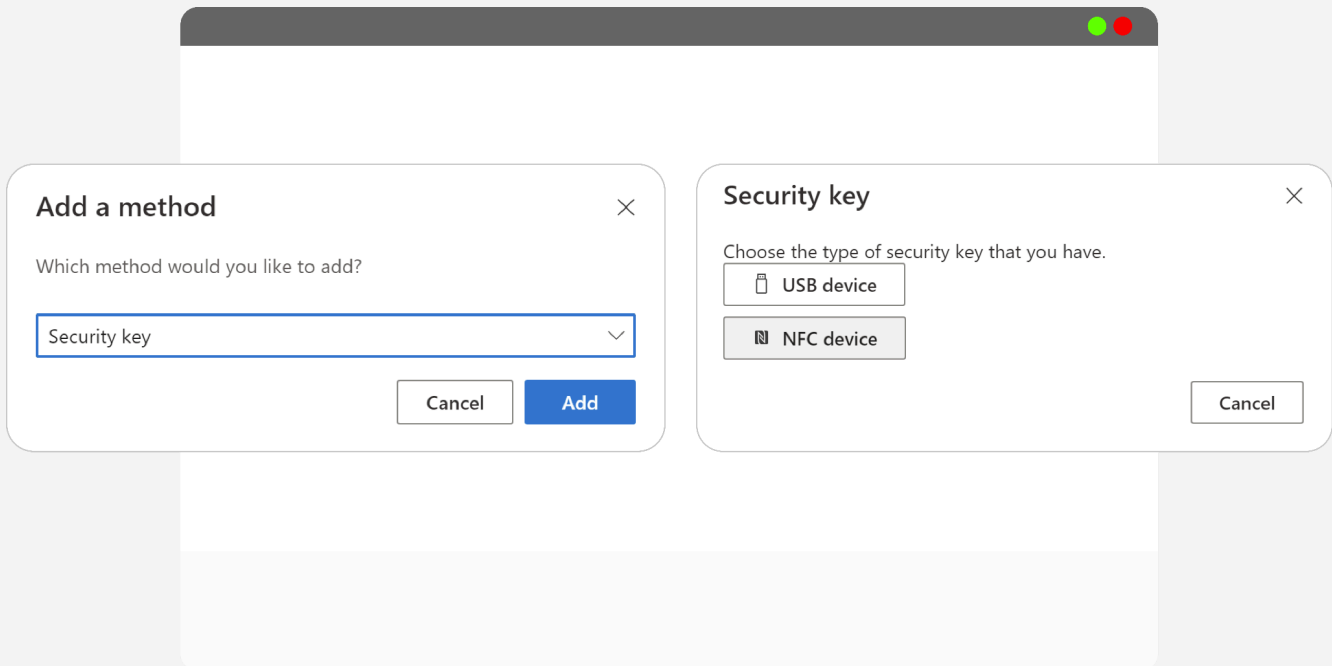
Step 2

In the Security info, select "Add sign-in method".



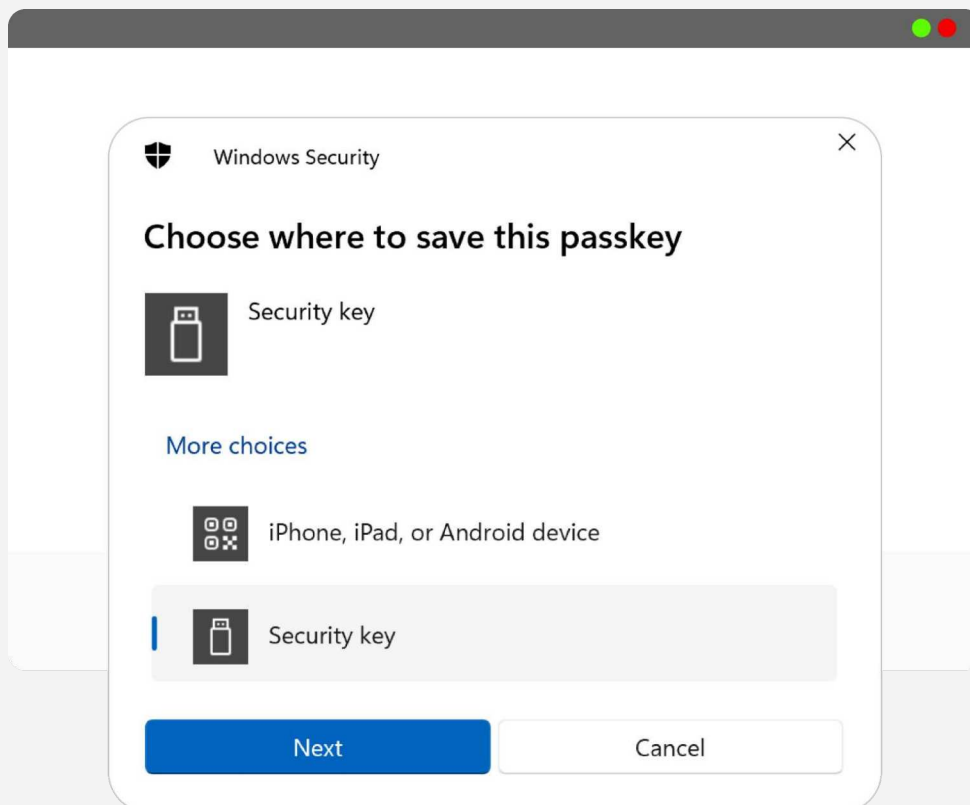
Step 3

The system will prompt you to select a method. Choose "Security Key" and select "Add". In the next pop up, select "NFC device".



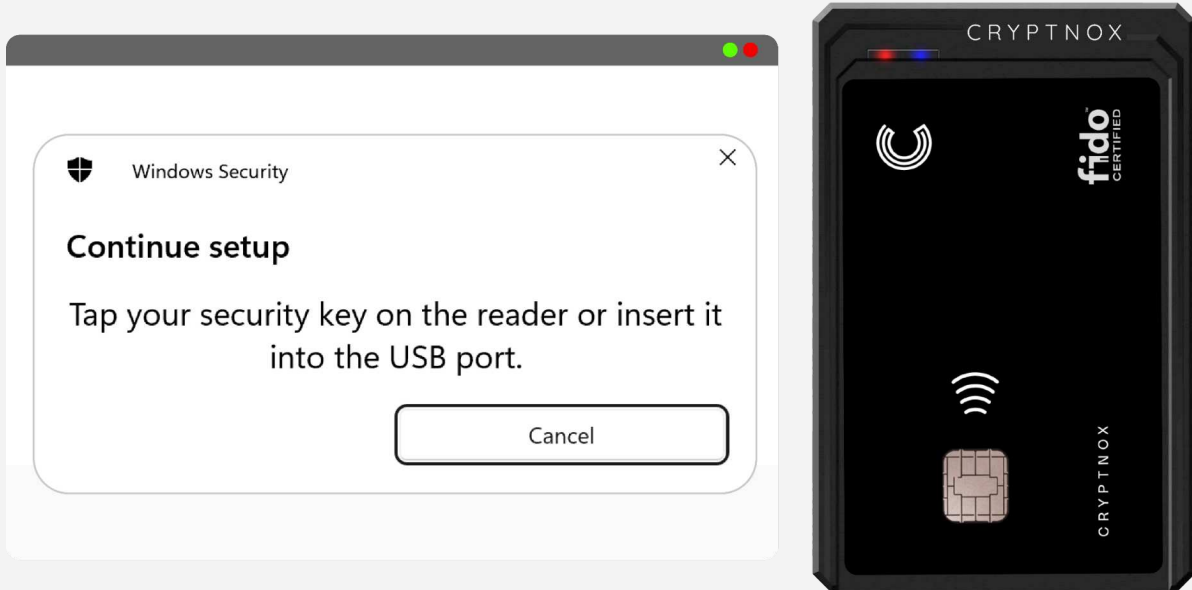
Step 4

Select "Security key" from the Passkey options.



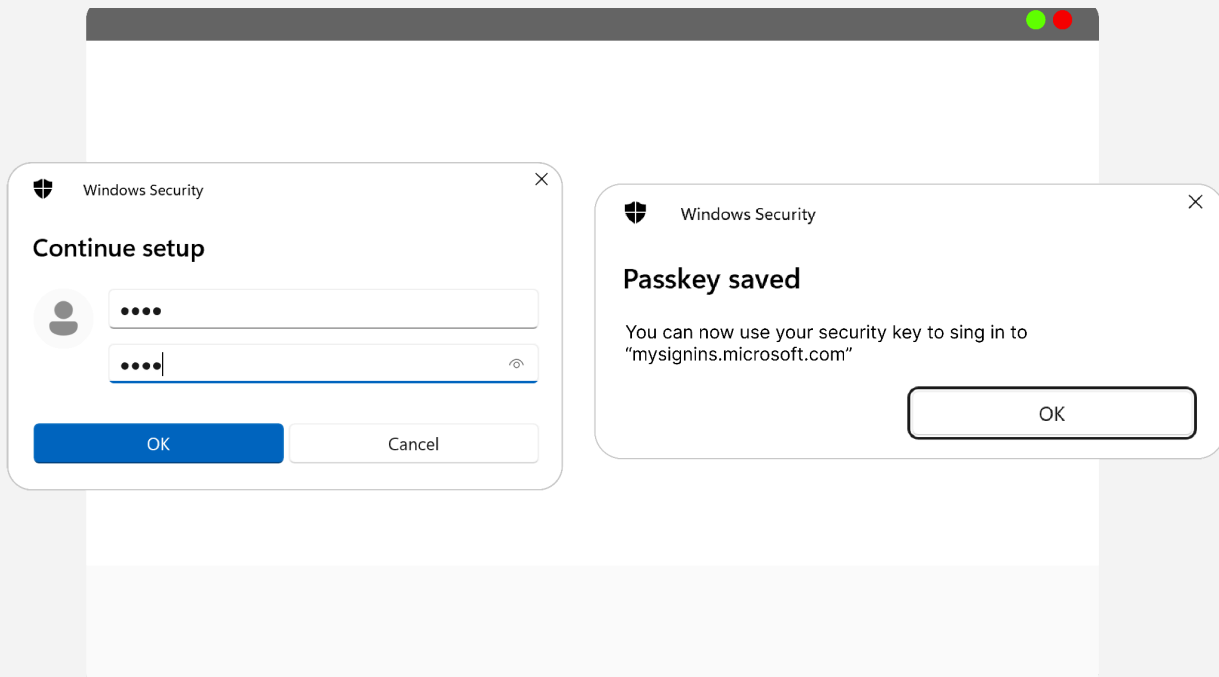
Step 5

The system will prompt the message to set up the Security Key. While the prompt is opening, place the card on the contactless reader.



Step 6

Before the card is properly registered, the system will ask for the PIN. After that, select "Continue" and in the next pop up, select "OK" again.



Step 7 Security key setup successfully.

The screenshot shows the Windows 'Security info' page. At the top, it says 'Security info' and 'These are the methods you use to sign into your account or reset your password.' Below that, it states 'You're using the most advisable sign-in method where it applies.' and 'Sign-in method when most advisable is unavailable: Phone - text +66 0628764401'. There are three sign-in methods listed in a table:

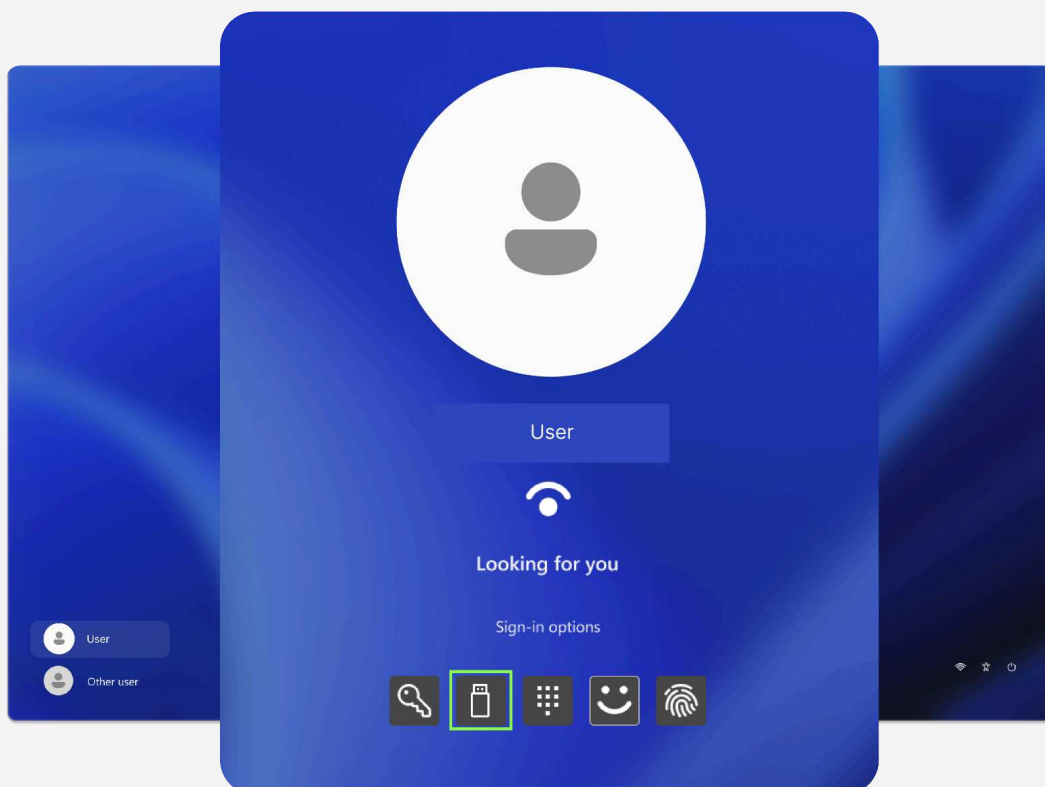
+ Add sign-in method				
	Phone	+66 0628764401	Change	Delete
	Password	Last updated: a day ago	Change	
	Security key Security Key	Cryptnox2.1.4		Delete

The 'Security key' row is highlighted with a green border.

Step 8

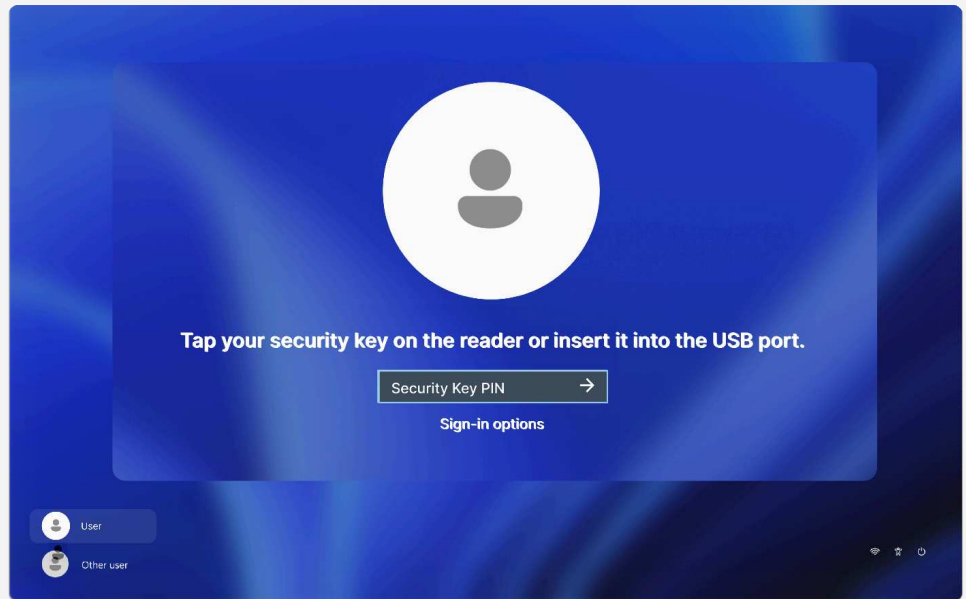
Now a Cryptnox Card can be used for Passwordless login into your online account.
The process is similar to other websites.

If you are using a work or school account, you can also use it to log into your desktop.
For this, restart your computer and in the login screen, select the "Security key" icon.



Step 9

Place the card on the reader and enter the passkey you set for the card to log in.



Cryptnox FIDO2 App on the Apple Store

How to check the genuinity of a Cryptnox Card

Cryptnox Card

An iPhone is required along with the Cryptnox Card.



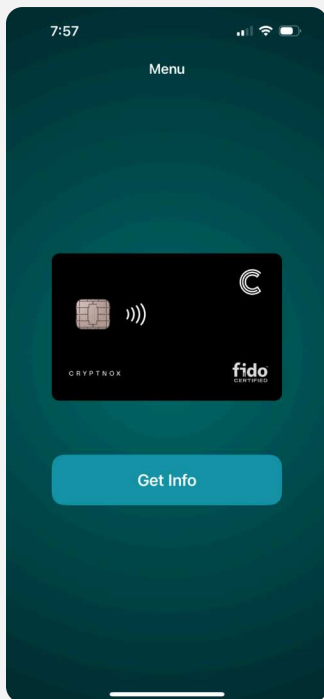
Cryptnox Card Management application

Ensure that the application is installed on the iPhone.



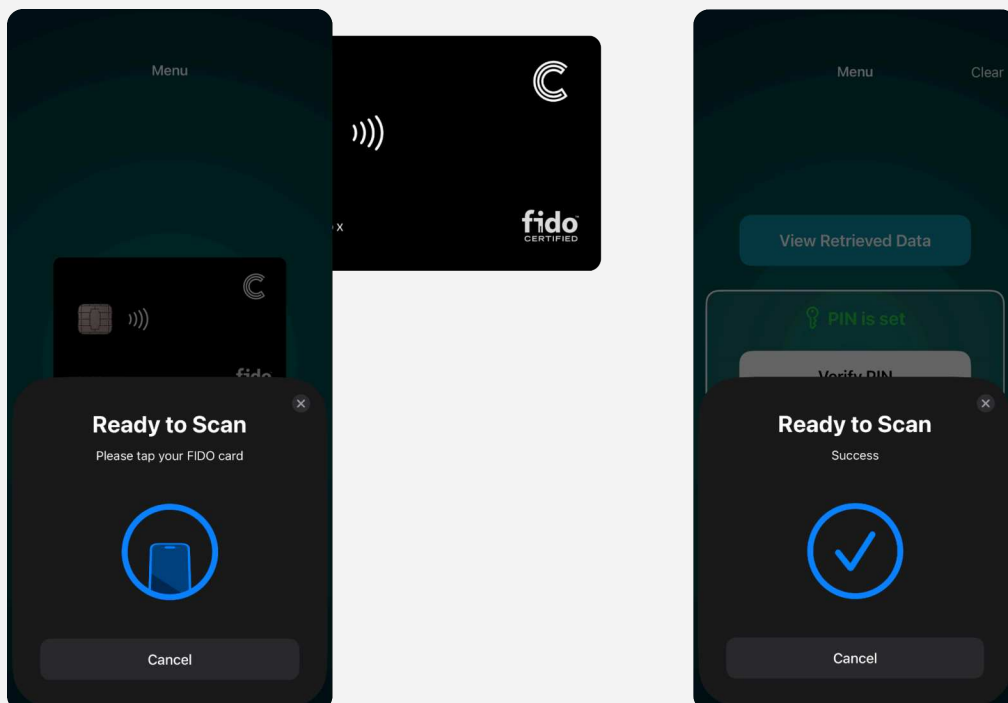
Step 1

Open the Cryptnox Card Management app on your phone and press "Get Info".



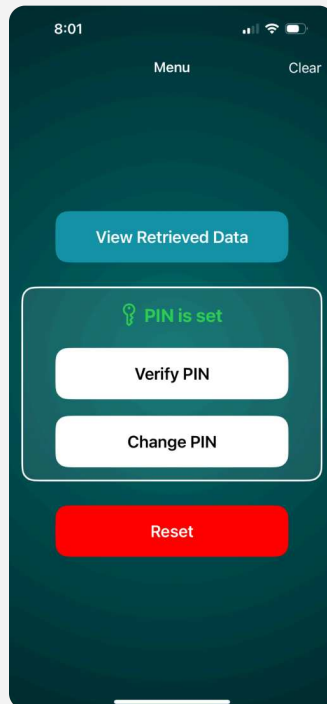
Step 2

Scan the Cryptnox Card by tapping it on the back of the phone.



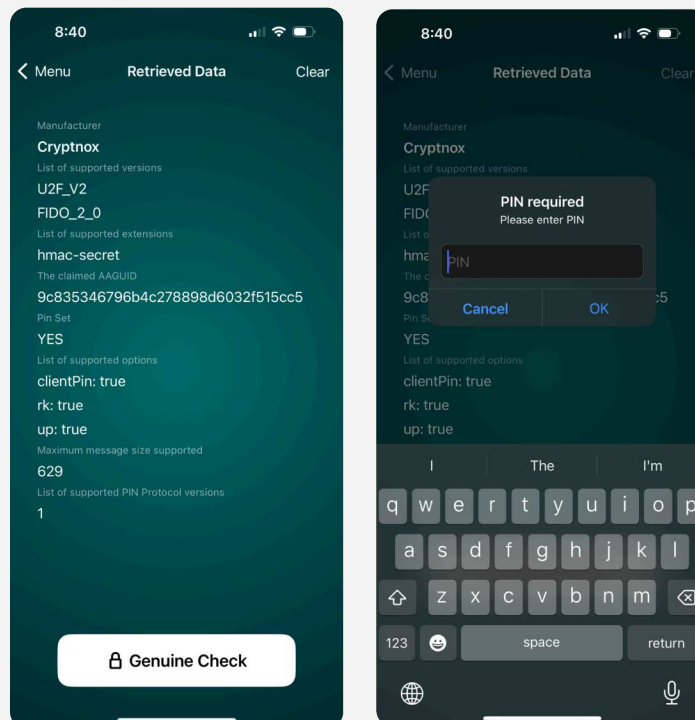
Step 3

Select "View Retrieved Data"



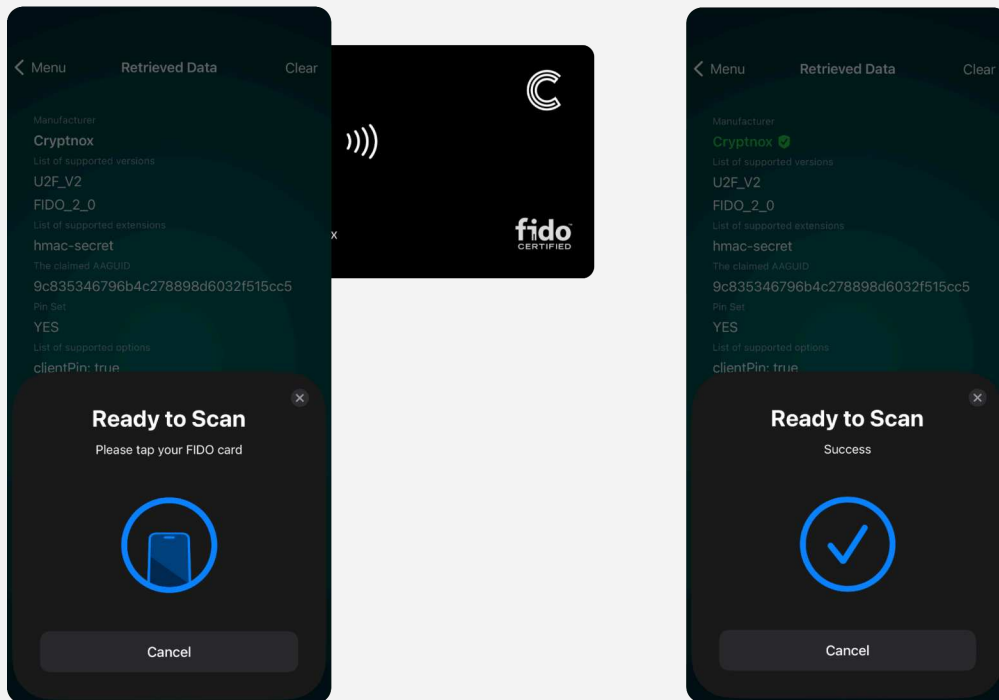
Step 4

Select the "Genuine Check" button and then you will have to enter the PIN you set for the card.



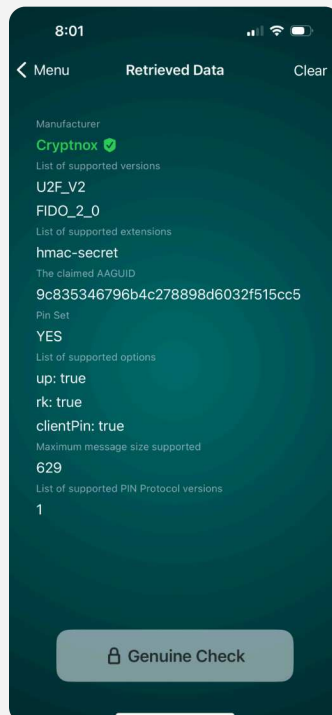
Step 5

You will have to scan the Cryptnox Card by tapping it on the back of the phone.



Step 6

You have successfully retrieved the data.



Other features of the Cryptnox FIDO2 application

The Cryptnox FIDO application offers a range of features, including:

- Setting up the Cryptnox Card
- Creating a PIN for the Cryptnox Card
- Resetting the PIN for the Cryptnox Card
- Changing the PIN for the Cryptnox Card

Discover more about the Cryptnox FIDO application here:

<https://cryptnox.com/tutorials-for-fido2-products/>

Chip Specification

Category	Details
Provider	NXP
Model	P71
JCOP Platform	JCOP 4 / JCOP 4.5
Capacitances available	17PF / 56PF / 69PF
Available functionalities from Cryptnox	FIDO2 V2.0 / V2.1 MIFARE DESFire EV1/EV2/EV3 memory 2kb - 32kb
Chip Certifications	Common Criteria EAL 6+ NIST FIPS 140-2
Communication	Contact: ISO/IEC 7816 Contactless: ISO/IEC 14443 (13,56 Mhz)
Form Factors Available	<ul style="list-style-type: none"> • Printable contact and contactless smartcard • Printable contactless smartcard (NFC only, no contact module) • Keyknob
Unique Identifier	Each Chip contain a readable unique identifier (Card ID)

Note:

FIDO functionality available on other chips upon request. MIFARE DESFire only on NXP chips.

FIDO2 v2.1 Specifications

Category	Details
Execution Environment	JCOP 4 / 4.5 from NXP with ECC module (other chips on request) - JCOP 4 / DESFire EV2-J Applet Size: 68 kb (with 64 credential slots)
Applet Certification	FIDO 2.1, Level1 Note : higher certifications available on request
Applet characteristics	<ul style="list-style-type: none"> • U2Fv2, FIDO 2.0 and FIDO 2.1 standards • NFC ISO 14443 contactless and ISO 7816 contact interfaces • EC Digital Signature (ECDSA) with NIST P256 (256R1) parameters • 32 bits signature counter, reset to 0 upon authenticator reset • Multiple accounts per Relying Party • Resident keys credentials (64 credential slots) • CredManagement commands
Applet Options	<ul style="list-style-type: none"> • HmacSecret • CredProtect • CredBlob for Resident-Keys • minPinLength: stores up to 4 authorized RPs
Client Management Application	IOS mobile application (PIN & configuration management)
AAGUID	1d1b4e33-76a1-47fb-97a0-14b10d0933f1

Certification

In recognition of Cryptnox SA's achievement of FIDO2® Authenticator Certification:

Company: Cryptnox SA
Product: Cryptnox Fido 2.1
Specification: FIDO2
Specification Version: CTAP2.1
Implementation Class: Authenticator
Authenticator Level: Level 1 (L1)
Functional Policy Version: 1.3.9
Authenticator Policy Version: 1.4
Security Requirements Version: 1.5
Interoperability Date: June 18, 2024
Conformance Self-Validation Date: May 26, 2024
Vendor Questionnaire Approval Date: August 4, 2024



Certificate No.

FIDO20020240806001

Issued

August 6, 2024

Certification

In recognition of Cryptnox SA's achievement of FIDO® U2F Authenticator Certification:

Company: Cryptnox SA
Product: Cryptnox Fido 2.1
Specification: U2F
Specification Version: 1.2
Implementation Class: Authenticator
Authenticator Level: Level 1 (L1)
Functional Policy Version: 1.3.9
Authenticator Policy Version: 1.4
Security Requirements Version: 1.5
Interoperability Date: June 18, 2024
Conformance Self-Validation Date: May 26, 2024
Vendor Questionnaire Approval Date: August 4, 2024



Certificate No.

U2F100020240806001

Issued

August 6, 2024

MIFARE DESFire

Overview

MIFARE DESFire is a family of contactless smart cards developed by NXP Semiconductors. These cards operate at a frequency of 13.56 MHz and are based on open global standards for both air interface and cryptographic methods. The DESFire product line is designed for multi-application use, where security, speed, and data integrity are paramount. They are commonly employed in applications such as public transportation, access control, and secure ID management.

Application Areas

Due to their robust security and adaptability, MIFARE DESFire cards are ideally suited for:

- **Public Transport:** E-ticketing in metro, bus, and other forms of public transportation.
- **Access Control:** Secure access to buildings, rooms, and IT assets.
- **Cashless Payment:** For canteens, vending machines, and stores.
- **Loyalty Programs:** Storage of loyalty points, membership data, etc.

Mifare Technical Specifications on Cryptnox Card

Category	Details
Versions	<ul style="list-style-type: none"> • EV2
Memory	<ul style="list-style-type: none"> • 4KB
Capacitance	<ul style="list-style-type: none"> • 17pF

About FIDO Alliance

The FIDO Alliance is an open industry association with a focused mission: reduce the world's reliance on passwords. To accomplish this, the FIDO Alliance promotes the development of, use of, and compliance with standards for authentication and device attestation.

Learn more about FIDO Alliance at: <https://fidoalliance.org/overview/>

About Mifare

MIFARE is a brand name from NXP Semiconductors, referring to a series of chips widely used in contactless smart cards and proximity cards. Today, MIFARE products are used in a variety of applications beyond transit systems, including access control, school and campus cards, and loyalty programs.

MIFARE's widespread adoption is due to its ease of integration, cost-effectiveness, and the secure nature of the technology, making it a popular choice for electronic smart card solutions globally.

Learn more about MIFARE at: <https://www.mifare.net>

About Cryptnox

Cryptnox SA is a Swiss company specializing in secure smartcards solutions for authentication and blockchain applications. They offer products like hardware wallets and FIDO2 smartcards, tailored for both individuals and businesses.

Learn more about Cryptnox at: <https://cryptnox.com>

References

<https://www.w3.org/>

<https://fidoalliance.org/>

<https://www.nxp.com/>

<https://www.nist.gov/>

<https://www.commoncriteriaportal.org/>

<https://www.mifare.net/>

<https://support.apple.com/guide/iphone/use-security-keys-iph5acc5b28c/ios>

<https://support.apple.com/en-us/102637>

NXP ® wordmark and logo are trademarks of NXP B.V.

MIFARE ® is a trademark of NXP B.V.

DESFire ® is a trademark of NXP B.V.

Document Version: 1.3 - August 2024

Copyright © 2024 CRYPTNOX SA

Address: 36 Avenue Cardinal Mermillod, 1227 Geneva, Switzerland

IDE: CHE-432.952.622